

Snowflake External Stage

Tuesday, July 25, 2023 9:10 PM

External Stage Creation

Step 1 : Open AWS account and Login to that.

Step 2: First create a bucket :

The screenshot shows the AWS S3 Buckets page. At the top, there's an 'Account snapshot' section with a 'View Storage Lens dashboard' button. Below it, the 'Buckets (3) Info' section shows three buckets: 'newproductbucketsk', 'testbuckets3k', and 'titanicbucketk'. To the right of the table is a 'Create bucket' button, which is circled in red. The table has columns for Name, AWS Region, Access, and Creation date.

Name	AWS Region	Access	Creation date
newproductbucketsk	US East (Ohio) us-east-2	Bucket and objects not public	July 24, 2023, 14:14:02 (UTC+05:30)
testbuckets3k	US East (Ohio) us-east-2	Bucket and objects not public	July 24, 2023, 12:08:08 (UTC+05:30)
titanicbucketk	US East (Ohio) us-east-2	Objects can be public	July 25, 2023, 08:37:54 (UTC+05:30)

The screenshot shows the 'Create bucket' wizard. The first step, 'General configuration', has two fields highlighted with red circles: 'Bucket name' containing 'bucketproduct' and 'AWS Region' set to 'US East (Ohio) us-east-2'. Below these, there's a note about copy settings and a 'Choose bucket' button. The next section, 'Bucket Key', is partially visible. At the bottom, there's an 'Advanced settings' section and a note about uploading files after creation, followed by a 'Create bucket' button.

Step 3: Upload data into the bucket :

The image consists of three vertically stacked screenshots of the AWS S3 console, illustrating the upload process for a new bucket.

Screenshot 1: Bucket Overview

This screenshot shows the 'Objects' tab of the 'bucketproductnew' bucket. The top navigation bar includes 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. A red circle highlights the 'Upload' button in the top right corner of the toolbar.

Screenshot 2: Upload Page

This screenshot shows the 'Upload' page for the 'bucketproductnew' bucket. It features a large central area for dragging and dropping files, with the placeholder text 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Below this is a table for managing files and folders, with a red circle highlighting the 'Add files' button. The table has columns for Name, Folder, Type, and Size.

Screenshot 3: Destination Configuration

This screenshot shows the 'Destination' configuration step. It displays the destination bucket as 's3://bucketproductnew'. Below it, 'Destination details' are shown, along with sections for 'Permissions' and 'Properties'. At the bottom right, a red circle highlights the 'Upload' button. A green status bar at the bottom indicates 'Upload succeeded'.

Upload succeeded
View details below.

s3://bucketproductnew	1 file, 180.0 B (100.00%)	0 files, 0 B (
-----------------------	---------------------------	----------------

Files and folders Configuration

Files and folders (1 Total, 180.0 B)

Name	Folder	Type	Size	Status
productkousik.csv	-	text/csv	180.0 B	Succeeded

Step 4: Go to IAM :

The screenshot shows the AWS search bar with 'IAM' typed in and highlighted with a red circle. Below the search bar, the 'Services' section is visible, with the 'IAM' service card highlighted with a red oval. The card text reads: 'Manage access to AWS resources'.

Step 5: Go to User groups:

The screenshot shows the IAM dashboard. On the left, the navigation menu has a section titled 'Access management' with a 'User groups' link, which is circled in red. The main dashboard area displays security recommendations and IAM resources statistics (2 user groups, 3 users).

Step 6: Create User group:

User groups (2) <small>Info</small>																		
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.																		
<input type="button" value="Create group"/> <input type="button" value="Delete"/>																		
<input type="text" value="Filter User groups by property or group name and press enter"/>																		
<table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Group name</th> <th>Users</th> <th>Permissions</th> <th>Creation time</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>kousikdutta1</td> <td>>Loading</td> <td>>Loading</td> <td>Yesterday</td> </tr> <tr> <td><input type="checkbox"/></td> <td>titanickousik</td> <td>>Loading</td> <td>>Loading</td> <td>12 hours ago</td> </tr> </tbody> </table>				<input type="checkbox"/>	Group name	Users	Permissions	Creation time	<input type="checkbox"/>	kousikdutta1	>Loading	>Loading	Yesterday	<input type="checkbox"/>	titanickousik	>Loading	>Loading	12 hours ago
<input type="checkbox"/>	Group name	Users	Permissions	Creation time														
<input type="checkbox"/>	kousikdutta1	>Loading	>Loading	Yesterday														
<input type="checkbox"/>	titanickousik	>Loading	>Loading	12 hours ago														

