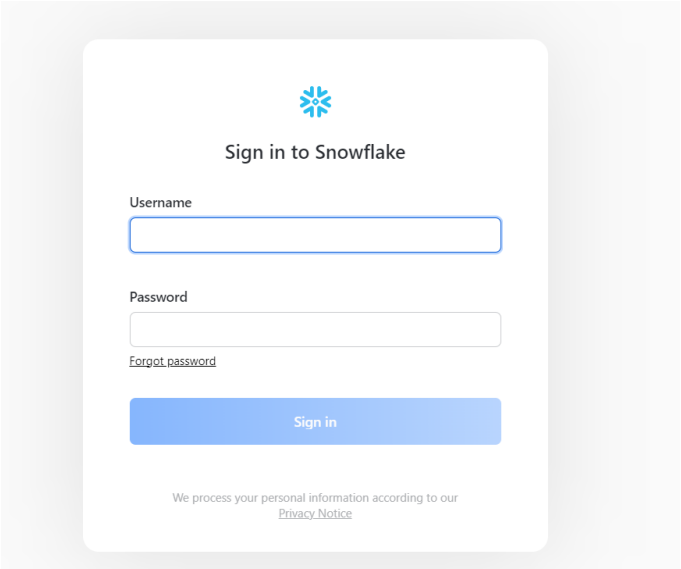
Integration of AWS with Snowflake

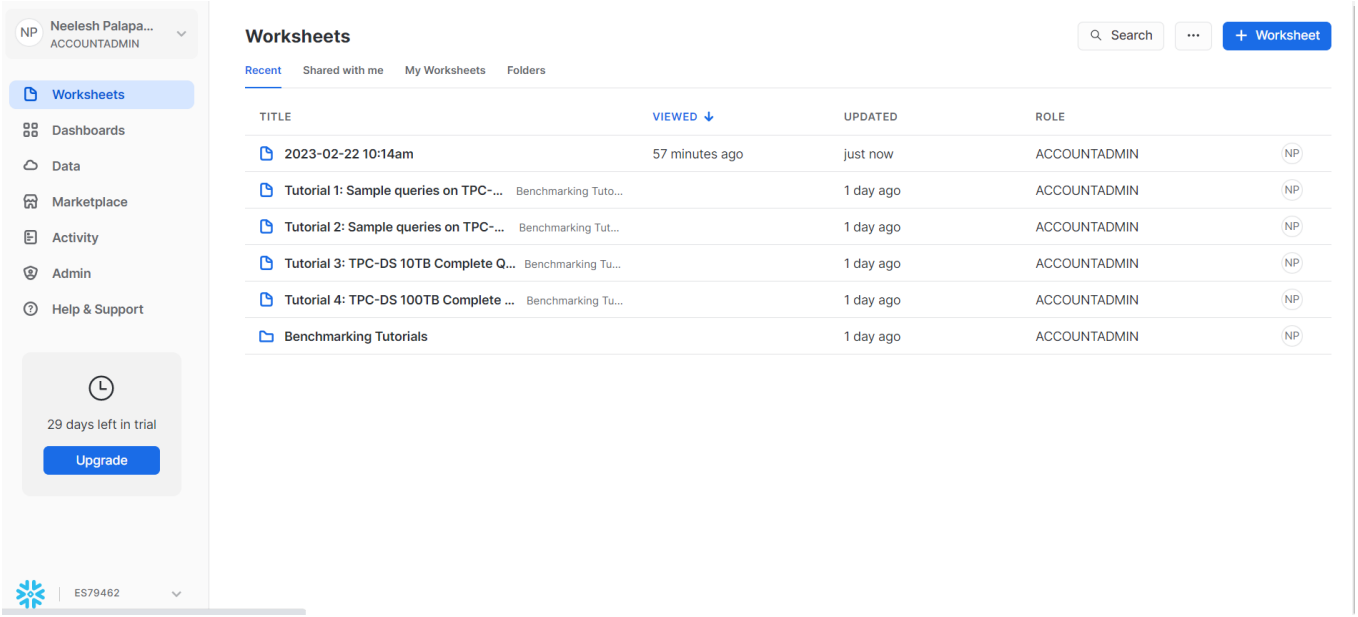
Neelesh Palaparthi

Documentation:

Step 1:

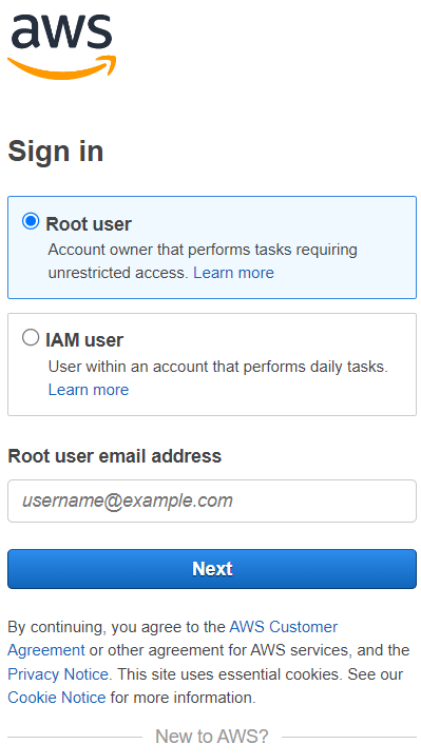
Login into snowflake account:

