**Configure an external volume for Amazon S3**

This topic covers how to grant Snowflake restricted access to your Amazon S3 bucket using an external volume for Iceberg tables.

As a best practice, create a designated IAM policy that grants Snowflake access to your S3 location. You can then attach the policy to a role and use the security credentials generated by AWS for that role to access the files.

**Prerequisites**

Before you configure an external volume, you need the following:

* An S3 storage bucket in the **same region** that hosts your Snowflake account.
  + To use the external volume for externally managed Iceberg tables, all of your table data and metadata files must be located in the bucket.
  + Snowflake can’t support external volumes with bucket names that contain dots (for example, my.s3.bucket). Snowflake uses virtual-hosted-style paths and HTTPS to access data in S3. However, S3 does not support SSL for virtual-hosted-style buckets with dots in the name.
  + To support data recovery, [enable versioning for your external cloud storage location](https://docs.snowflake.com/en/user-guide/tables-iceberg-storage.html#label-tables-iceberg-enable-storage-versioning).
* Permissions in AWS to create and manage IAM policies and roles. If you aren’t an AWS administrator, ask your AWS administrator to perform these tasks.

**To create an external volume, you should complete below steps:**

**A screenshot of a computer

Description automatically generated**

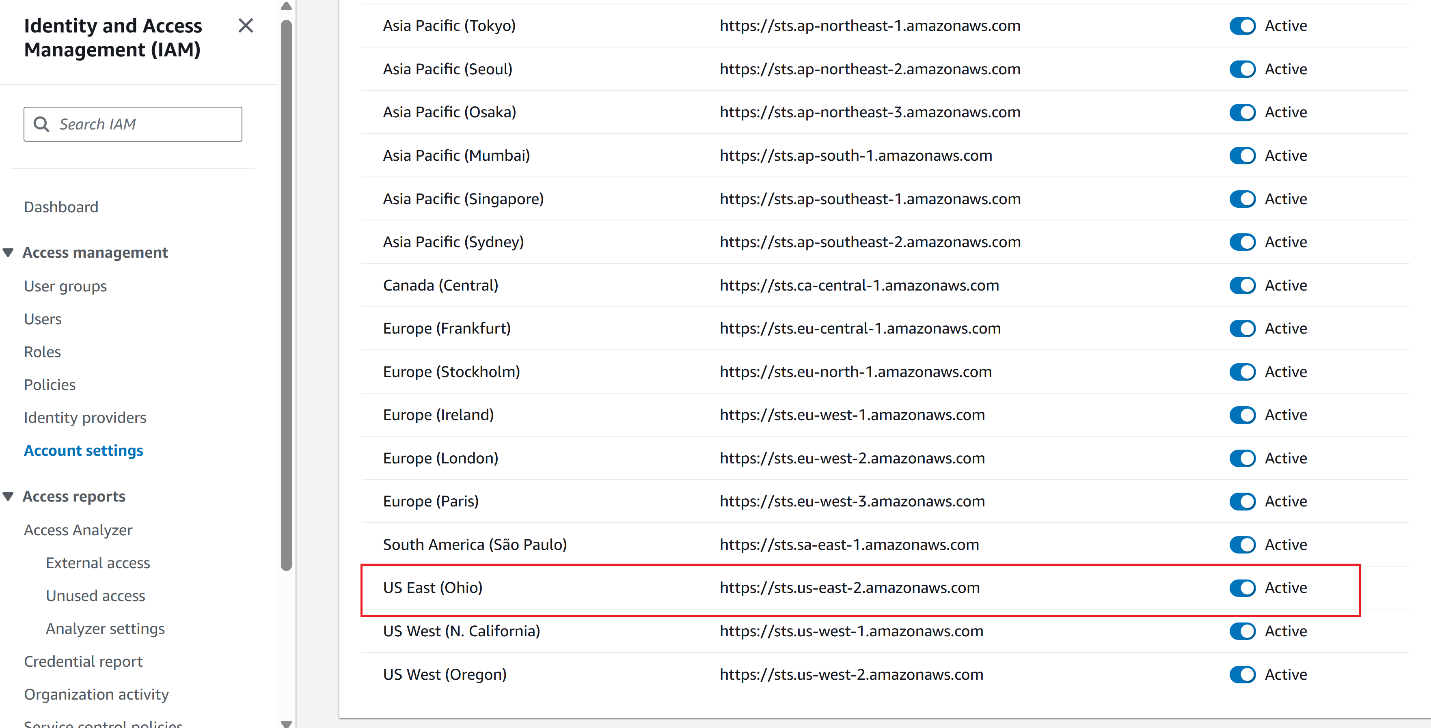
**Step 1: Create an IAM policy that grants access to your S3 location**

