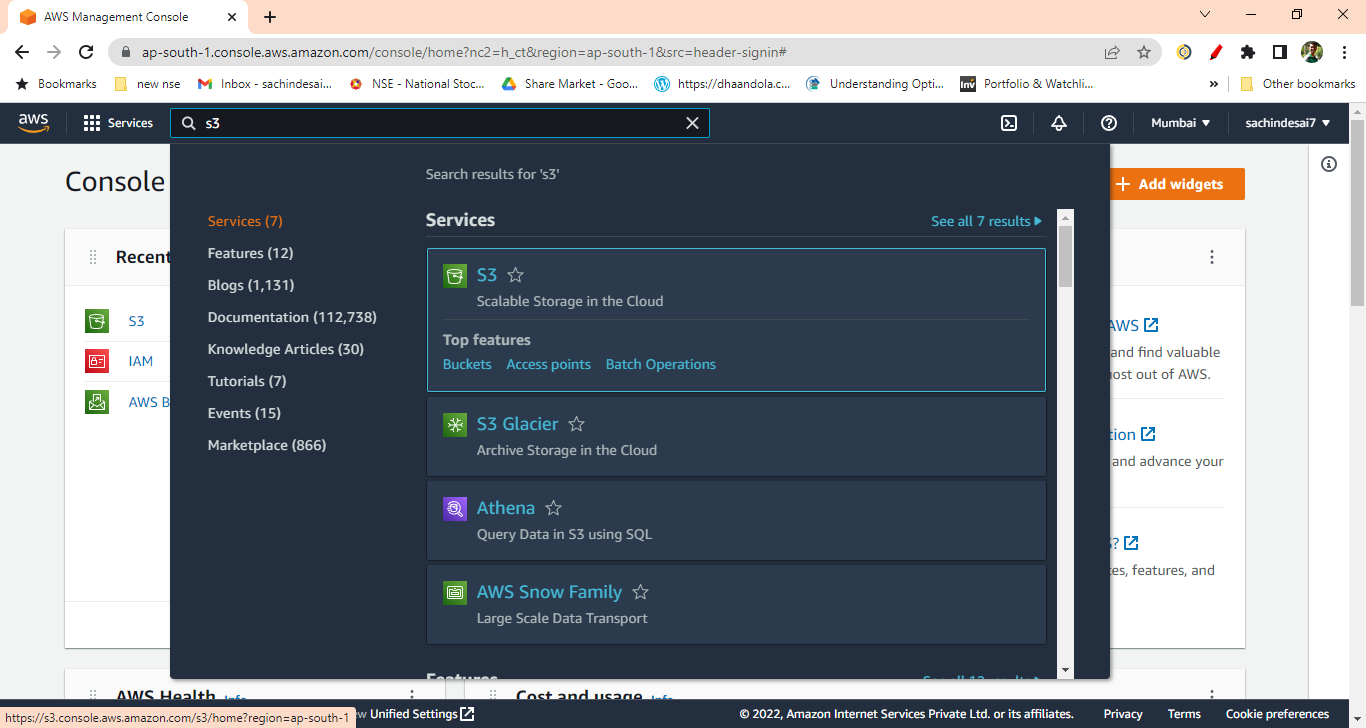
**SNOWFLAKE CONTINUOUS DATA LOADING**

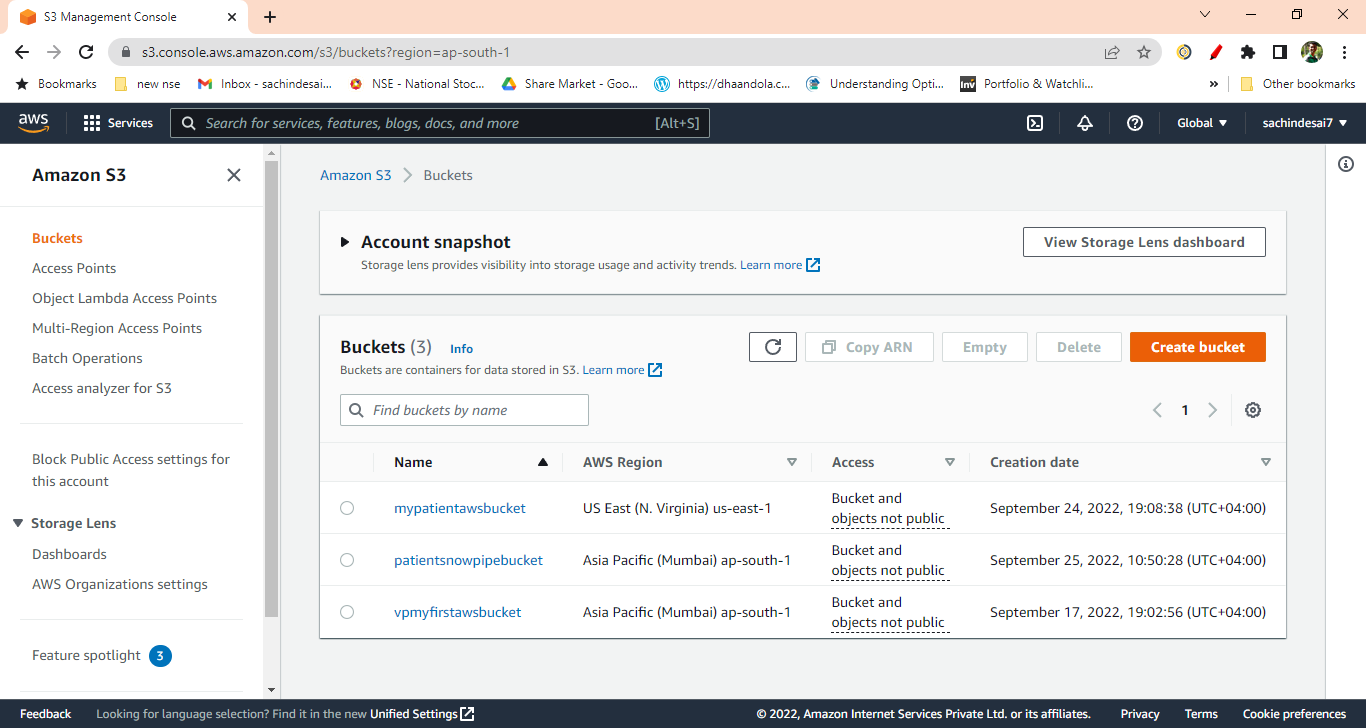
1]. Create an AWS account in aws.amazon.com

2]. After successful account creation and activation, you can use the AWS service.

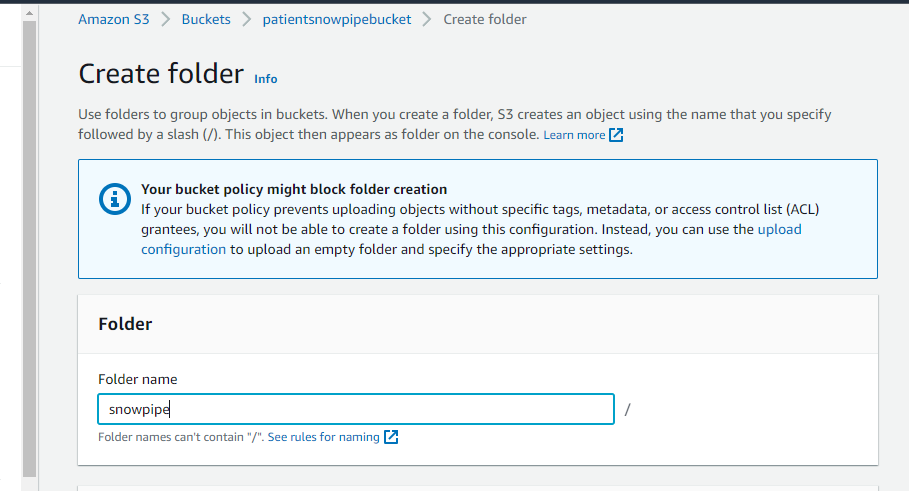
3]. Go to the Console home and search for S3 (Simple Storage Service) and click on it.