Provide a name to the group :

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

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

Give permission to "S3 full access" and "administrator access" :

Attach permissions policies - <small>Optional</small>			
(Selected 2/860)			
Info			
<p>You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.</p>			
<input type="text" value="Filter policies by property or policy name and press enter."/>		9 matches	< 1 >
<input style="border: 1px solid #ccc; padding: 2px; width: 100px; margin-right: 10px;" type="text" value="s3"/> <input type="button" value="Clear filters"/>			
Policy name	Type	Description	
<input checked="" type="checkbox"/>  AmazonS3FullAccess	AWS managed	Provides full access to all objects in an Amazon S3 bucket.	
<input type="checkbox"/>  AmazonS3ReadOnlyAccess	AWS managed	Provides read only access.	
<input type="checkbox"/>  AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage Amazon DMS Redshift S3.	

Step 6: Create User :

Users (3) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

<input type="button" value=""/>	<input type="button" value="Delete"/>	<input style="background-color: #0072BC; color: white; font-weight: bold; border-radius: 5px; padding: 2px 10px; border: none;" type="button" value="Add users"/>
---------------------------------	---------------------------------------	---

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password a...
<input type="checkbox"/>	kousikdutta	kousikduttasl	Never	None	None
<input type="checkbox"/>	kousikduttasl	kousikduttasl	Never	None	None
<input type="checkbox"/>	Kousikttanicuser	titanickousik	Never	None	None

Give user name :**Specify user details**

User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

i If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Map the particular user to the group :

Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
 Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
 Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/3)

<input type="checkbox"/>	Group name	Users	Attached policies	Created
--------------------------	------------	-------	-------------------	---------

<input type="checkbox"/>	kousikduttasl	2	AmazonS3FullAccess	2023-07-24 (Y...)
<input checked="" type="checkbox"/>	newproductgroup	0	AmazonS3FullAccess ...	2023-07-25 (3...)
<input type="checkbox"/>	titanickousik	1	AmazonS3FullAccess ...	2023-07-25 (1...)

Next we will be able to see something like below:

The screenshot shows the 'Review and create' step of the IAM user creation wizard. On the left, a sidebar lists 'Step 1 Specify user details', 'Step 2 Set permissions', and 'Step 3 Review and create'. The main area displays 'User details' with a red underline under the 'User name' field, which contains 'newproductuser'. It also shows 'Console password type' as 'None' and 'Require password' as 'No'. Below this is a 'Permissions summary' table with one row: 'newproductgroup' (Type: Group, Used as: Permissions group), also underlined in red.

Then click on create User.

Step 7: Create Role :

The screenshot shows the 'Roles' page in the IAM console. The sidebar includes 'Identity and Access Management (IAM)', 'Dashboard', and 'Access management' sections with 'User groups', 'Users', 'Roles' (selected), 'Policies', 'Identity providers', and 'Account settings'. The main area shows a table of existing roles, with the 'Create role' button at the top right highlighted by a red circle.

Click on AWS Account :

The screenshot shows the 'Select trusted entity' step of the IAM role creation wizard. The sidebar includes 'Step 1 Select trusted entity', 'Step 2 Add permissions', and 'Step 3 Name, review, and create'. The main area shows a 'Trusted entity type' section with five options: 'AWS service' (radio button unselected), 'AWS account' (radio button selected and highlighted with a red arrow), 'Web identity' (radio button unselected), 'SAML 2.0 federation' (radio button unselected), and 'Custom trust policy' (radio button unselected).

Click on next :

An AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

- This account (530595819296)
 Another AWS account

Options

- Require external ID (Best practice when a third party will assume this role)
 Require MFA
Requires that the assuming entity use multi-factor authentication.

Cancel

Next



Give permission to "S3 full access" and "administrator access" :

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

Permissions policies (Selected 2/860) Info

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



Create policy

<input type="checkbox"/>	Policy name	Type	Description
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS m...	Provides full access to all buckets via the AWS Management...
<input type="checkbox"/>	AmazonS3ReadOnl...	AWS m...	Provides read only access to all buckets via the AWS Manag...
<input type="checkbox"/>	AmazonDMSRedshi...	AWS m...	Provides access to manage S3 settings for Redshift endpoint...

Click on next :

Cancel

Previous

Next

Give the name of the role :

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

newproductrole

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

Description

Add a short explanation for this role.

This is for creating external stage

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

Click on create role :

Tags

Add tags - optional [Info](#)

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.

[Add tag](#)

You can add up to 50 more tags.