To configure access permissions for Snowflake in the AWS Management Console, do the following:

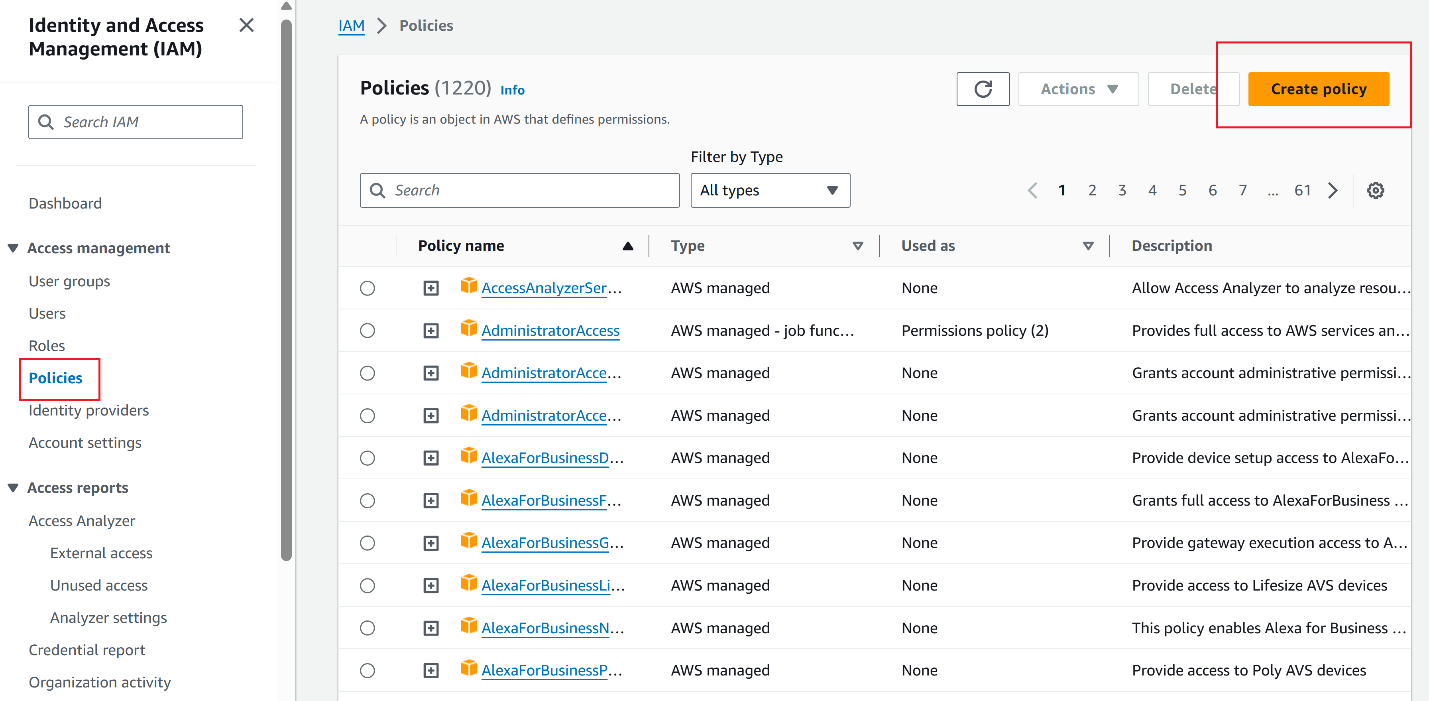
1. Log in to the AWS Management Console.
2. From the home dashboard, search for and select IAM.
3. From the left-hand navigation pane, select Account settings.
4. Under **Security Token Service (STS)** in the Endpoints list, find the Snowflake [region](https://docs.snowflake.com/en/user-guide/intro-regions) where your account is located. If the STS status is inactive, move the toggle to Active.