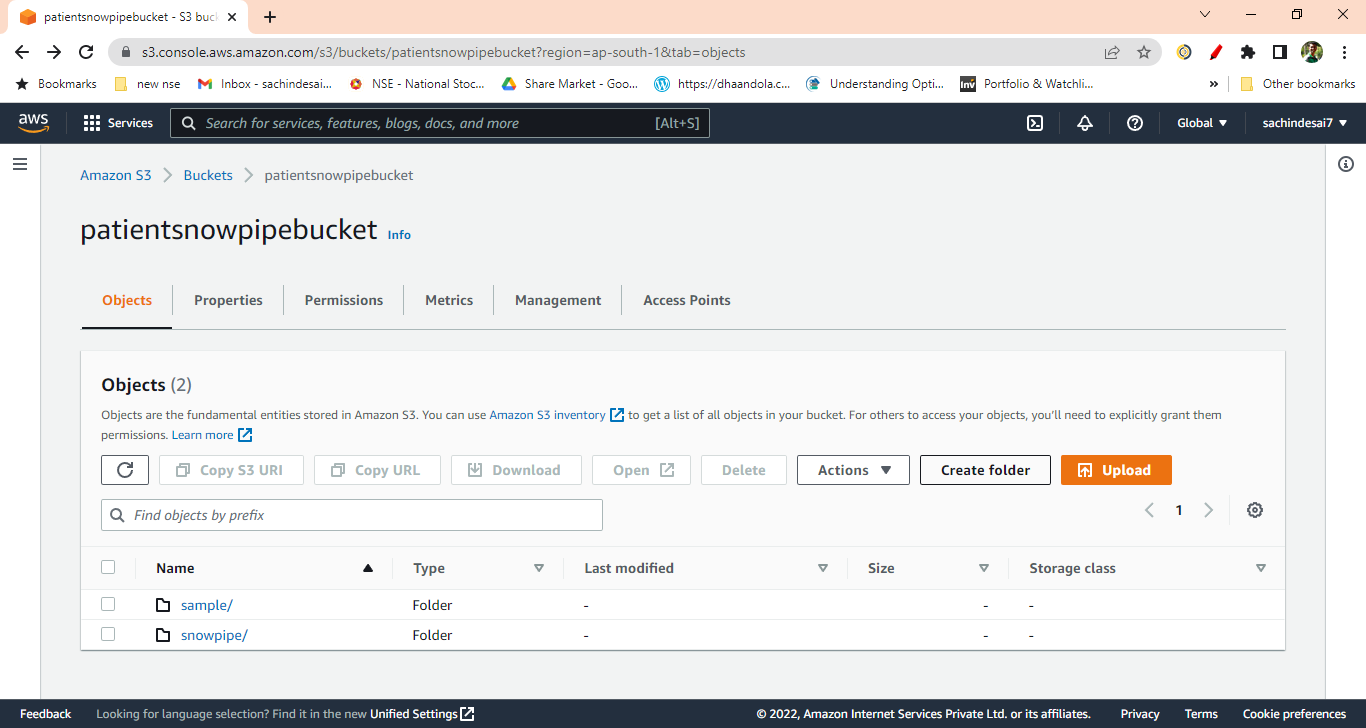


4]. Create S3 bucket

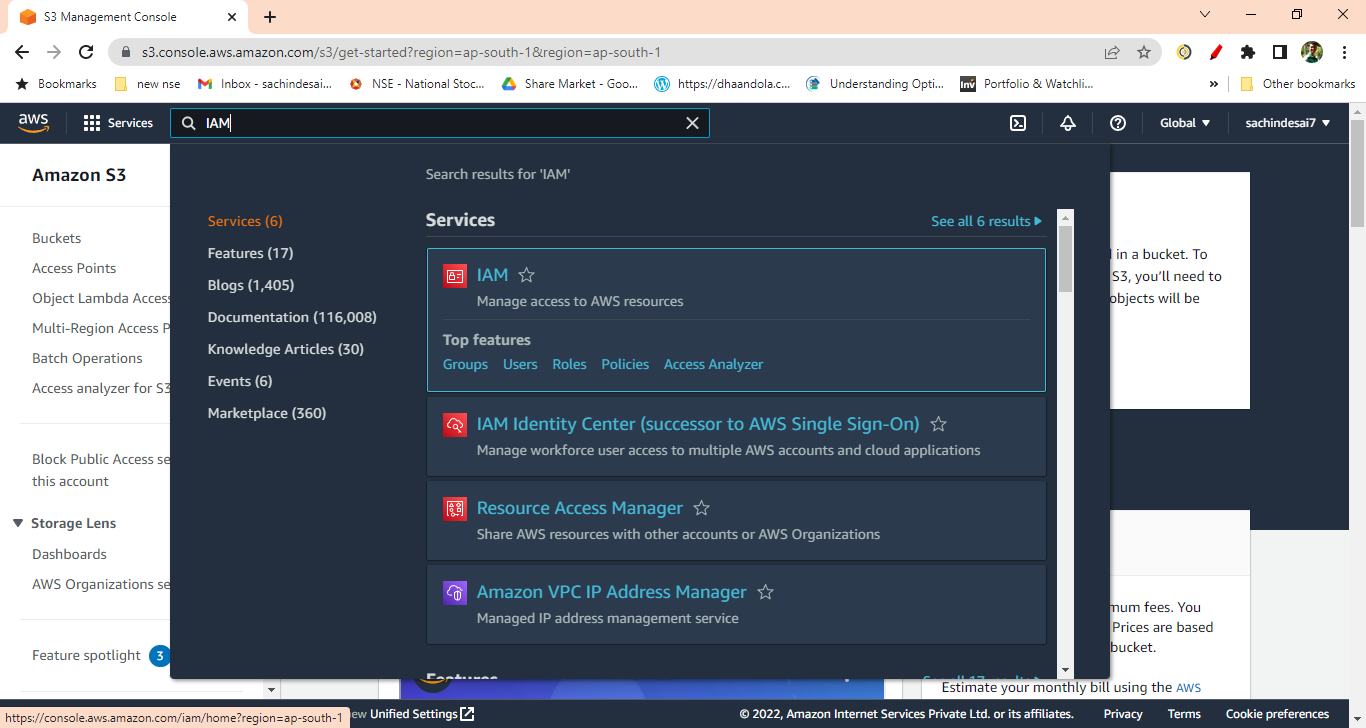


5]. Create a folder inside the bucket ( e.g. snowpipe)