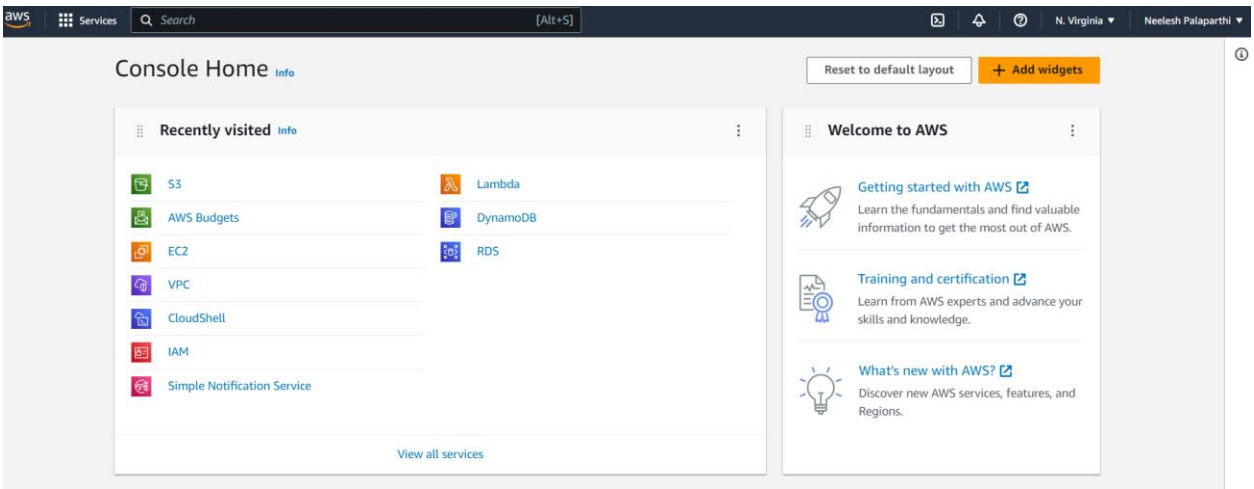




Step 2:

Login into AWS account by using Root user:

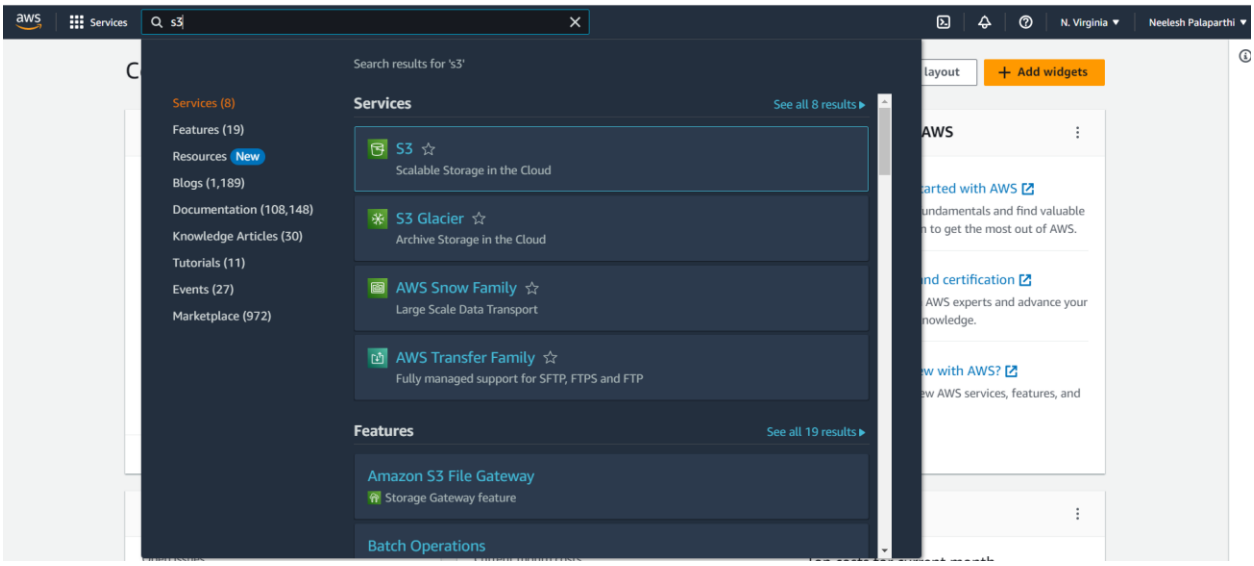




2.1:

