

Date

CREATE INTEGRATION OBJECT

1. GOALS

In this assignment, we will create integration object. Integration object helps to make secure connection from snowflake to aws s3.


Prerequisites,

AWS Free tier account.

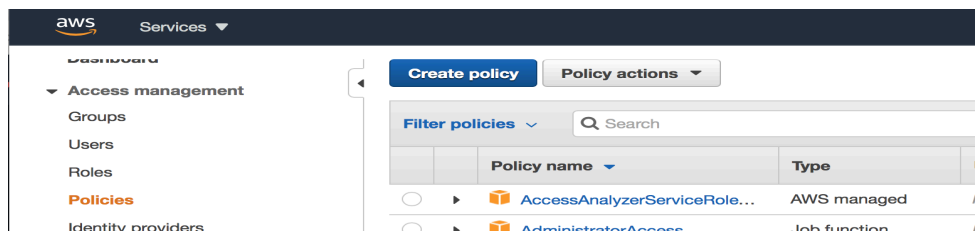
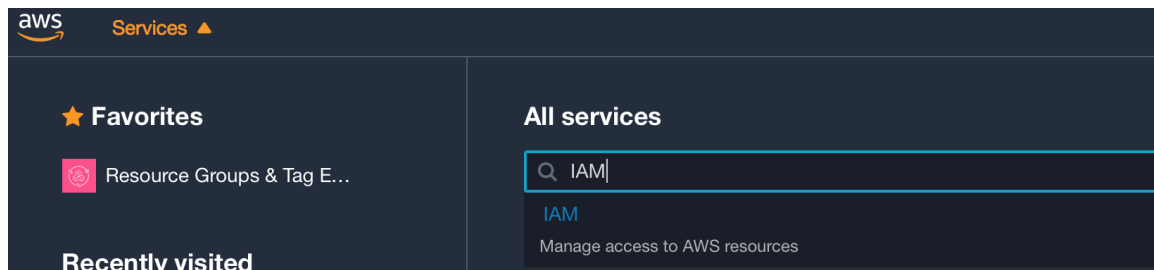
Click on below link and create aws free tier account.

2. CREATE AWS S3 BUCKET

Search for s3 in search panel and create bucket as below,

+ Create bucket		Edit public access settings	Empty	Delete	1 Buckets		1 Regions	↻
<input type="checkbox"/>	Bucket name ▾	Access ⓘ ▾	Region ▾		Date created ▾			
<input type="checkbox"/>	 hartfordstar	Bucket and objects not public	US East (N. Virginia)		Oct 9, 2020 3:50:03 PM GMT+0530			

3. CREATE POLICY



Add policy in the json tab.

Please find the attached policy below,

Visual editorJSONImport managed policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "s3:PutObject",  
8         "s3:GetObject",  
9         "s3:GetObjectVersion",  
10        "s3:DeleteObject",  
11        "s3:DeleteObjectVersion"  
12      ],  
13      "Resource": "arn:aws:s3:::<bucket>/<prefix>/*"  
14    },  
15    {  
16      "Effect": "Allow",
```

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:PutObject",  
        "s3:GetObject",  
        "s3:GetObjectVersion",  
        "s3:DeleteObject",  
        "s3:DeleteObjectVersion"  
      ],  
      "Resource": "arn:aws:s3:::<bucket>/<prefix>/*"  
    },  
    {  
      "Effect": "Allow",  
      "Action": "s3:ListBucket",  
      "Resource": "arn:aws:s3:::<bucket>",  
      "Condition": {  
        "StringLike": {
```

```

"s3:prefix": [
  "<prefix>/*"
]
}
}
}
}
}
}
}
}
}
}

```

Name the policy and create it,

I am naming policy as, **snowflake_access**

Review policy

Name*

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

Description

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

Summary

<input type="text" value="Filter"/>			
Service ▾	Access level	Resource	Request condition
Allow (1 of 241 services) Show remaining 240			
S3	Limited: List, Read, Write	Multiple	s3:prefix string like All

4. CREATE ROLE

Search for IAM and click on Roles.

Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- [IAM Roles FAQ](#)
- [IAM Roles Documentation](#)
- [Tutorial: Setting Up Cross Account Access](#)
- [Common Scenarios for Roles](#)

[Create role](#) [Delete role](#)

Search IAM

Search

Role name	Trusted entities
AWSServiceRoleForSupport	AWS service: support (Service-Linked role)

AWS account ID:
579834220952

Note down your AWS account id,


AWS account ID:
579834220952

Choose another AWS account,

Create role

1 2 3 4

Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID*

Options
☐ Require external ID (Best practice when a third party will assume this role)
☐ Require MFA

Fill Account ID in the, Account ID test box.