**A screenshot of a computer

Description automatically generated**

****

1. From the left-hand navigation pane, select Policies.
2. Select Create Policy.



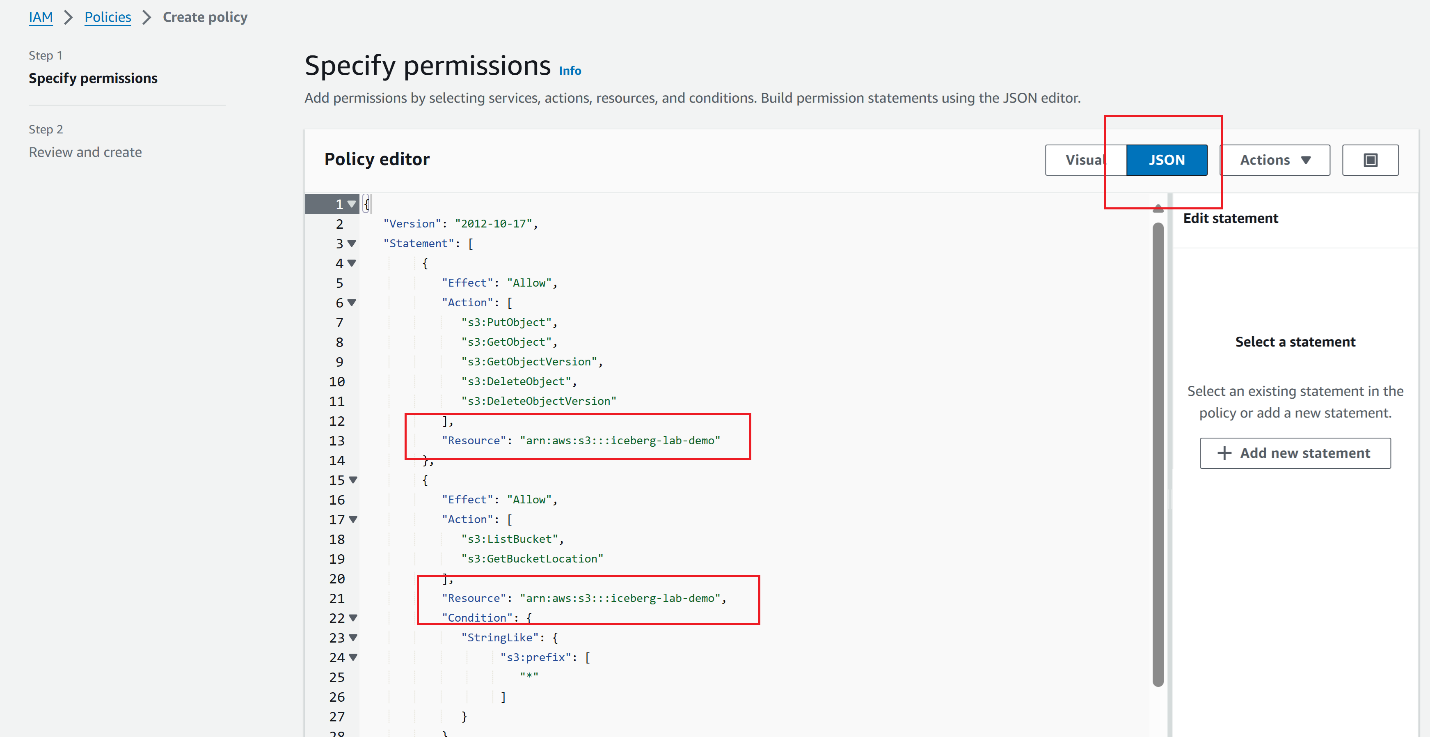
1. For **Policy editor**, select **JSON**.
2. Add a policy to provide Snowflake with the required permissions to read and write data to your S3 location.

The following example policy grants access to all locations in the specified bucket.