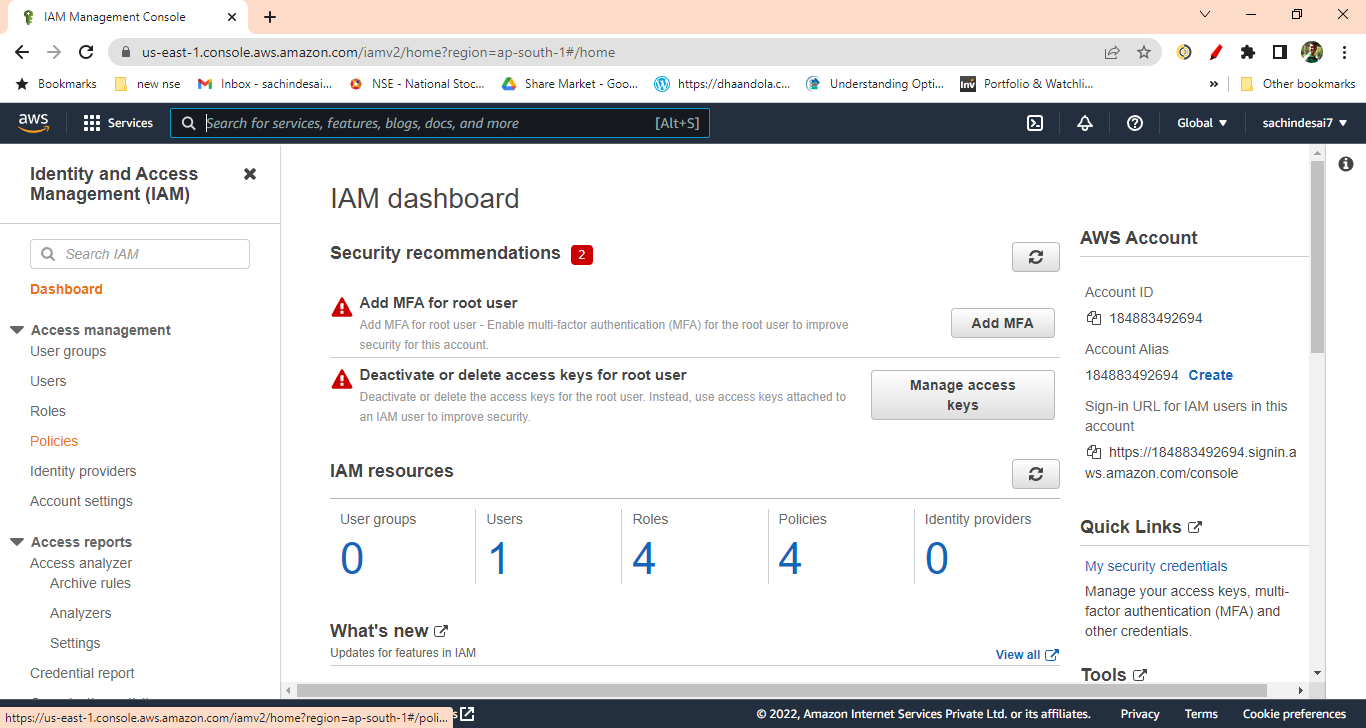




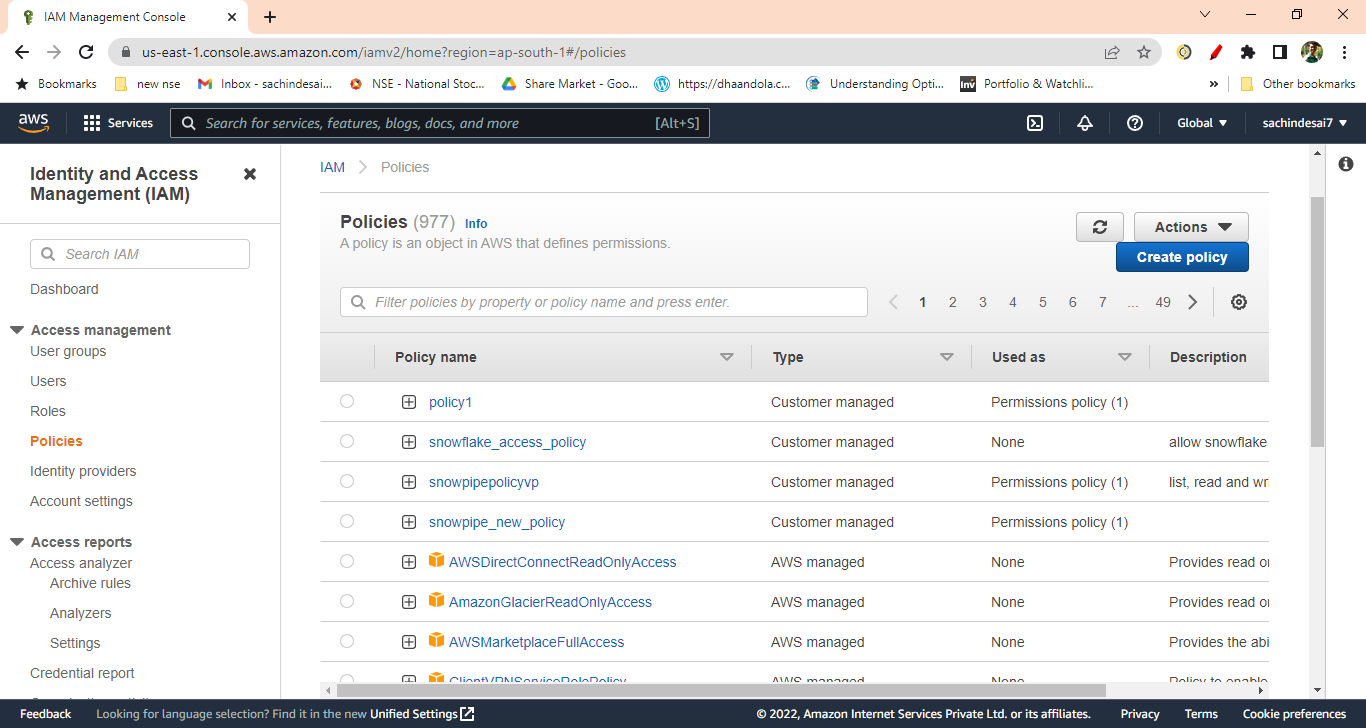
6]. Once the S3 bucket and folder are created, search and select the IAM (Identity and Access Management) service from the AWS console.