Choose external id check box to add snowflake external id.

Specify accounts that can use this role

Account ID* ⓘ

Options ☒ Require external ID (Best practice when a third party will assume this role)

You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. [Learn more](#)

External ID

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. [Learn more](#)

☐ Require MFA ⓘ

For time being we will fill external Id as 0000.

Click on next and choose the policy we created in the previous step,

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy ↺

Filter policies ▼ Showing 3 results

	Policy name ▼	Used as
<input type="checkbox"/>	▶ AmazonMobileAnalyticsNon-financialReportAccess	None
<input type="checkbox"/>	▶ AWSServiceRoleForAmazonEKSNodegroup	None
<input checked="" type="checkbox"/>	▶ snowflake_access	None

Leave next page blank,

Create role

1 2 3 4

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 50 more tags.

Click on next, to create role. Name the role as , snowflake_role.

Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name*

Use alphanumeric and '+=,@-_' characters. Maximum 64 characters.

Role description

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

Trusted entities The account 579834220952

Policies [snowflake_access](#)

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

[Cancel](#) [Previous](#) [Create role](#)

5. CREATE INTEGRATION OBJECT

Login to snowflake. Execute below command to create integration object.

```
create or replace storage integration s3_int
```

```
type = external_stage
```

```
storage_provider = s3
```

```
enabled = true
```

```
storage_aws_role_arn = 'arn:aws:iam::579834220952:role/snowflake_role'
```

```
storage_allowed_locations = ('s3://hartfordstar/');
```

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with 'Identity and Access Management (IAM)' selected. The main content area displays the 'Summary' for the role 'snowflake_role'. A box highlights the 'Role ARN' field, which contains 'arn:aws:iam::579834220952:role/snowflake_role'. An arrow points from the 'storage_aws_role_arn' command in the previous block to this highlighted ARN. Other details shown include the role description, instance profile ARNs, path, creation time (2020-10-09 16:35 UTC+0530), last activity, and maximum session duration (1 hour).

Add snowflake external id to aws s3. In below image external id is not updated,

Permissions
Trust relationships
Tags
Access Advisor
Revoke sessions

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

Trusted entities

The account 579834220952

Conditions

The following conditions define how and when trusted entities can assume the role.

Condition	Key	Value
StringEquals	sts:ExternalId	0000

Describe integration object, **DESC INTEGRATION s3_int;**

DESC INTEGRATION s3_int;

5

Data Preview

Open Histor

query ID

SQL

147ms

7 rows

result...

Download

Copy

Columns

Row	property	property_type	property_value	property_default
1	ENABLED	Boolean	true	false
2	STORAGE_PROVIDER	String	S3	
3	STORAGE_ALLOWED_LOCATIONS	List	s3://hartfordstar/	[]
4	STORAGE_BLOCKED_LOCATIONS	List		[]
5	STORAGE_AWS_IAM_USER_ARN	String	arn:aws:iam::98...	
6	STORAGE_AWS_ROLE_ARN	String	arn:aws:iam::57...	
7	STORAGE_AWS_EXTERNAL_ID	String	EGA46122_SFC...	

Click on,

You can view the trusted entities that can assume the role.

Edit trust relationship

Trusted entities

Update trust relationship as below,

DESC INTEGRATION s3_int;

5

Data Preview

Open Histor

query ID

SQL

147ms

7 rows

result...

Download

Copy

Columns

Row	property	property_type	property_value	property_default
1	ENABLED	Boolean	true	false
2	STORAGE_PROVIDER	String	S3	
3	STORAGE_ALLOWED_LOCATIONS	List	s3://hartfordstar/	[]
4	STORAGE_BLOCKED_LOCATIONS	List		[]
5	STORAGE_AWS_IAM_USER_ARN	String	arn:aws:iam::98...	
6	STORAGE_AWS_ROLE_ARN	String	arn:aws:iam::57...	
7	STORAGE_AWS_EXTERNAL_ID	String	EGA46122_SFC...	

Policy Document

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::579834220952:root"  
8       },  
9       "Action": "sts:AssumeRole",  
10      "Condition": {  
11        "StringEquals": {  
12          "sts:ExternalId": "0000"  
13        }  
14      }  
15    }  
16  ]  
17 }
```