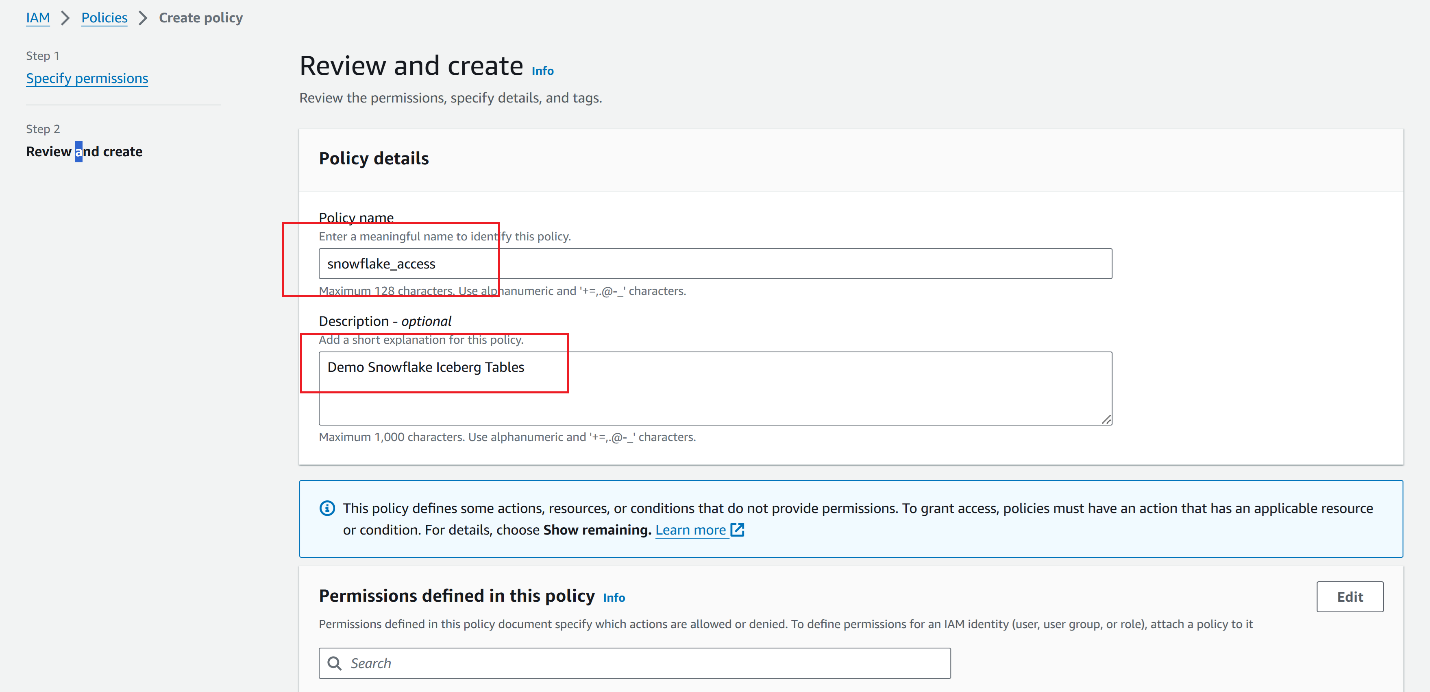
**Note**

* Replace *my\_bucket* with your actual bucket name. You can also specify a path in the bucket; for example, *my\_bucket*/*path*.
* Setting the "s3:prefix": condition to ["\*"] grants access to all prefixes in the specified bucket; setting it to ["*path*/\*"] grants access to a specified path in the bucket.
* For buckets in [government regions](https://docs.snowflake.com/en/user-guide/intro-regions.html#label-us-gov-regions), the bucket ARNs use the arn:aws-us-gov:s3::: prefix.





1. Select Next.
2. Enter a Policy name (for example, snowflake\_access) and an optional Description.
3. Select Create policy.



