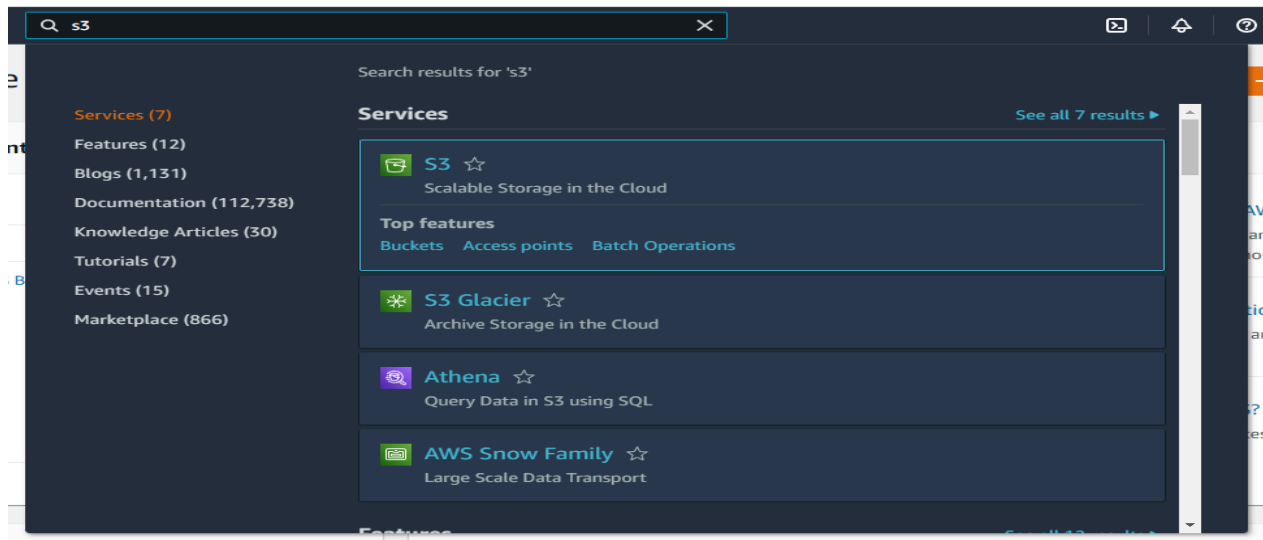
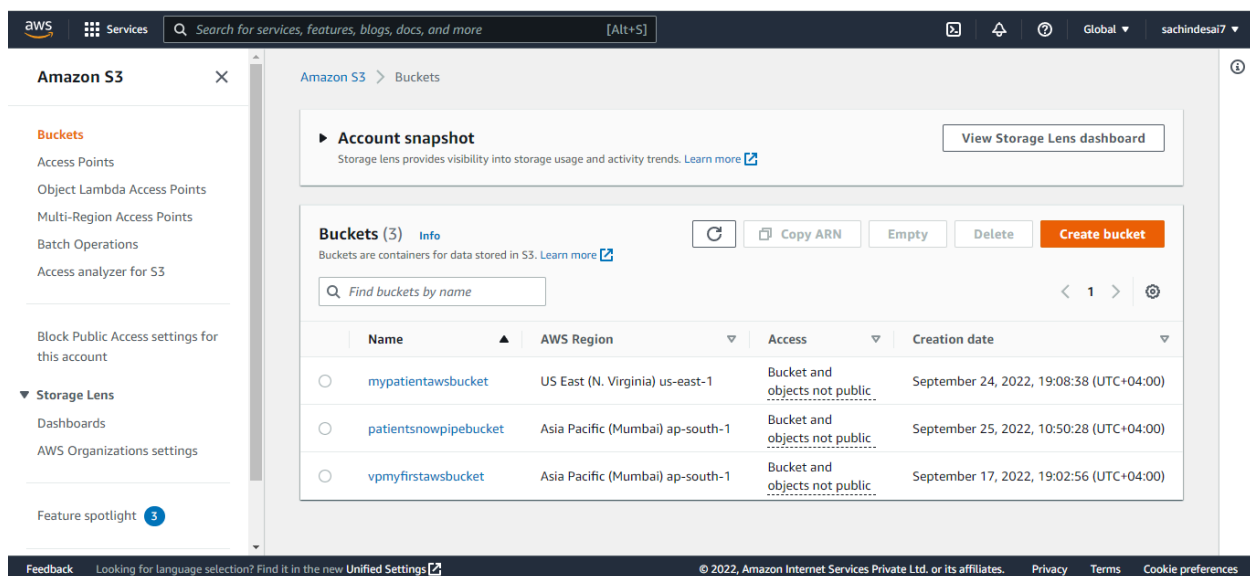