7]. Click on the Policies from IAM Dashboard



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

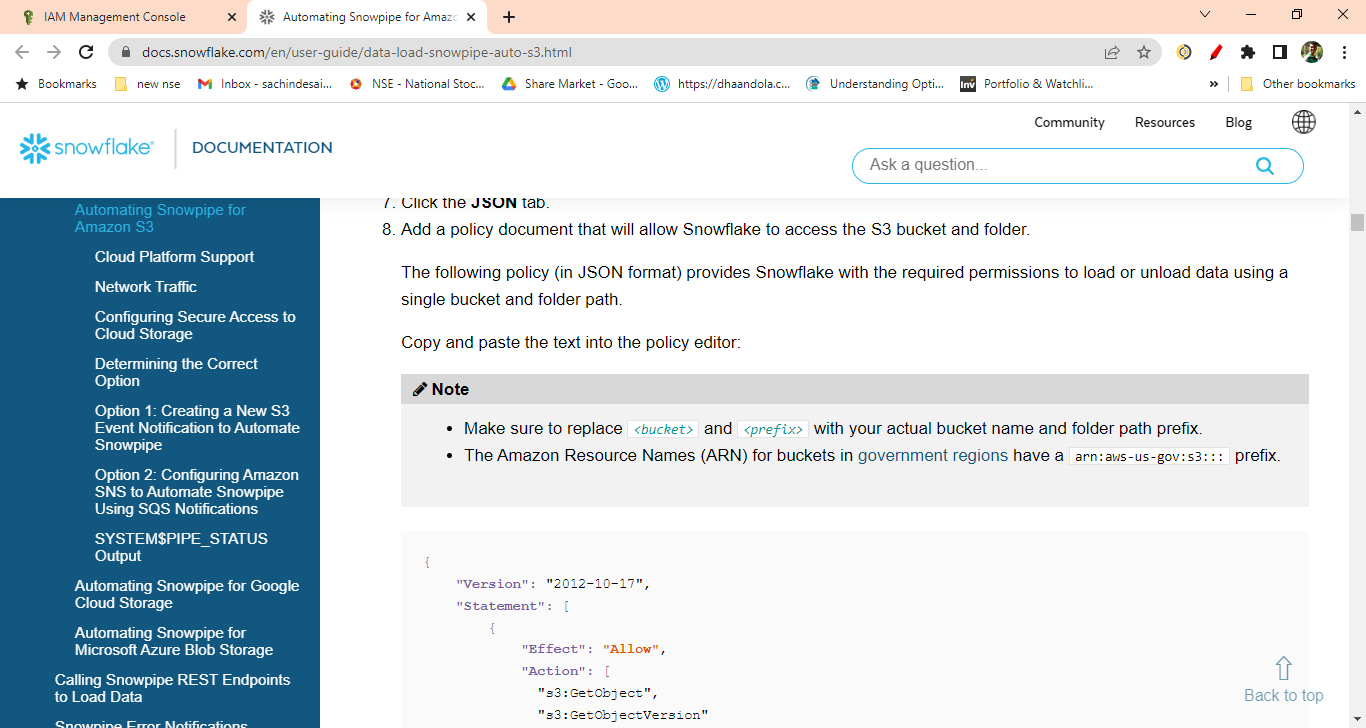


9]. Click on the JSON tab and replace the existing text with the text given in the reference

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)

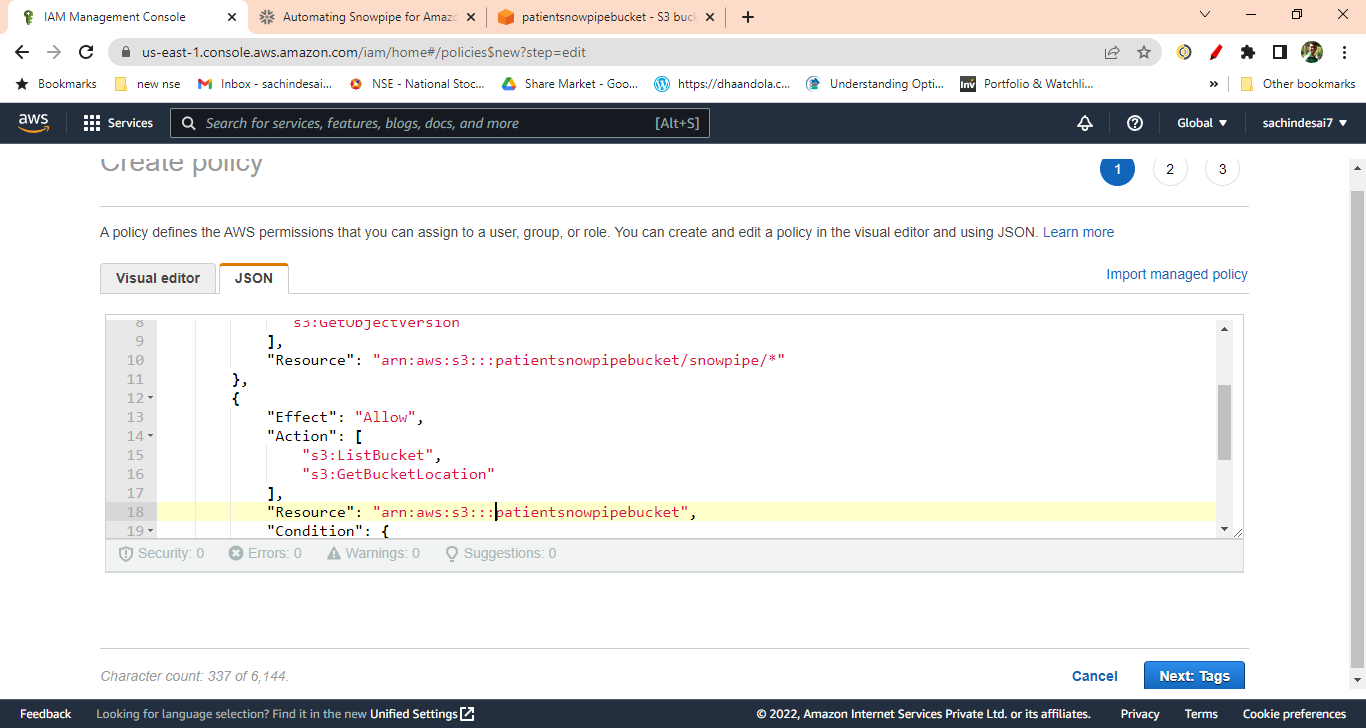


10]. Replace the <bucket> and <prefix> with your actual bucket name and folder path.

Also set the S3:prefix to “ \*”

"s3:prefix":[

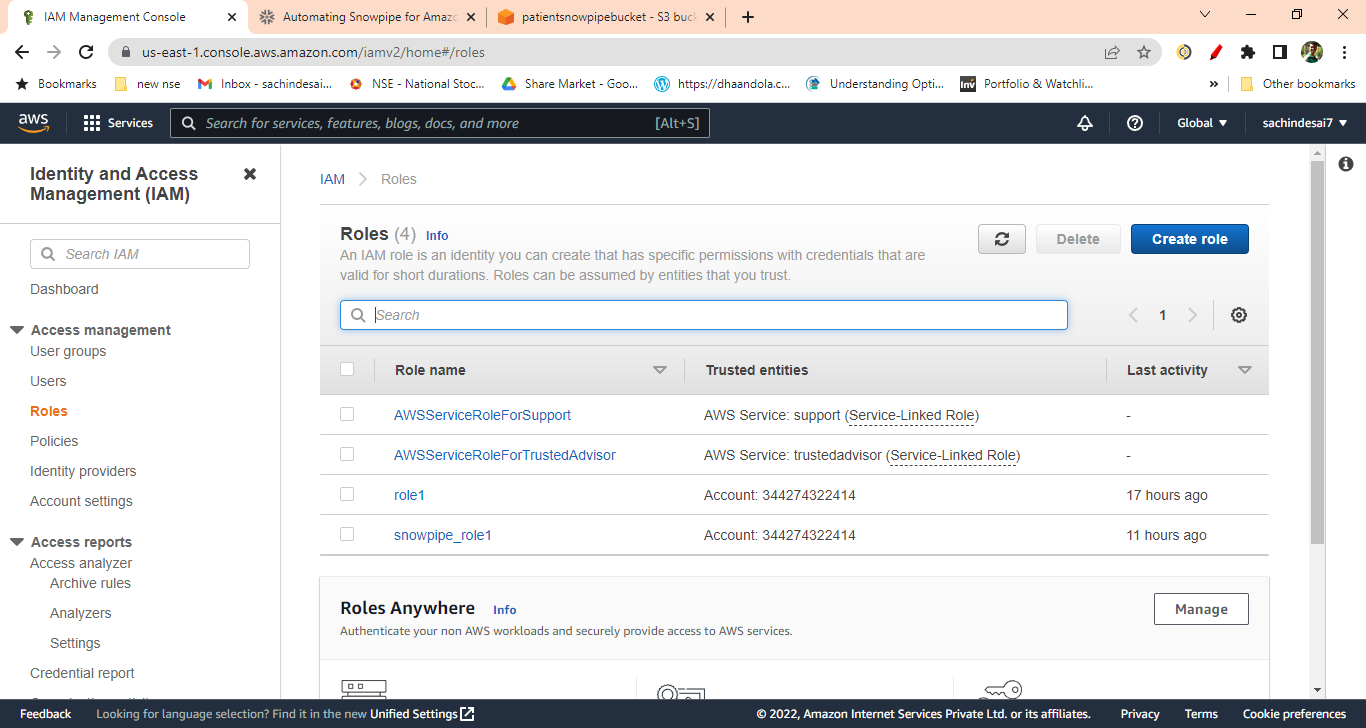
“\*"



