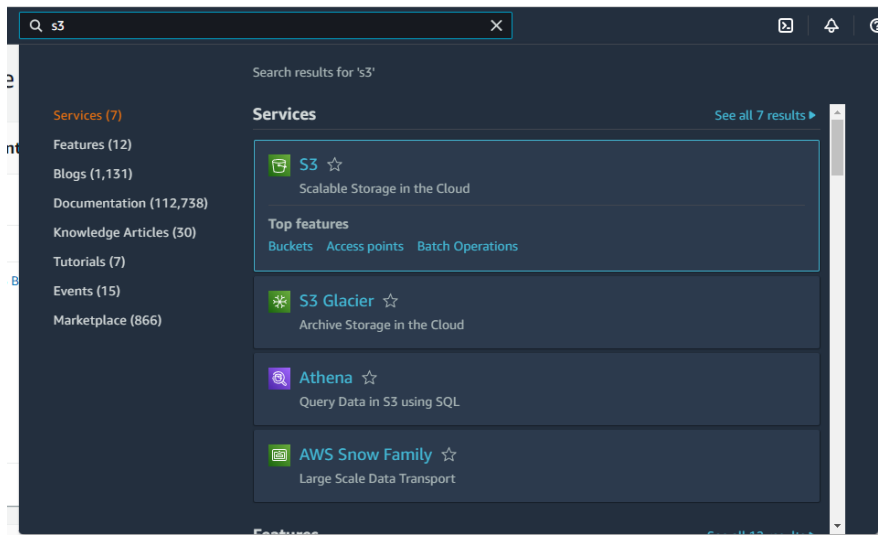


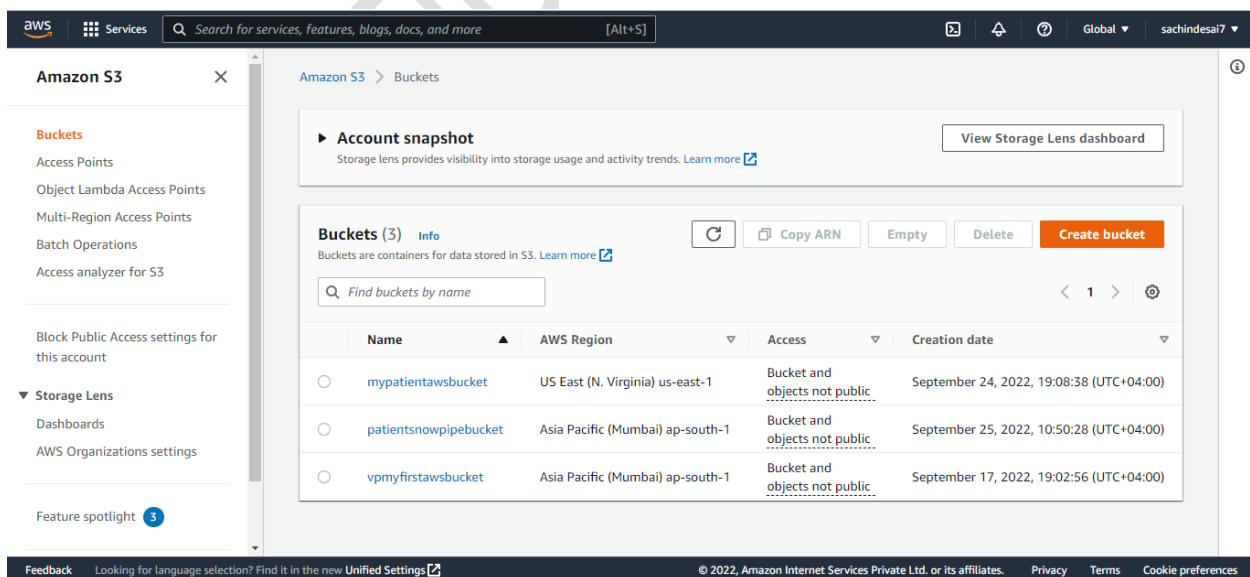


SNOWFLAKE CONTINUOUS DATA LOADING

- 1]. Create an AWS account in aws.amazon.com
- 2]. After successful account creation and activation, you can use the AWS service.
- 3]. Go to the Console home and search for S3 (Simple Storage Service) and click on it.