**Step 2: Create an IAM role**

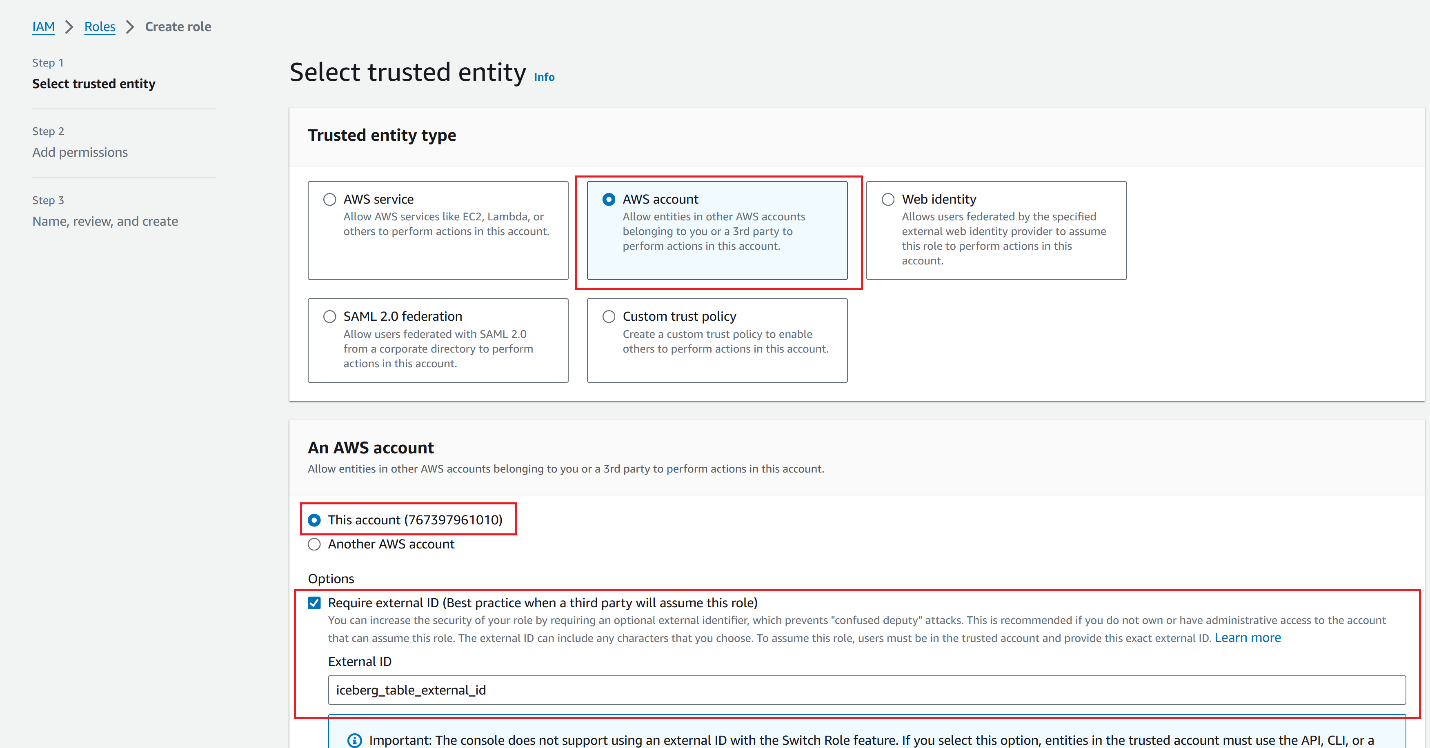
Create an AWS IAM role to grant privileges on the S3 bucket containing your data files.

1. From the left-hand navigation pane in the Identity and Access Management (IAM) Dashboard, select **Roles**.
2. Select **Create role**.