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

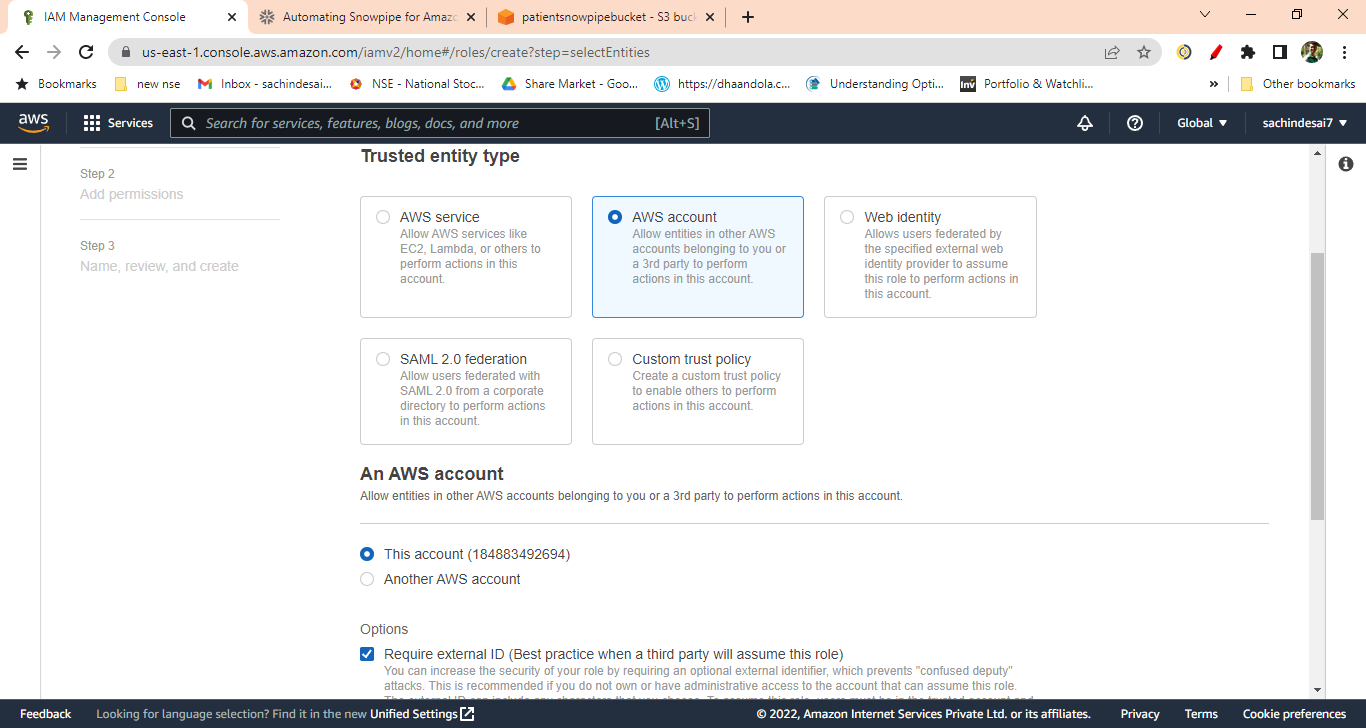
Your policy will get created.

12]. Create IAM Role. Click on Create Role

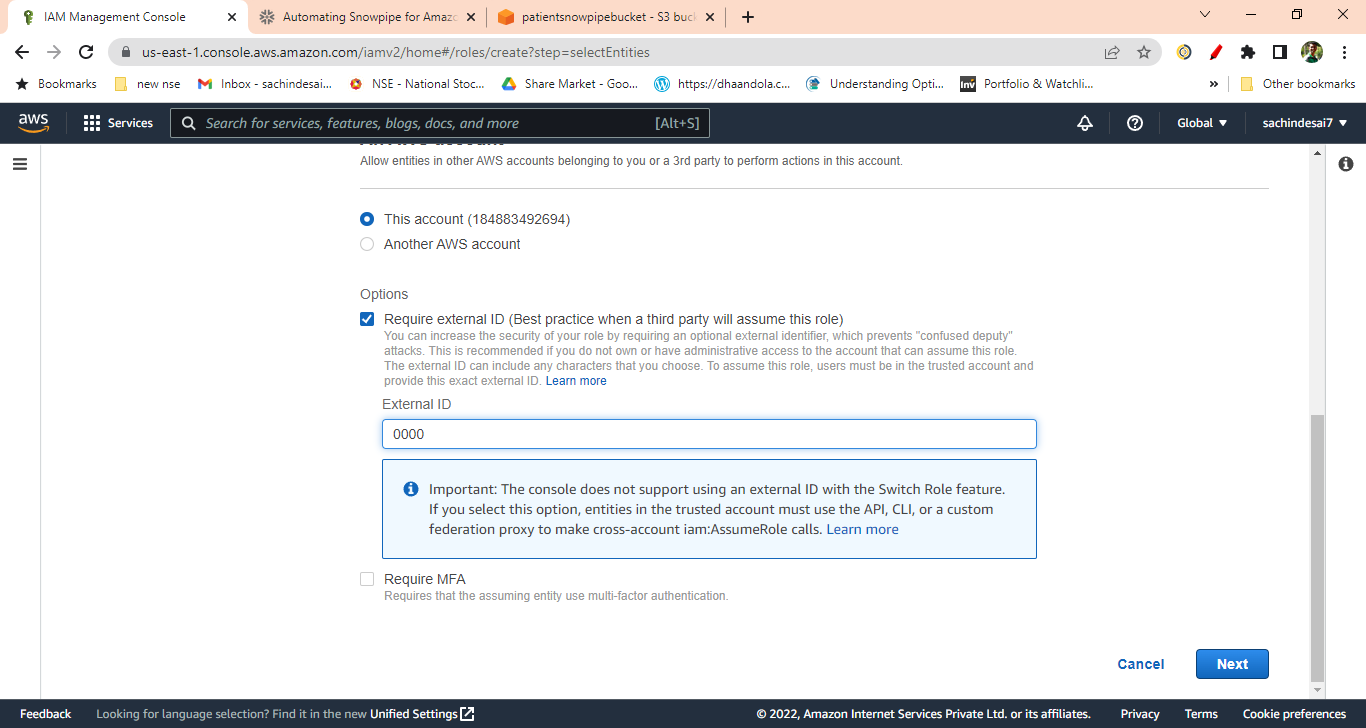


13]. Select AWS Account from Trusted Entity Type.