- 4]. Create S3 bucket





SNOWFLAKE CONTINUOUS DATA LOADING

5]. Create a folder inside the bucket (e.g. snowpipe)

Amazon S3 > Buckets > patientsnowpipebucket > Create folder

Create folder [Info](#)

Use folders to group objects in buckets. When you create a folder, S3 creates an object using the name that you specify followed by a slash (/). This object then appears as folder on the console. [Learn more](#)

ⓘ Your bucket policy might block folder creation

If your bucket policy prevents uploading objects without specific tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, you can use the [upload configuration](#) to upload an empty folder and specify the appropriate settings.

Folder

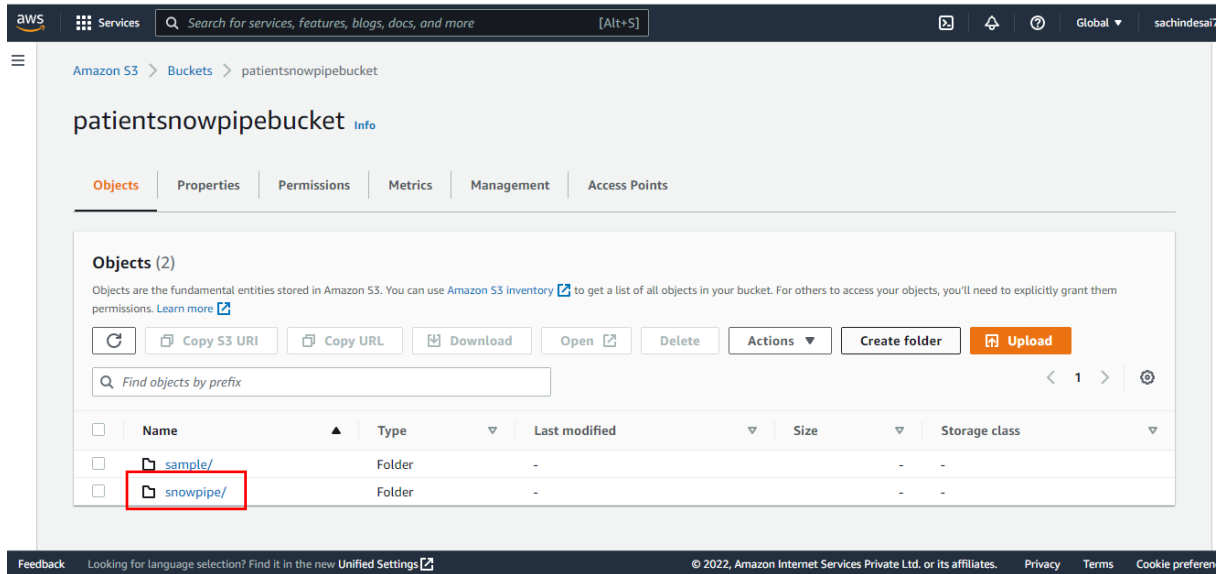
Folder name

 /

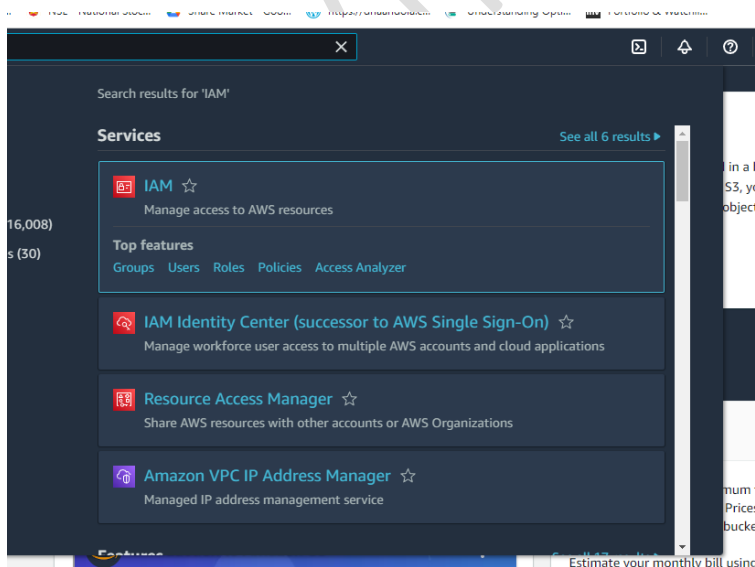
Folder names can't contain "/". See rules for naming [ⓘ](#)



SNOWFLAKE CONTINUOUS DATA LOADING



6]. Once the S3 bucket and folder are created, search and select the IAM (Identity and Access Management) service from the AWS console.