## SNOWFLAKE CONTINUOUS DATA LOADING

- 1]. Create an AWS account in [aws.amazon.com](https://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



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

snowpipe /

Folder names can't contain "/". See rules for naming

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

Amazon S3 > Buckets > patientsnowpipebucket

## patientsnowpipebucket [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

### Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

☐

Name

▲

Type

▼

Last modified

▼

Size

▼

Storage class

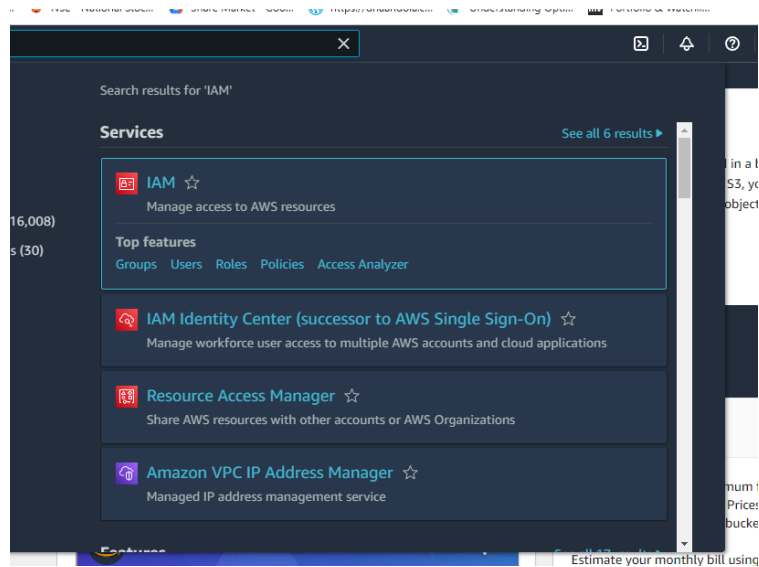
▼

<input type="checkbox"/>	sample/		Folder	-		-	-
<input type="checkbox"/>	snowpipe/		Folder	-		-	-

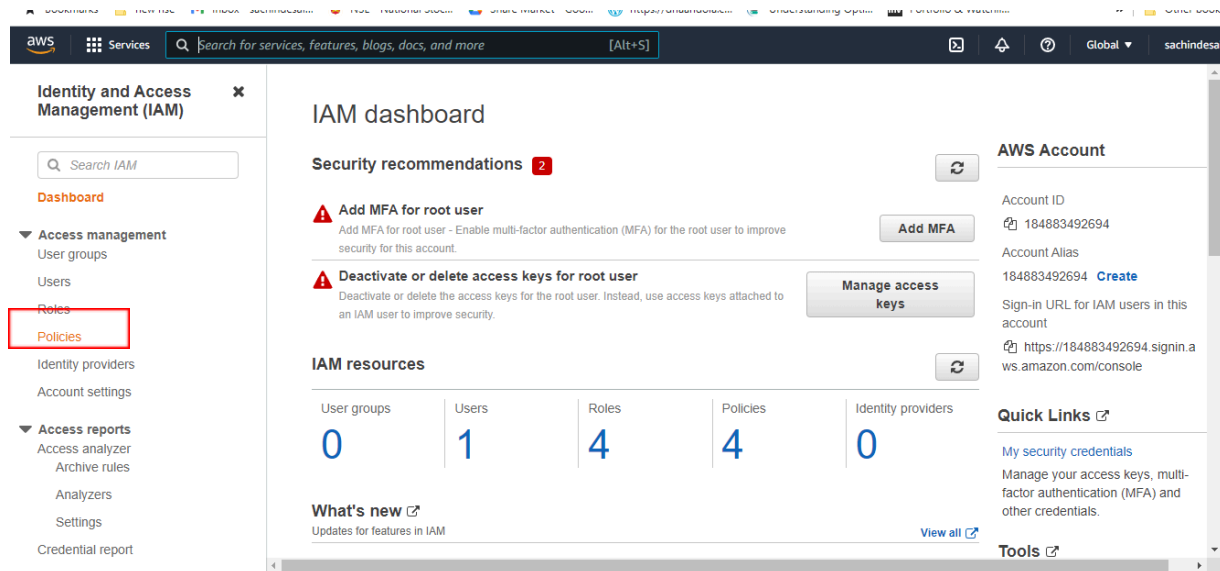
Feedback Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