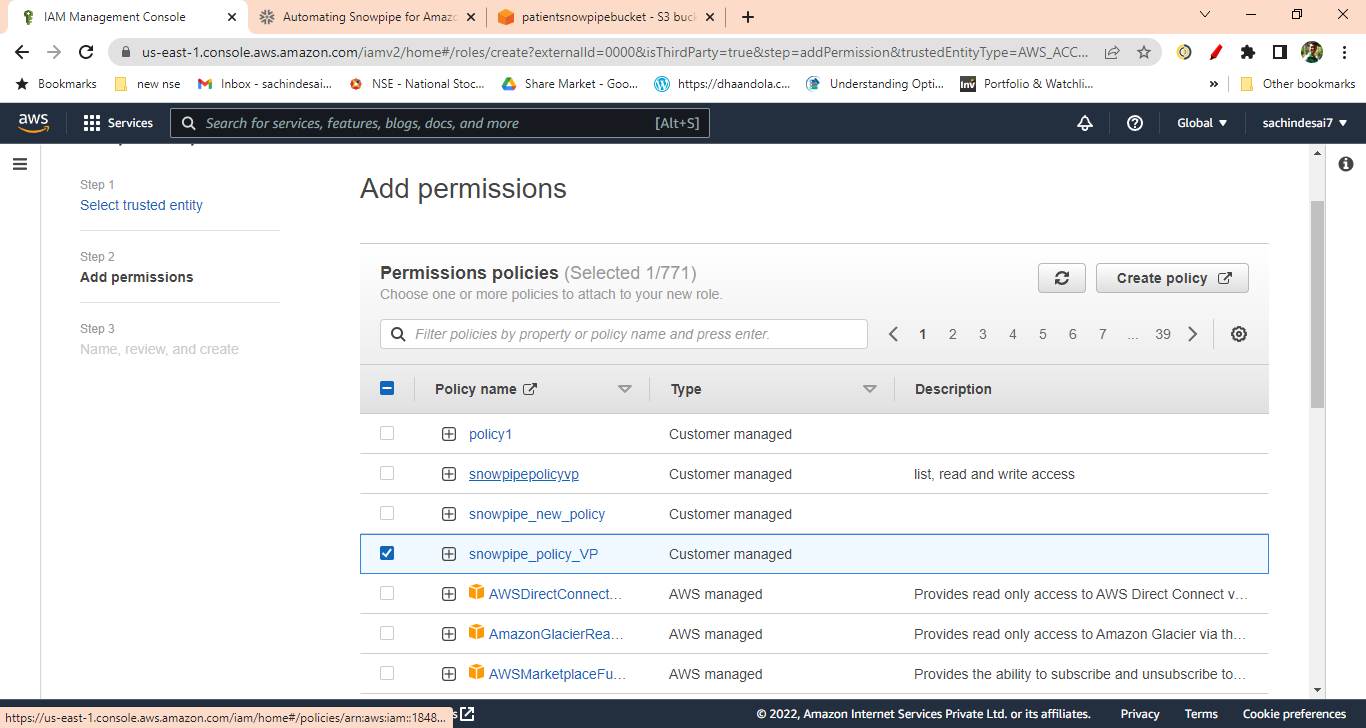
You will get your account number selected by default when you select AWS account.



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

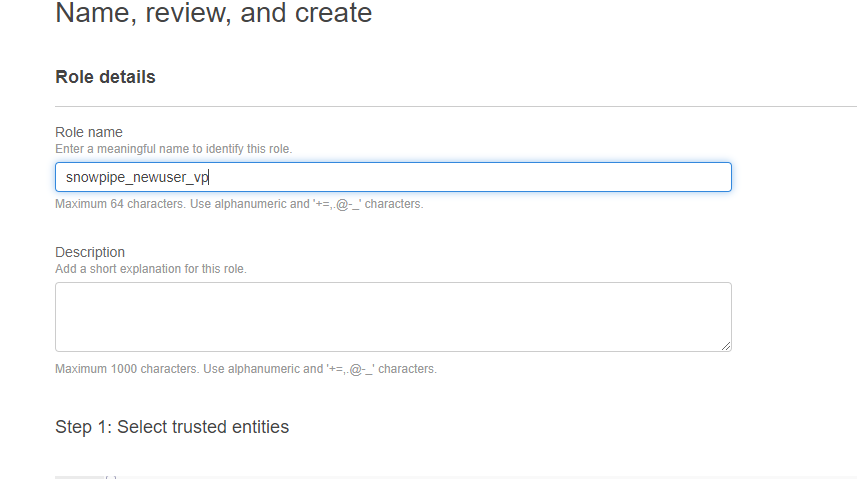


15]. On the next page, Select the IAM policy that you have created

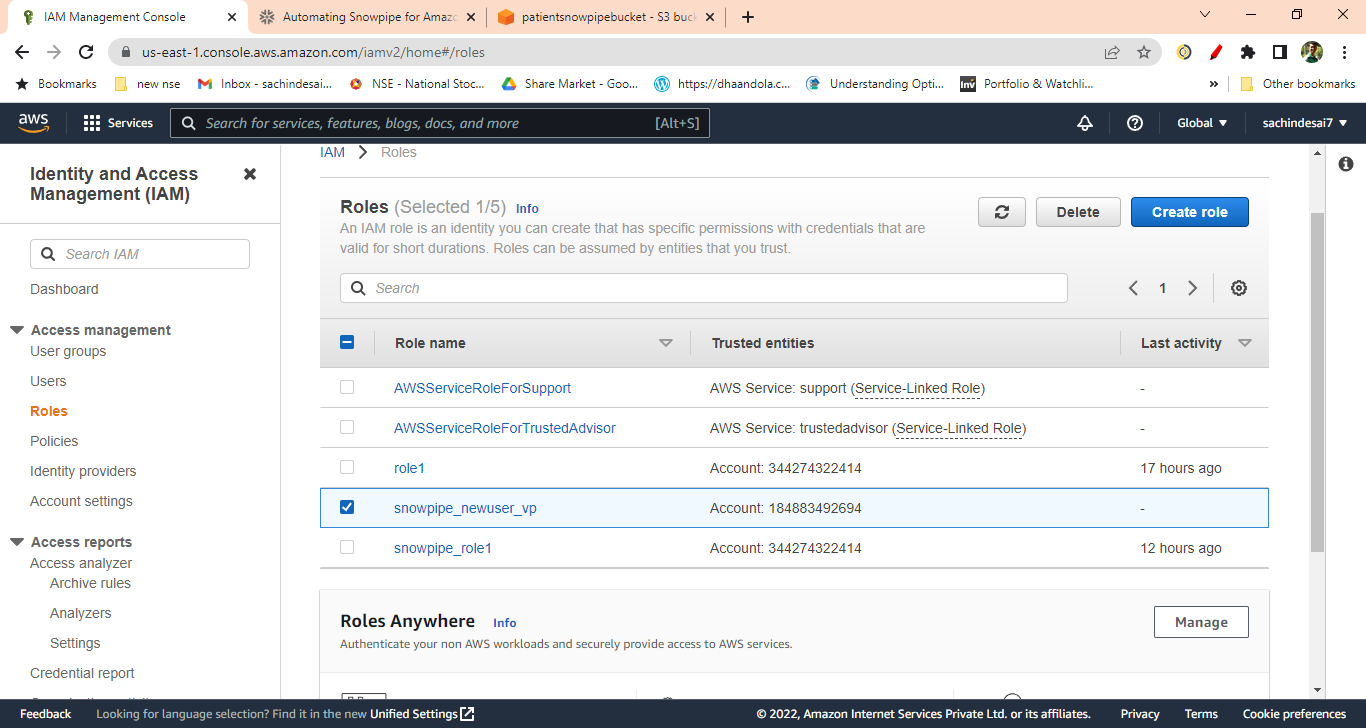


16]. On the next page Enter any unique name to the role you are creating. The description is optional.