SNOWFLAKE CONTINUOUS DATA LOADING

7]. Click on the Policies from IAM Dashboard

The screenshot shows the AWS IAM dashboard. On the left, the 'Policies' link is highlighted in the 'Access management' section. The main dashboard area displays 'IAM dashboard' with a 'Security recommendations' section showing two alerts: 'Add MFA for root user' and 'Deactivate or delete access keys for root user'. Below this, the 'IAM resources' section shows counts for User groups (0), Users (1), Roles (4), Policies (4), and Identity providers (0). The right sidebar shows 'AWS Account' information and 'Quick Links'.

8]. Create IAM policy for the bucket by clicking on the “Create Policy” button

The screenshot shows the 'Policies (977)' page in the AWS IAM console. The 'Create policy' button is highlighted in the top right corner. Below the button, there is a search bar and a table listing existing policies. The table has columns for Policy name, Type, Used as, and Description.

Policy name	Type	Used as	Description
policy1	Customer managed	Permissions policy (1)	
snowflake_access_policy	Customer managed	None	allow snowflake
snowpipepolicyvp	Customer managed	Permissions policy (1)	list, read and wr
snowpipe_new_policy	Customer managed	Permissions policy (1)	
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read o
AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read o
AWSMarketplaceFullAccess	AWS managed	None	Provides the abi
AmazonS3OutpostsDataPolicy	AWS managed	None	Policy to enable



SNOWFLAKE CONTINUOUS DATA LOADING

9]. Click on the JSON tab and replace the existing text with the text given in the reference Document (<https://docs.snowflake.com/en/user-guide/data-load-snowpipe-auto-s3.html>).

After clicking on the above link you will get following doc then just copy the code.
(It is under the step no. 8 from the document)

The screenshot shows the Snowflake documentation page for automating Snowpipe for Amazon S3. The sidebar on the left lists various topics under 'Automating Snowpipe for Amazon S3', including 'Cloud Platform Support', 'Network Traffic', 'Configuring Secure Access to Cloud Storage', 'Determining the Correct Option', 'Option 1: Creating a New S3 Event Notification to Automate Snowpipe', 'Option 2: Configuring Amazon SNS to Automate Snowpipe Using SQS Notifications', 'SYSTEM\$PIPE_STATUS Output', 'Automating Snowpipe for Google Cloud Storage', 'Automating Snowpipe for Microsoft Azure Blob Storage', 'Calling Snowpipe REST Endpoints to Load Data', and 'Snowpipe Error Notifications'. The main content area shows steps 7 and 8. Step 7 is 'Click the JSON tab.' and step 8 is 'Add a policy document that will allow Snowflake to access the S3 bucket and folder.' Below step 8, there is a note about replacing placeholders and a JSON policy snippet.

7. Click the **JSON** tab.

8. Add a policy document that will allow Snowflake to access the S3 bucket and folder.

The following policy (in JSON format) provides Snowflake with the required permissions to load or unload data using a single bucket and folder path.

Copy and paste the text into the policy editor:

Note

- Make sure to replace `<bucket>` and `<prefix>` with your actual bucket name and folder path prefix.
- The Amazon Resource Names (ARN) for buckets in [government regions](#) have a `arn:aws-us-gov:s3:::` prefix.

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

Back to top

10]. Replace the `<bucket>` and `<prefix>` with your actual bucket name and folder path.

Also set the S3:prefix to `"*"`

```
"s3:prefix": [
  "*"
]
```



SNOWFLAKE CONTINUOUS DATA LOADING

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor JSON Import managed policy

```
10  },
11  },
12  {
13    "Effect": "Allow",
14    "Action": [
15      "s3:ListBucket",
16      "s3:GetBucketLocation"
17    ],
18    "Resource": "arn:aws:s3:::patientsnowpipebucket",
19    "Condition": {
```

Character count: 337 of 6,144. Cancel Next: Tags

11]. Click Next then skip the Add Tags. Enter the policy name Click Create Policy.

Your policy will get created.

12]. Create IAM Role. Click on Create Role

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report

Roles (4) Info

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.