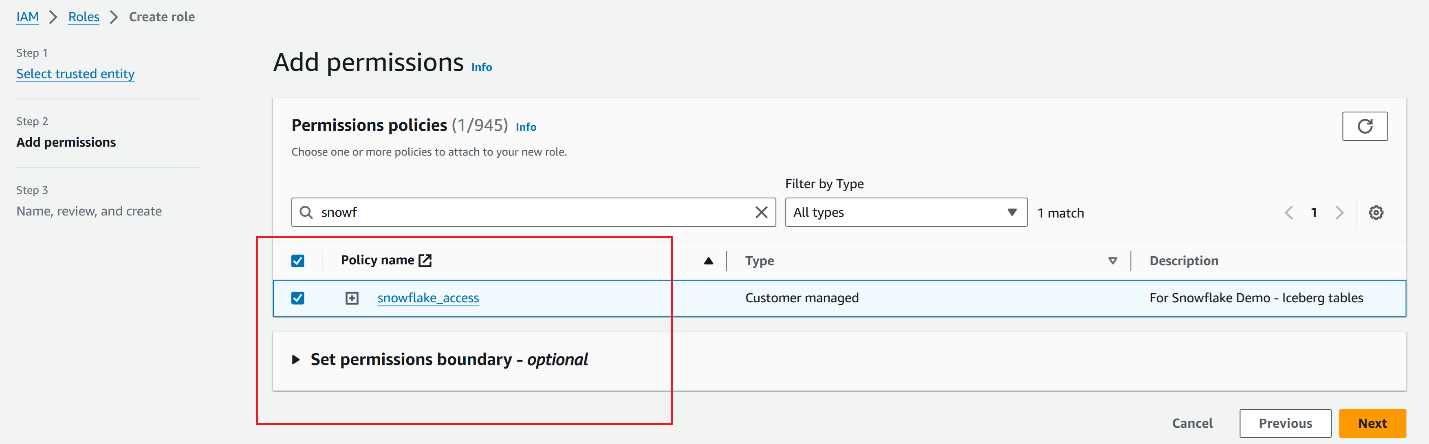
A screenshot of a computer

Description automatically generated

1. For the trusted entity type, select **AWS account**.
2. Under **An AWS account**, select **This account**. In a later step, you modify the trust relationship and grant access to Snowflake.
3. Select the **Require external ID** option. Enter an [external ID](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html) of your choice. For example, iceberg\_table\_external\_id. An external ID is used to grant access to your AWS resources (such as S3 buckets) to a third party like Snowflake.



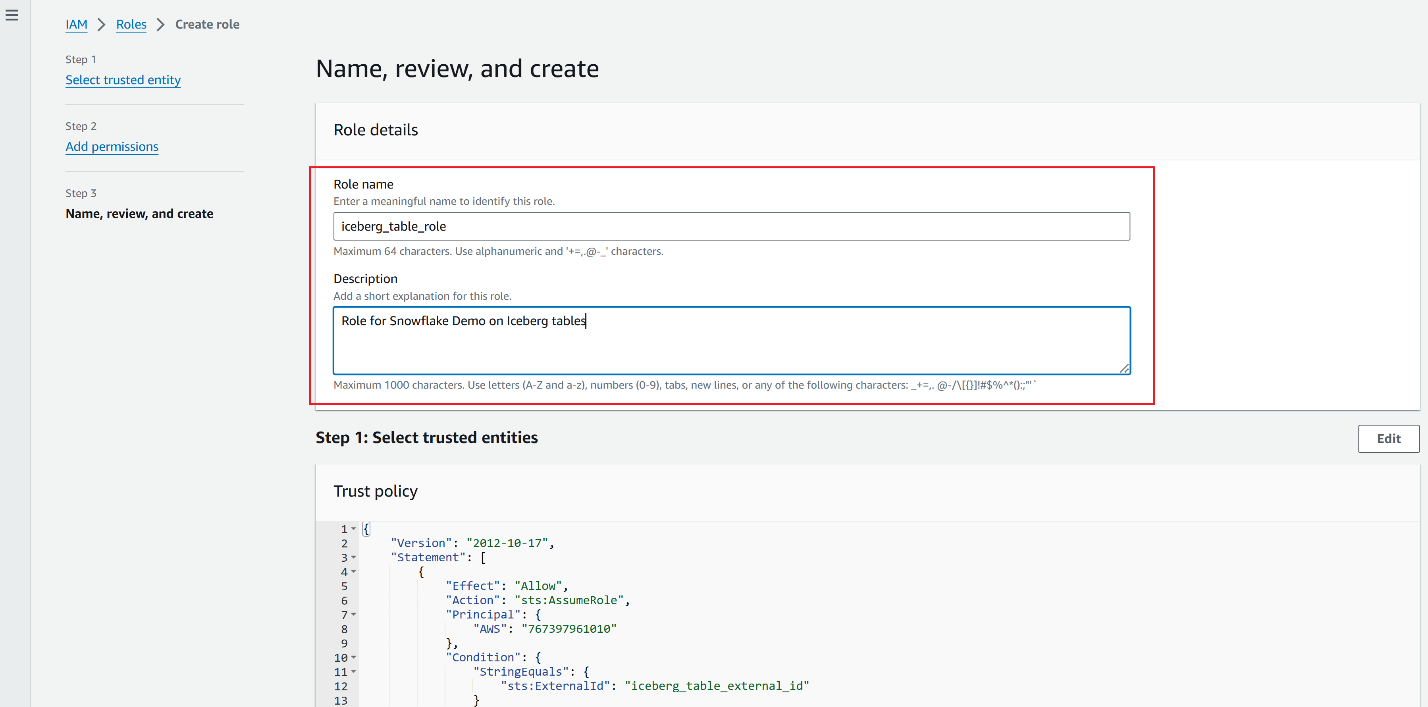
1. Select Next.
2. Select the policy that you created for the external volume, then select Next.