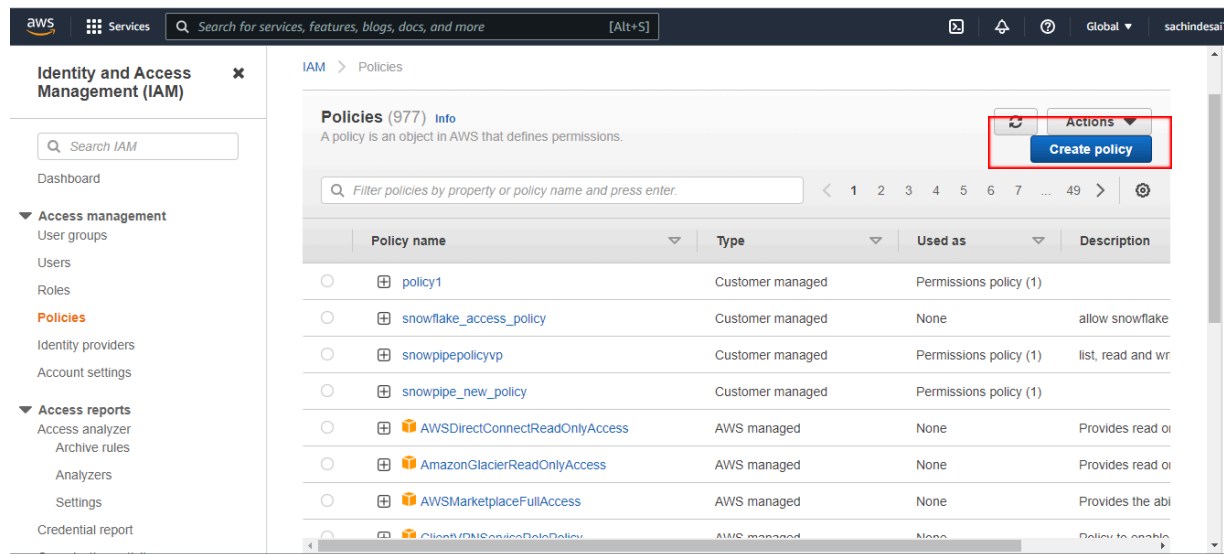
6]. Once the S3 bucket and folder are created, search and select the IAM (Identity and Access Management) service from the AWS console.