Create role

Search

	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
<input type="checkbox"/>	role1	Account: 344274322414	17 hours ago
<input type="checkbox"/>	snowpipe_role1	Account: 344274322414	11 hours ago

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Manage

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

13]. Select AWS Account from Trusted Entity Type.

You will get your account number selected by default when you select AWS account.



SNOWFLAKE CONTINUOUS DATA LOADING

Step 2
Add permissions

Step 3
Name, review, and create

Trusted entity type

☐ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

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

☐ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account

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

☒ This account (184883492694)

☐ Another AWS account

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](#)

Feedback Looking for language selection? Find it in the new Unified Settings [\[?\]](#) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

14] Check Require external ID and enter 000 (as currently we are not having it) and click next

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

☒ This account (184883492694)

☐ Another AWS account

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

0000

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
Requires that the assuming entity use multi-factor authentication.

Cancel Next

Feedback Looking for language selection? Find it in the new Unified Settings [\[?\]](#) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

15]. On the next page, Select the IAM policy that you have created



SNOWFLAKE CONTINUOUS DATA LOADING

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions

Permissions policies (Selected 1/771)
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter.

	Policy name	Type	Description
<input type="checkbox"/>	policy1	Customer managed	
<input type="checkbox"/>	snowpipepolicyvp	Customer managed	list, read and write access
<input type="checkbox"/>	snowpipe_new_policy	Customer managed	
<input checked="" type="checkbox"/>	snowpipe_policy_VP	Customer managed	
<input type="checkbox"/>	AWSDirectConnect...	AWS managed	Provides read only access to AWS Direct Connect v...
<input type="checkbox"/>	AmazonGlacierRea...	AWS managed	Provides read only access to Amazon Glacier via th...
<input type="checkbox"/>	AWSMarketplaceFu...	AWS managed	Provides the ability to subscribe and unsubscribe to...

https://us-east-1.console.aws.amazon.com/iam/home#/policies/arn:aws:iam:1848... © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

16]. On the next page Enter any unique name to the role you are creating. The description is optional.

Click on the Create Role (Skip the Add Tags).

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

snowpipe_newuser_vp

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

Description

Add a short explanation for this role.

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

Step 1: Select trusted entities

17]. Click on the role that you have created. It will show you the summary page.



SNOWFLAKE CONTINUOUS DATA LOADING

The screenshot shows the AWS IAM console 'Roles' page. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Credential report. The main content area shows a list of roles. The role 'snowpipe_newuser_vp' is selected and highlighted with a red box. The table below shows the details of the selected role.

Role name	Trusted entities	Last activity
<input type="checkbox"/> AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/> AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
<input type="checkbox"/> role1	Account: 344274322414	17 hours ago
<input checked="" type="checkbox"/> snowpipe_newuser_vp	Account: 184883492694	-
<input type="checkbox"/> snowpipe_role1	Account: 344274322414	12 hours ago

You will get the following window

Note down the Role ARN, which we will need when we create the 'Storage Integration'.

The screenshot shows the AWS IAM console 'Summary' page for the role 'snowpipe_newuser_vp'. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Credential report. The main content area shows the role details. The ARN is highlighted with a red box.

ARN: `arn:aws:iam::184883492694:role/snowpipe_newuser_vp`

Link to switch roles in console: https://signin.aws.amazon.com/switchrole?roleName=snowpipe_newuser_vp&account=184883492694

Maximum session duration: 1 hour

18]. Login to the Snowflake Account.



SNOWFLAKE CONTINUOUS DATA LOADING

Create Cloud Storage Integration in Snowflake and map S3 user/role with it(STORAGE_AWS_ROLE_ARN).

```
CREATE OR REPLACE STORAGE INTEGRATION snowpipe_integration
```

```
TYPE = external_stage
```

```
STORAGE_PROVIDER = s3
```

```
STORAGE_AWS_ROLE_ARN = 'arn:aws:iam::184883492694:role/snowpipe_newuser_vp'
```

```
ENABLED = true
```

```
STORAGE_ALLOWED_LOCATIONS =
```

19]. In Snowflake worksheet run command


```
Desc integration integration_name;
```

e.g. desc integration snowpipe_integration;

And Note down the STORAGE_AWS_IAM_USER_ARN and STORAGE_AWS_EXTERNAL_ID from the result set