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

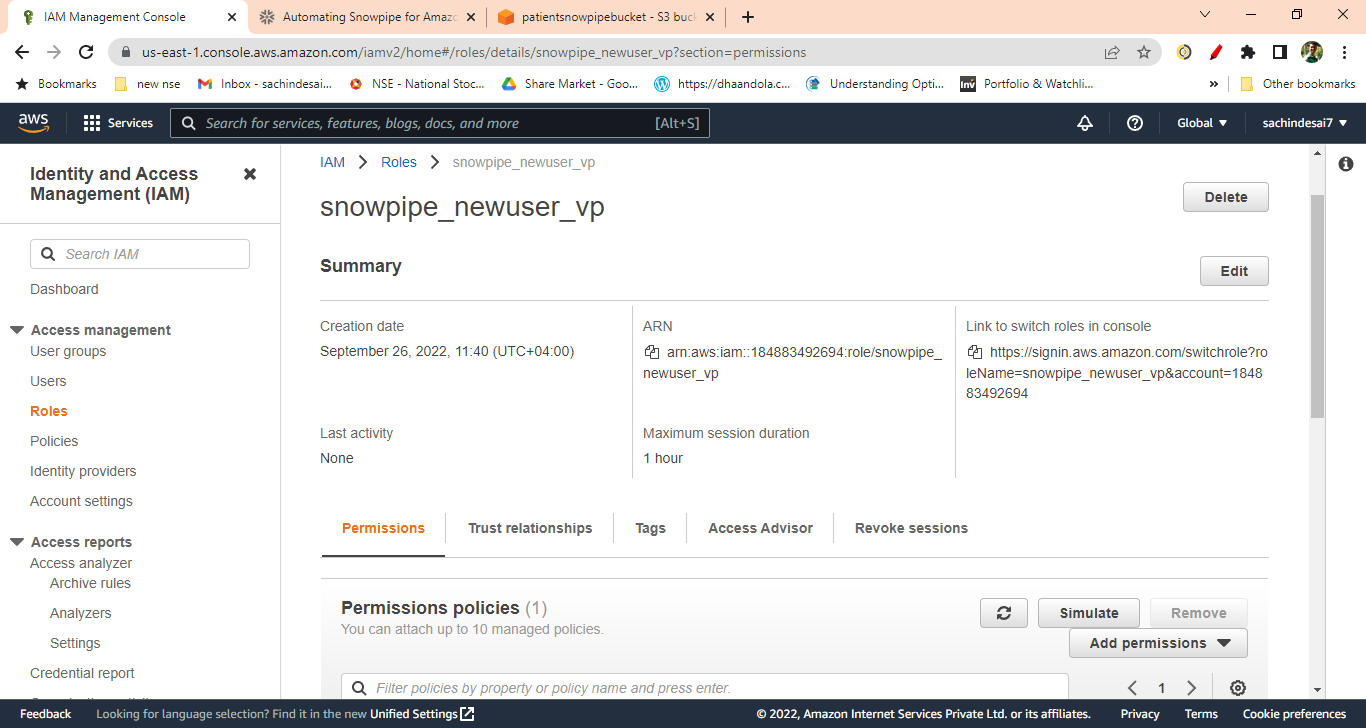


17]. Click on the role that you have created. It will show you the summary page.



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

C:\Users\ACER\Desktop\Screenshot 2022-09-26 130425.png

C:\Users\ACER\Desktop\Screenshot 2022-09-26 130609.png

20]. Now go to the AWS Console

IAM 🡪 Role

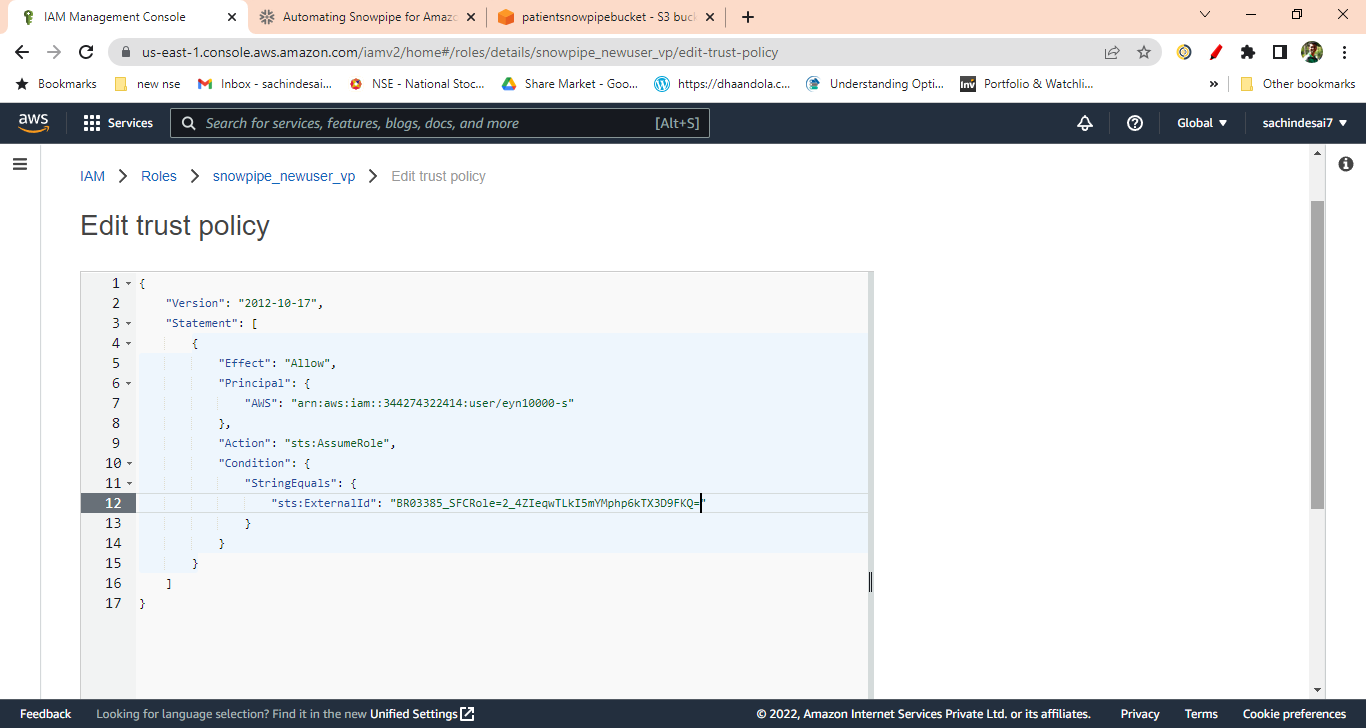
Select the role you created

Click Trust Relationships -> Edit trust relationship

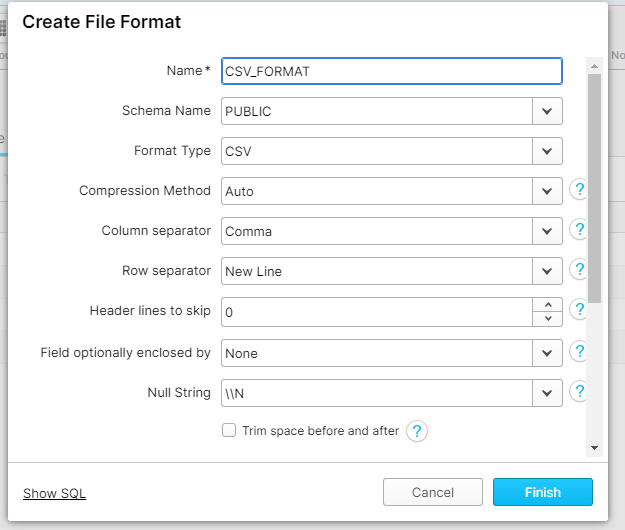
Replace the value of "AWS": with the AWS\_IAM\_USER\_ARN String you got using DESC INTEGRATION