7]. Click on the Policies from IAM Dashboard



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

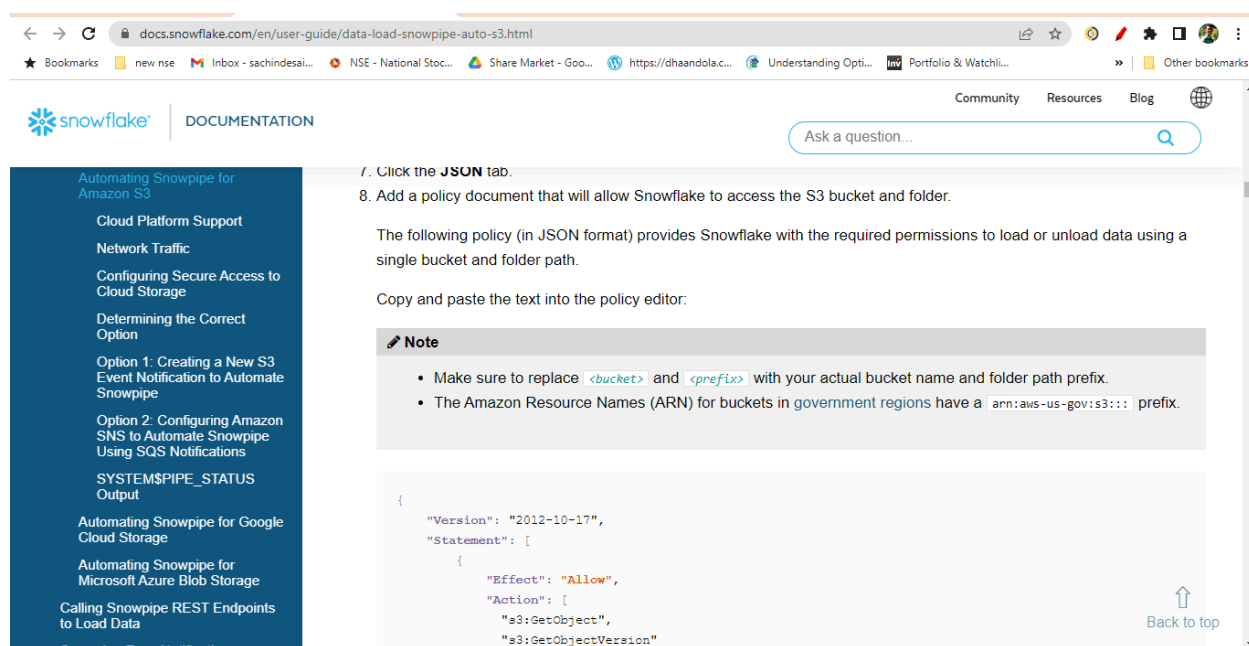


9]. Click on the JSON tab and replace the existing text with the text given in the reference

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)



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

Also set the S3:prefix to “\*”