5	STORAGE_AWS_IAM_USER_ARN	String	arn:aws:iam::344274322414:user/eyn10000-s
7	STORAGE_AWS_EXTERNAL_ID	String	BR03385_SFCRole=2_4ZleqwTLkI5mYMphp6kTX3D9FKQ=

20]. Now go to the AWS Console

IAM  Role

Select the role you created

Click Trust Relationships -> Edit trust relationship

Replace the value of "AWS": with the AWS_IAM_USER_ARN String you got using DESC INTEGRATION command and, value of "sts:ExternalId": with AWS_EXTERNAL_ID String

Click Update Policy



SNOWFLAKE CONTINUOUS DATA LOADING

us-east-1.console.aws.amazon.com/iamv2/home#/roles/details/snowpipe_newuser_vp/edit-trust-policy

★ Bookmarks new nse Inbox - sachindesai... NSE - National Stoc... Share Market - Goo... https://dhaandola.c... Understanding Opti... Portfolio & Watchli... Other bookmarks

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global sachindesai7

IAM > Roles > snowpipe_newuser_vp > Edit trust policy

Edit trust policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::344274322414:user/eyn10000-s"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {
11        "StringEquals": {
12          "sts:ExternalId": "BR03385_SFCRole=2_4ZieqTLkISmYmhp6kTX3D9FKQ"
13        }
14      }
15    }
16  ]
17 }
```

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

21]. Create Snowflake file format. This file format will be used at the time of Stage creation.



SNOWFLAKE CONTINUOUS DATA LOADING

Create File Format

Name*

Schema Name

Format Type

Compression Method

Column separator

Row separator

Header lines to skip

Field optionally enclosed by

Null String

☐ Trim space before and after

[Show SQL](#)

22]. Create a stage in snowflake pointing to your S3 bucket:

```
CREATE OR REPLACE STAGE patient_snowpipe_stage
```

```
STORAGE_INTEGRATION = snowpipe_integration
```

```
URL = 's3://patientsnowpipebucket/snowpipe' -- (Name of your bucket and folder)
```

```
FILE_FORMAT = (format_name = 'CSV_FORMAT');
```

23]. Now Create auto-ingest pipe.

```
CREATE OR REPLACE PIPE patient_snowpipe
```

```
AUTO_INGEST = TRUE
```

```
AS COPY INTO tab_patient -- (table name that you created in snowflake)
```

```
FROM @patient_snowpipe_stage -- (name of the stage)
```



SNOWFLAKE CONTINUOUS DATA LOADING

```
FILE_FORMAT = ( FORMAT_NAME = 'CSV_FORMAT');
```

24]. After creating snowpipe, get 'Notification Channel' value

Run command

Show pipes;

name	database_name	schema_name	definition	owner	notification_channel
DEMO1_SNOWPIPE	VP_DEMODA...	PUBLIC	COPY INTO ...	ACCOUNTA...	arn:aws:sqs:ap-south-1:344274322414:sf-snowpipe-AIDAVAKCZIPXGQXWUHIMU-M-ASvZXErhxxGpKYm5xGMA
PATIENT_SNOWPIPE	VP_DEMODA...	PUBLIC	copy into ta...	ACCOUNTA...	arn:aws:sqs:ap-south-1:344274322414:sf-snowpipe-AIDAVAKCZIPXGQXWUHIMU-M-ASvZXErhxxGpKYm5xGMA

Or Go to Database [Pipes](#)

Here also you will get the notification channel value.

Databases > VP_DEMODATABASE

TablesViewsSchemasStagesFile FormatsSequencesPipes

+

Create

✕

Drop

↗

Transfer Ownership

Search Pipes

Pipe Name	Schema	↓ Creation Time	Owner	Notification Channel	Comment
PATIENT_SNOWPIPE	PUBLIC	9/25/2022, 11:20:31...	ACCOUNTADMIN	arn:aws:sqs:ap-south-1:344274322414:sf-snow...	
DEMO1_SNOWPIPE	PUBLIC	9/25/2022, 5:34:16 ...	ACCOUNTADMIN	arn:aws:sqs:ap-south-1:344274322414:sf-snow...	

25]. This is the final step. Create an event on S3 bucket. Go to your S3 bucket that you have created. Click on Properties tab and scroll down to

Event Notification -> Click Create Event Notification

Enter any name for the Notification.



SNOWFLAKE CONTINUOUS DATA LOADING

Amazon S3 > Buckets > patientsnowpipebucket > Create event notification

Create event notification [Info](#)

To enable notifications, you must first add a notification configuration that identifies the events you want Amazon S3 to publish and the destinations where you want Amazon S3 to send the notifications.

General configuration

Event name

Event name can contain up to 255 characters.

Prefix - optional

Limit the notifications to objects with key starting with specified characters.

Suffix - optional

Limit the notifications to objects with key ending with specified characters.

Check All Object create Events

Event types

Specify at least one event for which you want to receive notifications. For each group, you can choose an event type for all events, or you can choose one or more individual events.

Object creation

☒ All object create events
s3:ObjectCreated:*

☐ Put
s3:ObjectCreated:Put

☐ Post
s3:ObjectCreated:Post



Scroll down to Destination

Select SQS Queue [?](#) Select Enter SQS Queue ARN [?](#) And paste that 'Notification Channel' under SQS Queue




SNOWFLAKE CONTINUOUS DATA LOADING

Destination

 Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. [Learn more](#) 

Destination

Choose a destination to publish the event. [Learn more](#) 

- ☐ Lambda function
Run a Lambda function script based on S3 events.
- ☐ SNS topic
Fanout messages to systems for parallel processing or directly to people.
- ☒ SQS queue
Send notifications to an SQS queue to be read by a server.

Specify SQS queue

- ☐ Choose from your SQS queues
- ☒ Enter SQS queue ARN

SQS queue

arn:aws:sqs:ap-south-1:344274322414:sf-snowpipe-AIDAVAKCZIPXGQXWUHIMU-M-A

Now you are ready to load the file to s3 bucket.

26]. Following are some snowpipe command which will help you to check snowpipe status