1. Enter a Role name and description for the role, then select Create role.

You have now created an IAM policy for an S3 location, created an IAM role, and attached the policy to the role.

1. Select View role to view the role summary page. Locate and record the ARN (Amazon Resource Name) value for the role.



**Step 3: Grant privileges required for SSE-KMS encryption to the IAM role (optional)**

If you want to upload an object encrypted with an AWS KMS key to Amazon S3, the IAM role that you created for your external volume needs kms:GenerateDataKey permissions on the key. To download an object encrypted with an AWS KMS key, the IAM role needs kms:Decrypt permissions on the key.

If you want to use a KMS key for your server-side encryption, follow these steps to create a key and reference it.

1. In the AWS Management Console, go to the Key Management Service (KMS). From the left navigation, select **Customer managed keys**, and then select **Create key**. You must create a key in the same region as your bucket.
2. Create a **Symmetric** key type. For the key usage, select **Encrypt and decrypt**. Select **Next**.
3. For **Alias**, enter a name for the key and select **Next**.
4. If needed, select an administrator for the key and select **Next**.
5. For **Define key usage permissions**, select your IAM role, then select **Next**.
6. Review the key configuration details, then select **Finish** to create the key.
7. Find the key in the list of customer managed keys, select it, and record its ARN. The following is an example of an ARN for a key: arn:aws:kms:us-west-2:111111122222:key/1a1a11aa-aa1a-aaa1a-a1a1-000000000000.

When you create your external volume, set the KMS\_KEY\_ID value to the ARN of your key.

**Step 4: Create an external volume in Snowflake**

Create an external volume using the [CREATE EXTERNAL VOLUME](https://docs.snowflake.com/en/sql-reference/sql/create-external-volume) command. The following example creates an external volume named **iceberg\_lab\_vol** that defines a single Amazon S3 storage location.

**USE ROLE ACCOUNTADMIN;**

**CREATE OR REPLACE EXTERNAL VOLUME iceberg\_lab\_vol**

**STORAGE\_LOCATIONS =**

**(**

**(**

**NAME = 'my-s3-us-east-1'**

**STORAGE\_PROVIDER = 'S3'**

**STORAGE\_BASE\_URL = 's3://iceberg-lab-demo/'**

**STORAGE\_AWS\_ROLE\_ARN = 'arn:aws:iam::\*\*\*\*\*\*\*\*\*:role/iceberg\_table\_role'**

**STORAGE\_AWS\_EXTERNAL\_ID = 'iceberg\_table\_external\_id'**

**)**

**);**

The example specifies the external ID (**iceberg\_table\_external\_id**) associated with the IAM role that you created for the external volume. Specifying an external ID lets you use the same IAM role (and external ID) across multiple external volumes.

**Step 5: Retrieve the AWS IAM user for your Snowflake account**

1. Retrieve the ARN for the AWS IAM user that was created automatically for your Snowflake account using the [DESCRIBE EXTERNAL VOLUME](https://docs.snowflake.com/en/sql-reference/sql/desc-external-volume) command. Specify the name of your external volume.

The following example describes an external volume.

**DESC EXTERNAL VOLUME iceberg\_lab\_vol;**

1. Record the value for the STORAGE\_AWS\_IAM\_USER\_ARN property, which is the AWS IAM user created for your Snowflake account;

for example,  arn:aws:iam:: 123456789001:role/iceberg\_table\_role.

Snowflake provisions a single IAM user for your entire Snowflake account. All S3 external volumes in your account use that IAM user.