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

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

```
8
9
10
11
12
13
14
15
16
17
18
19
s3:GetObjectVersion
},
"Resource": "arn:aws:s3:::patientsnowpipebucket/snowpipe/*"
},
{
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketLocation"
  ],
  "Resource": "arn:aws:s3:::patientsnowpipebucket",
  "Condition": {
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

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

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

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

IAM > Roles

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

<input type="checkbox"/>	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.

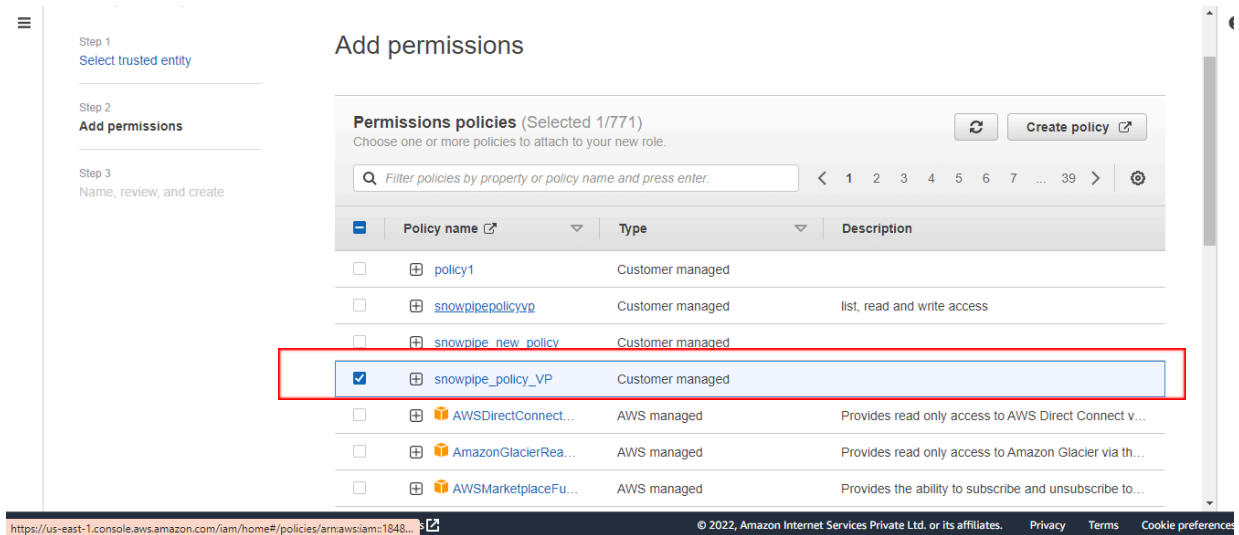
You will get your account number selected by default when you select AWS account.

The screenshot shows the 'Trusted entity type' step in the AWS IAM console. The left sidebar indicates 'Step 2: Add permissions' and 'Step 3: Name, review, and create'. The main content area has five radio button options: 'AWS service', 'AWS account' (selected), 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. Below these, the 'An AWS account' section shows 'This account (184883492694)' selected. Under 'Options', 'Require external ID' is checked. A footer bar contains 'Feedback', a language selection link, copyright information, and links for 'Privacy', 'Terms', and 'Cookie preferences'.

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