```
select SYSTEM$PIPE_STATUS('patient_snowpipe');
```

```
select * from table(information_schema.copy_history(table_name=>'tab_patient', start_time=>
dateadd(hours, -1, current_timestamp())));
```

CODE PART :

```
CREATE OR REPLACE DATABASE AWS_DATABASE;
```

```
USE AWS_DATABASE;
```

```
CREATE OR REPLACE TABLE RETAIL_TXNS LIKE AZUREDATABSE.PUBLIC.TRANSACTION_RAW;
```



SNOWFLAKE CONTINUOUS DATA LOADING

create or replace file format AWS_RETAIL_TXNS_CSV LIKE
AZUREDATABASE.PUBLIC.RETAIL_TRNXS_CSV;

-----AWS (S3) INTEGRATION-----

CREATE OR REPLACE STORAGE integration RETAIL_TXNS_S3_AWS_INT
TYPE = EXTERNAL_STAGE
STORAGE_PROVIDER = S3
ENABLED = TRUE
STORAGE_AWS_ROLE_ARN ='arn:aws:iam::441615131317:role/retail_txns_access_role'
STORAGE_ALLOWED_LOCATIONS =('s3://retailraw/');

DESC integration RETAIL_TXNS_S3_AWS_INT;

CREATE OR REPLACE STAGE RETAIL_TXNS_STG
URL ='s3://retailraw'
file_format = AWS_RETAIL_TXNS_CSV
storage_integration = RETAIL_TXNS_S3_AWS_INT;

SHOW STAGES;
LIST @RETAIL_TXNS_STG;

--CREATE SNOWPIPE THAT RECOGNISES CSV THAT ARE INGESTED FROM EXTERNAL STAGE AND COPIES
THE DATA INTO EXISTING TABLE

--The AUTO_INGEST=true parameter specifies to read

--- event notifications sent from an S3 bucket to an SQS queue when new data is ready to load.



SNOWFLAKE CONTINUOUS DATA LOADING

```
CREATE OR REPLACE PIPE RETAIL_SNOWPIPE_TRANSACTION AUTO_INGEST = TRUE AS
COPY INTO AWS_DATABASE.PUBLIC.RETAIL_TXNS
FROM '@RETAIL_TXNS_STG/TRANSACTION/'
FILE_FORMAT = CSV;
SHOW PIPES;
```

```
ALTER PIPE RETAIL_SNOWPIPE_TRANSACTION REFRESH;
select *
from table(information_schema.copy_history (table_name=> 'RETAIL_TXNS',
start_time=> dateadd (hours, -1, current_timestamp())));
```

```
SELECT COUNT(*) FROM RETAIL_TXNS;
SELECT * FROM RETAIL_TXNS;
```