command and, value of "sts:ExternalId": with AWS\_EXTERNAL\_ID String

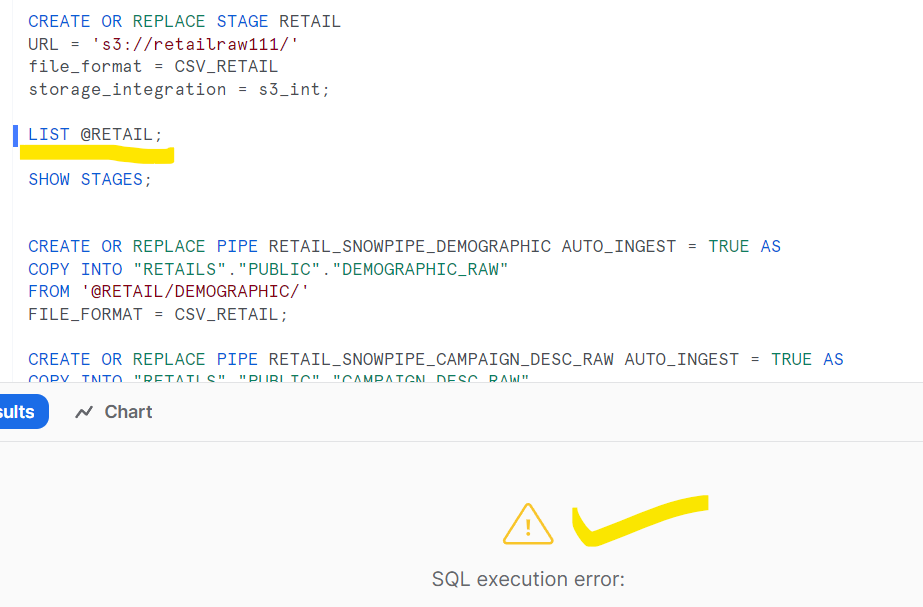
Click Update Policy



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



If error occur during run the command of LIST then copy property value path of STORAGE\_AWS\_IAM\_USER\_ARN & past the AWS account in role (edit thrust relationship)



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)

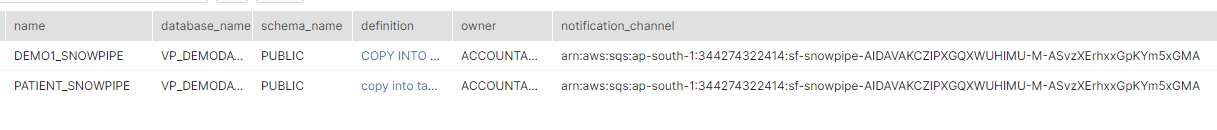
FROM @patient\_snowpipe\_stage -- (name of the stage)

FILE\_FORMAT = ( FORMAT\_NAME = 'CSV\_FORMAT');

24]. After creating snowpipe, get ‘Notification Channel’ value

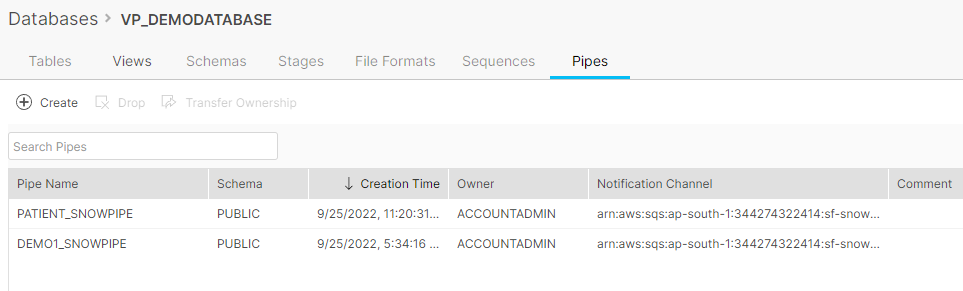
Run command

Show pipes;



Or Go to Database 🡪 Pipes

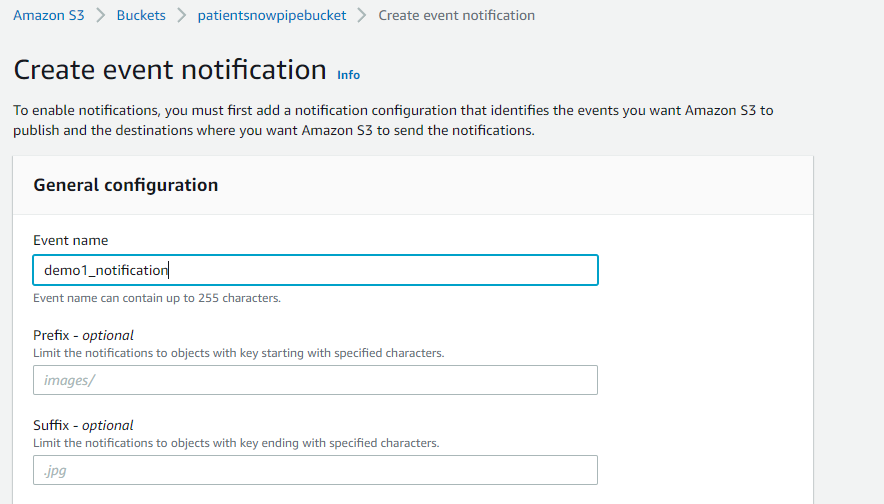
Here also you will get the notification channel value.



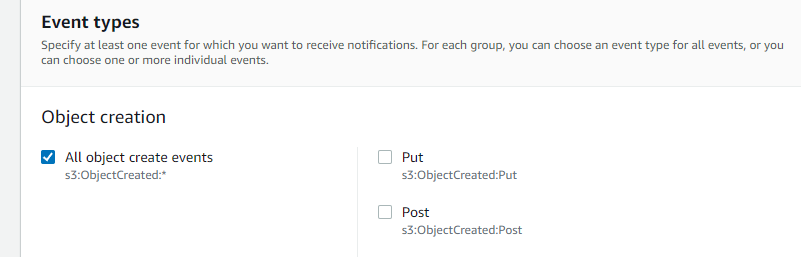
25]. This is the final step. Create an event on S3 bucket. Go to your S3 bucket that you have created. Click on Properties tab and scroll down to

Event Notification -> Click Create Event Notification

Enter any name for the Notification.

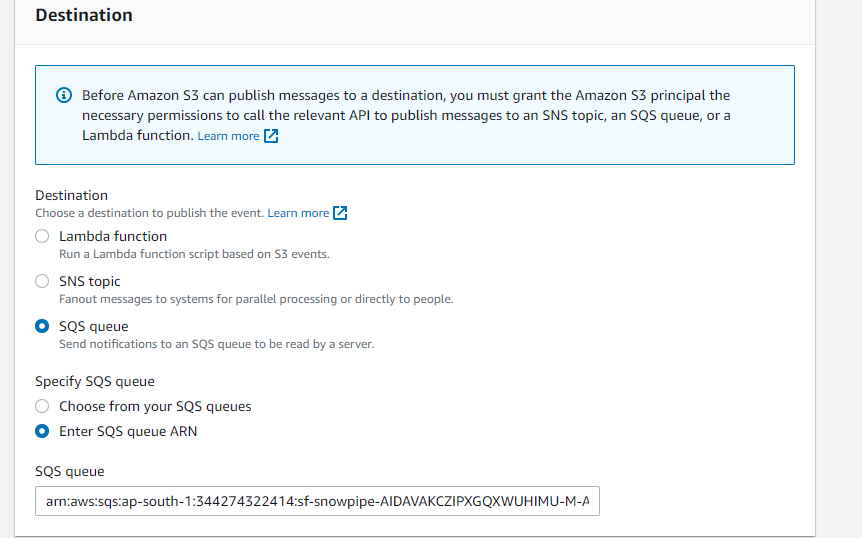


Check All Object create Events



Scroll down to Destination

Select SQS Queue 🡪 Select Enter SQS Queue ARN 🡪 And paste that ‘Notification Channel’ under SQS Queue



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())));