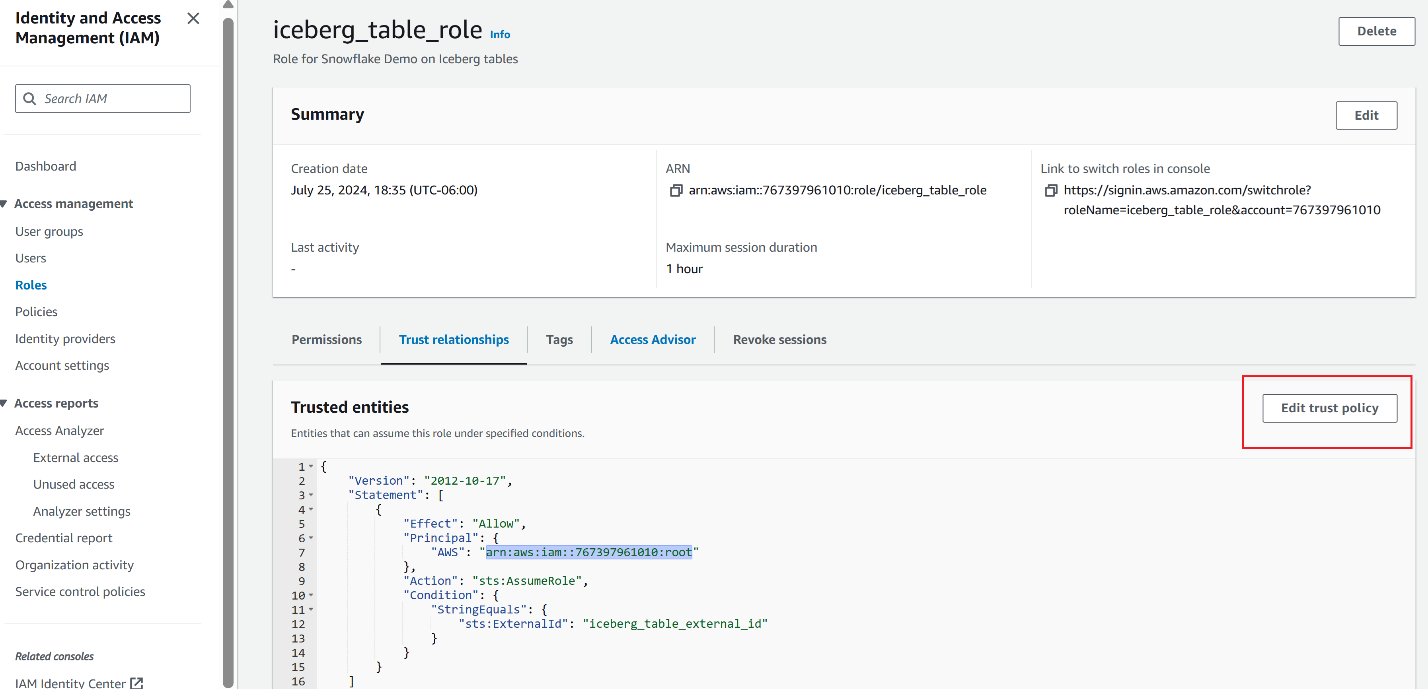
**Note**

If you didn’t specify an external ID (STORAGE\_AWS\_EXTERNAL\_ID) when you created an external volume, Snowflake generates an ID for you to use. Record the value so that you can update your IAM role trust policy with the generated external ID.

**Step 6: Grant the IAM user permissions to access bucket objects**

In this step, you configure permissions that allow the IAM user for your Snowflake account to access objects in your S3 bucket.

1. Log in to the AWS Management Console.
2. From the home dashboard, search for and select **IAM**.
3. From the left-hand navigation pane, select **Roles**.
4. Select the IAM role that you created for your external volume.
5. Select the **Trust relationships** tab.
6. Select **Edit trust policy**.



1. Modify the policy document with the DESC EXTERNAL VOLUME output values that you recorded.



Where:

* + *snowflake\_user\_arn* is the STORAGE\_AWS\_IAM\_USER\_ARN value you recorded.
  + *iceberg\_table\_external\_id* is your external ID. If you *already* specified an external ID when you created the role, and used the same ID to create your external volume, leave the value as-is. Otherwise, update sts:ExternalId with the value that you recorded.

**Note**

You must update this policy document if you create a new external volume (or recreate an existing external volume using the CREATE OR REPLACE EXTERNAL VOLUME syntax) and don’t provide your own external ID. For security reasons, a new or recreated external volume has a different external ID and cannot resolve the trust relationship unless you update this trust policy.

1. Select Update policy to save your changes.

**Step 7: Create a Snowflake-managed Iceberg Table**

Create an Iceberg Table referencing the external volume you just created.