[Cancel](#)

[Previous](#)

[Create role](#)

It will show like below :

The screenshot shows the AWS IAM Roles page. At the top, there is a green banner with a checkmark icon and the text "Role newproductrole created." To the right of the banner are "View role" and "X" buttons. Below the banner, the page title is "IAM > Roles". A sub-header "Roles (6) [Info](#)" is displayed, with a description: "An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust." To the right of the sub-header are "Edit" and "Delete" buttons, and a blue "Create role" button. Below the sub-header is a search bar with the placeholder "Search" and navigation controls for pages 1, 2, and 3. The main table has columns: a checkbox, "Role name", "Trusted entities", and "Last acti...".

Step 7: Next go to Snowflake CLI and execute below commands:

Select a particular database and schema

```
Kousikdutta#COMPUTE_WH@(no database).(no schema)>use myfirstdatabase.salesschema;
+-----+
| status
+-----+
| Statement executed successfully.
+-----+
```

Create CSV Format :

```
create or replace file format MYFIRSTDATABASE.SALESSCHEMA.my_csv_format
  type = csv
  field_delimiter = ','
  skip_header = 1
  null_if = ('NULL', 'null')
  empty_field_as_null = true;
```

Next go to the role and copy the ARN :

The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' at the top, followed by 'Dashboard', 'Access management' (with 'User groups' and 'Policies' under it), 'Users', and 'Roles' (which is highlighted with a red circle). Below these are 'Identity providers' and 'AWS services'. The main area shows a role named 'newproductrole' with the following details:

Summary
Creation date: July 25, 2023, 21:52 (UTC+05:30)
ARN: arn:aws:iam::530595819296:role/newproductrole
Last activity: None
Maximum session duration: 1 hour

A red box highlights the ARN value 'arn:aws:iam::530595819296:role/newproductrole'.

Then , copy the bucket name which you have created and ARN and write the below code and execute:

```
Kousikdutta#COMPUTE_WH@MYFIRSTDATABASE.SALESSCHEMA>create or replace storage integration s3_int2
  type = external_stage
  storage_provider = s3
  enabled = true
  storage_aws_role_arn = 'arn:aws
  :iam::530595819296:role/newproductrole'
  storage_allowed_locations = ('s3://bucketproductnew/');

+-----+
| status |
+-----|
| Integration S3_INT2 successfully created. |
```

Next create the below stage :

```
Kousikdutta#COMPUTE_WH@MYFIRSTDATABASE.SALESSCHEMA>CREATE STAGE my_s3_stage3
  STORAGE_INTEGRATION = s3_int2
  URL = 's3://bucketproductnew/productkousik.csv'
  file_format = my_csv_format;

+-----+
| status |
+-----|
| Stage area MY_S3_STAGE3 successfully created. |
```

Don't forget to check the integration description :

```
Kousikdutta#COMPUTE_WH@MYFIRSTDATABASE.SALESSCHEMA>desc integration s3_int2;
+-----+-----+-----+-----+
| property | property_type | property_value | property_default |
+-----+-----+-----+-----+
| ENABLED | Boolean | true | false |
| STORAGE_PROVIDER | String | S3 | [] |
| STORAGE_ALLOWED_LOCATIONS | List | s3://bucketproductnew/ | [] |
| STORAGE_BLOCKED_LOCATIONS | List | | [] |
| STORAGE_AWS_IAM_USER_ARN | String | arn:aws:iam::942624237177:user/5psa0000-s | |
| STORAGE_AWS_ROLE_ARN | String | arn:aws:iam::530595819296:role/newproductrole | |
| STORAGE_AWS_EXTERNAL_ID | String | ZC56539_SFCRole=2_uXHmkGGm4cLVAW+GKXzERb/of1s= | |
| COMMENT | String | | |
+-----+-----+-----+-----+
8 Row(s) produced. Time Elapsed: 0.324s
Kousikdutta#COMPUTE_WH@MYFIRSTDATABASE.SALESSCHEMA>
```