This screenshot shows the 'Require external ID' step. The 'This account (184883492694)' option remains selected. The 'Require external ID' checkbox is checked, and the 'External ID' text box now contains '0000'. An information box states that the console does not support external IDs with the Switch Role feature. The 'Require MFA' checkbox is unchecked. At the bottom right, there are 'Cancel' and 'Next' buttons. The footer bar is identical to the previous screenshot.

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



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.

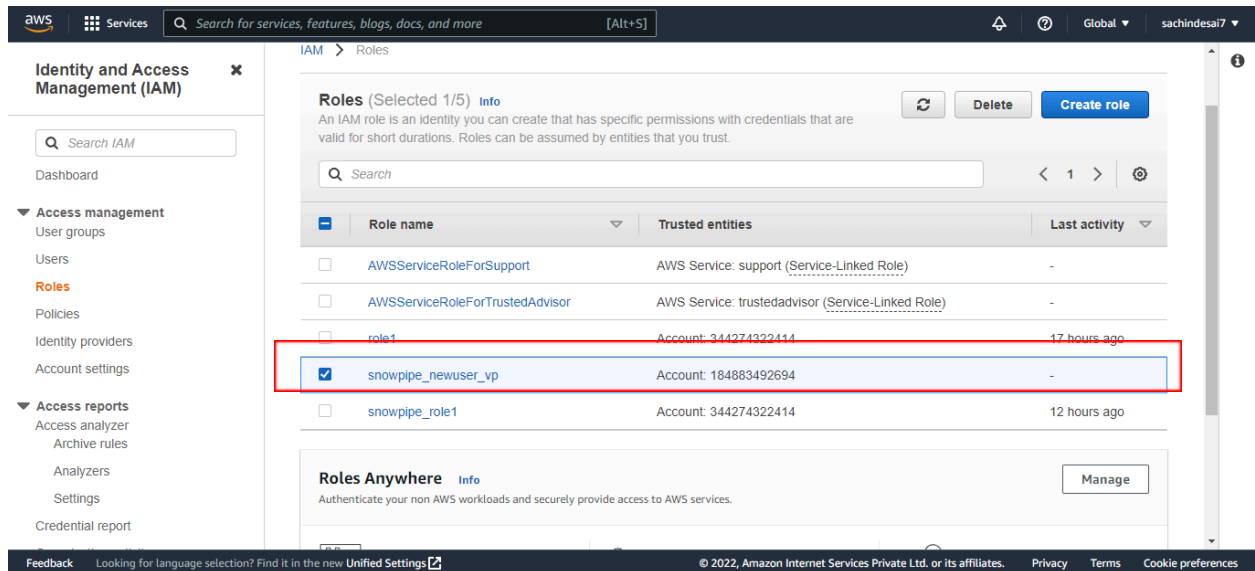
#### Description

Add a short explanation for this role.

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

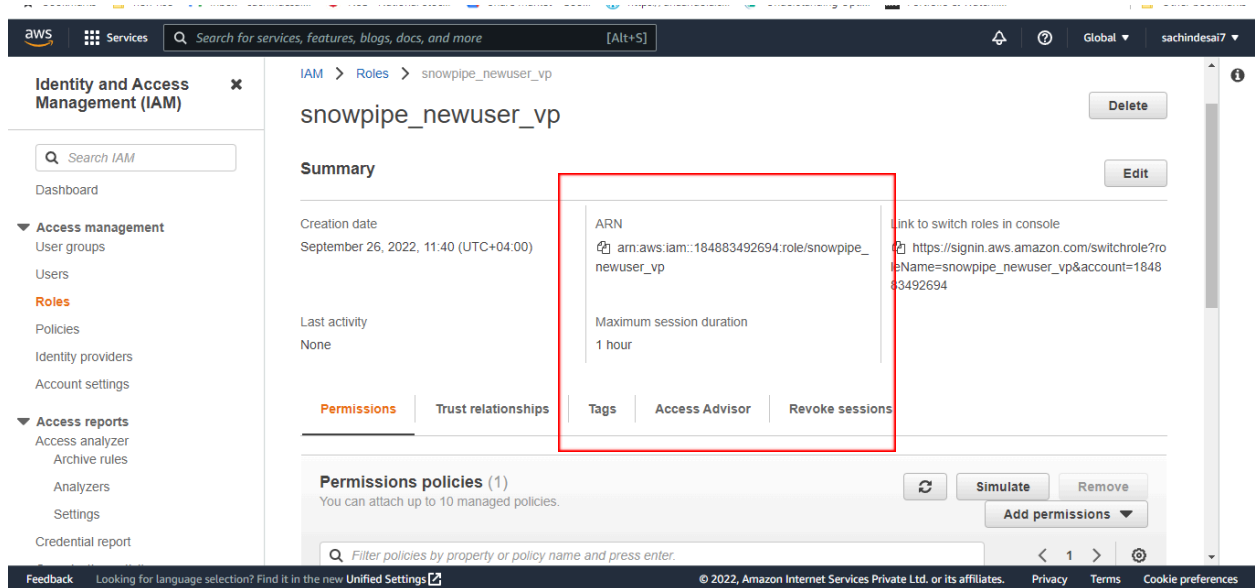
### Step 1: Select trusted entities

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



You will get the following window

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



18]. Login to the Snowflake Account.

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_4ZleqwTLkl5mYMphp6kTX3D9FKQ=

20]. Now go to the AWS Console

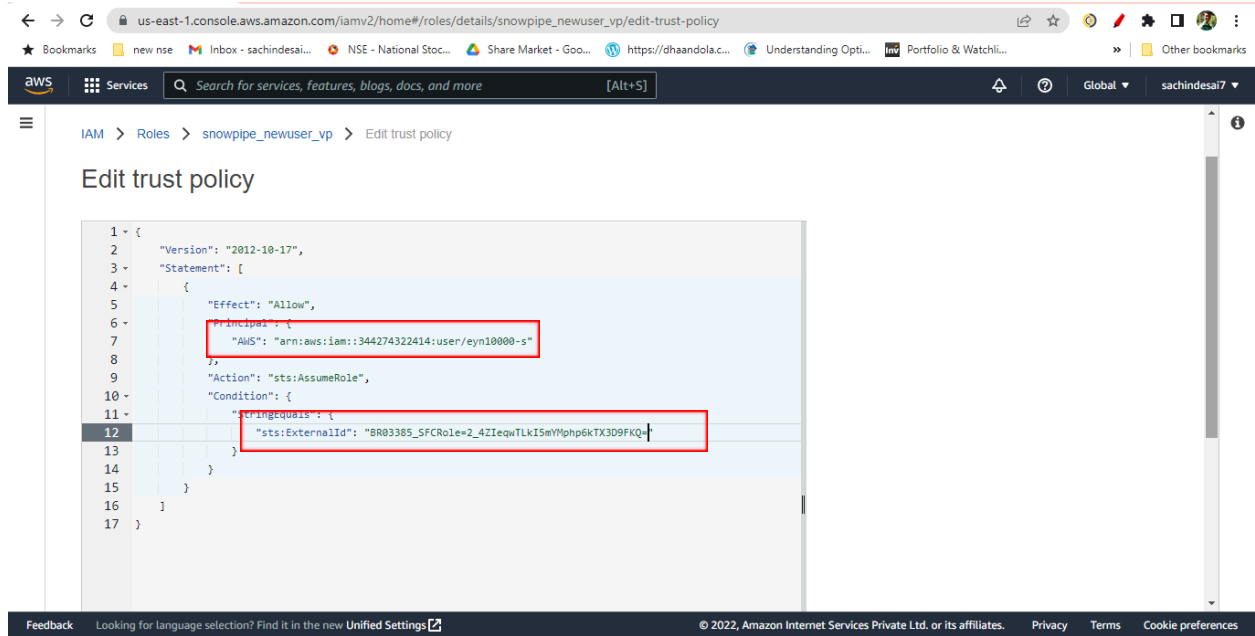
IAM  Role

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



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

### Create File Format

Name\* CSV\_FORMAT

Schema Name PUBLIC

Format Type CSV

Compression Method Auto

Column separator Comma

Row separator New Line

Header lines to skip 0

Field optionally enclosed by None

Null String \\N

☐ Trim space before and after

Show SQL Cancel Finish

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)

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						
Tables Views Schemas Stages File Formats Sequences Pipes						
 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.

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

## 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())));
```