Step 8: Next change the Trust relationship in role:

```
Kousikdutta#COMPUTE_WH@MYFIRSTDATABASE.SALESSCHEMA>desc integration s3_int2;
+-----+-----+-----+-----+
| property | property_type | property_value | property_default |
+-----+-----+-----+-----+
| ENABLED | Boolean | true | false |
| STORAGE_PROVIDER | String | S3 | [] |
| STORAGE_ALLOWED_LOCATIONS | List | s3://bucketproductnew/ | [] |
| STORAGE_BLOCKED_LOCATIONS | List | | [] |
| STORAGE_AWS_IAM_USER_ARN | String | arn:aws:iam::942624237177:user/5psa0000-s | |
| STORAGE_AWS_ROLE_ARN | String | arn:aws:iam::530595819296:role/newproductrole | |
| STORAGE_AWS_EXTERNAL_ID | String | ZC56539_SFCRole=2_uXHmkGGm4cLVAW+GKXzERb/of1s= | |
| COMMENT | String | | |
+-----+-----+-----+-----+
8 Row(s) produced. Time Elapsed: 0.324s
Kousikdutta#COMPUTE_WH@MYFIRSTDATABASE.SALESSCHEMA>
```

In the above "Storage_AWS_IAM_User_ARN" and "External ID" <- copy both of them and paste it in trust relationship :

Go to : --> role >> Trust relationship --> Edit trust policy

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there's a navigation pane with links like 'Dashboard', 'Access management' (which is expanded), 'User groups', 'Users', 'Roles' (which is highlighted with a red circle), 'Policies', and 'Identity providers'. The main area has tabs for 'Permissions', 'Trust relationships' (which is highlighted with a red circle), 'Tags', 'Access Advisor', and 'Revoke sessions'. Below the tabs, there's a section titled 'Trusted entities' with the sub-instruction 'Entities that can assume this role under specified conditions.' To the right, there's a large text area showing a JSON policy document. A red circle highlights the 'Edit trust policy' button at the top right of this area.

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Principal": {
7                  "AWS": "arn:aws:iam::530595819296:root"
8              },
9              "Action": "sts:AssumeRole",
10             "Condition": {}
11         }
12     ]
13 }
```

Let's edit that :

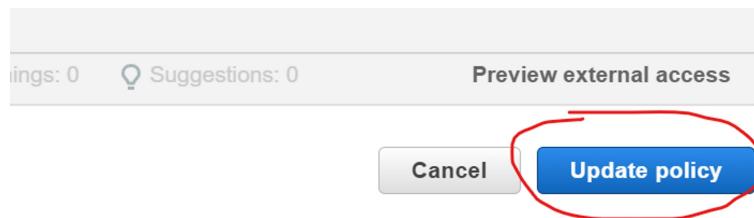
Below are the "Storage_AWS_IAM_User_ARN" and "External ID" values which we have got from the above, change them accordingly as shown below :

```

1 v {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Effect": "Allow",
6             "Principal": {
7                 "AWS": "arn:aws:iam::942624237177
8                     :user/5psa0000-s"
9             },
10            "Action": "sts:AssumeRole",
11            "Condition": {"StringEquals": {"sts
12                :ExternalId": "ZC56539_SFCRole
13                    =2_uXHmkGGm4cLVAW+GKXzERb/of1s="}
14        }
15    }

```

Click on update policy :



Step 9: Next create the schema in snowflake :

```

create table productnew (
    ProductID varchar(512),
    ProductName varchar(512),
    Cost varchar(512),
    ShippingLocation varchar(512),
    SellerName varchar(512)
)

```

Step 10 : Load the data into that schema with the help of external stage :

```
Kousikdutta#COMPUTE_WH@MYFIRSTDATABASE.SALESSCHEMA>COPY INTO productnew
    FROM @my_s3_stage3;
+-----+-----+-----+-----+
| file | status | rows_parsed | rows_loaded | error_limit | error_r_line | first_error_character | first_error_column_name |
+-----+-----+-----+-----+
| s3://bucketproductnew/productkousik.csv | LOADED | 4 | 4 | 1 |
| NULL | NULL | NULL |
+-----+-----+-----+
1 Row(s) produced. Time Elapsed: 3.946s
Kousikdutta#COMPUTE_WH@MYFIRSTDATABASE.SALESSCHEMA>select * from productnew;
+-----+-----+-----+-----+
| PRODUCTID | PRODUCTNAME | COST | SHIPPINGLOCATION | SELLERNAME |
+-----+-----+-----+-----+
| 1 | LEDTV | 32990 | Delhi | ABC Pvt |
| 2 | Printer | 5990 | Delhi | ABC Pvt |
| 3 | Split AC | 32050 | Pune | XY Corp |
| 4 | Microwave | 12670 | Mumbai | PQ Corp |
+-----+-----+-----+-----+
4 Row(s) produced. Time Elapsed: 0.789s
Kousikdutta#COMPUTE_WH@MYFIRSTDATABASE.SALESSCHEMA>
```

Yes!!! We have received the data in snowflake.