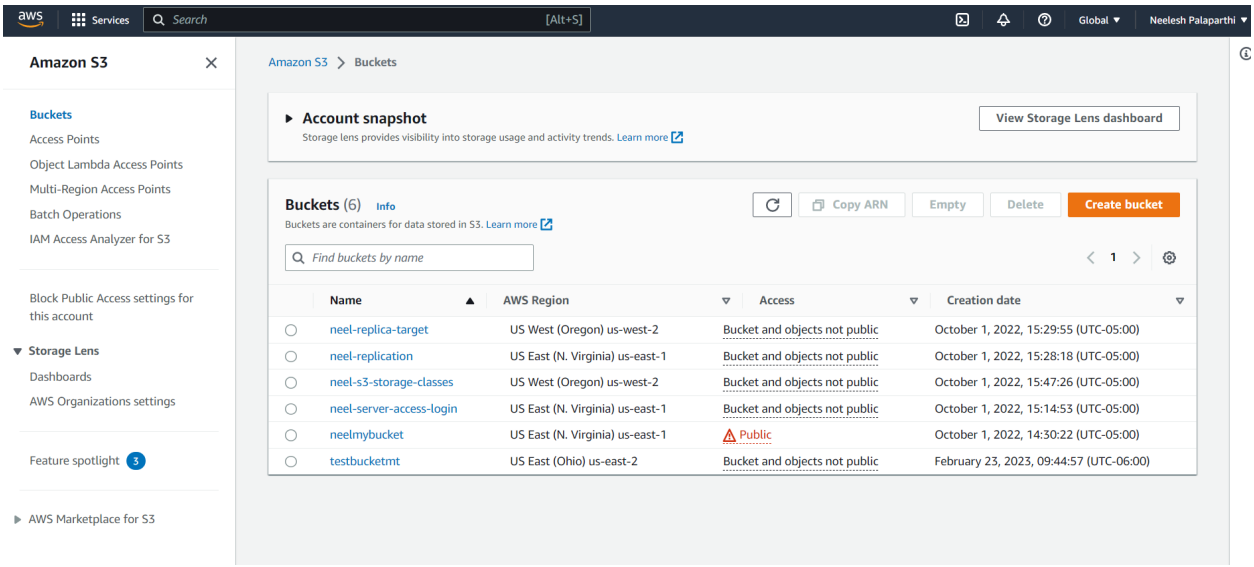
Create S3 Bucket:

Type S3 in the search bar and click on S3.



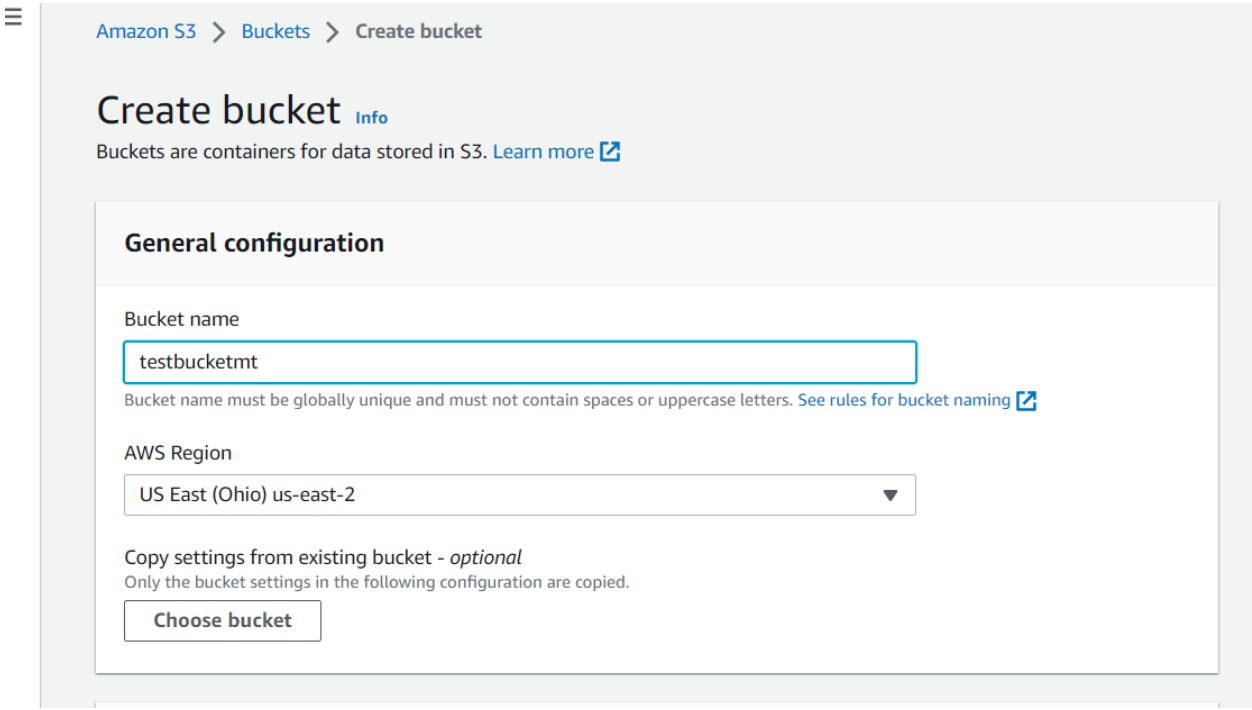
Create a new bucket:

Click on orange button to create new bucket.

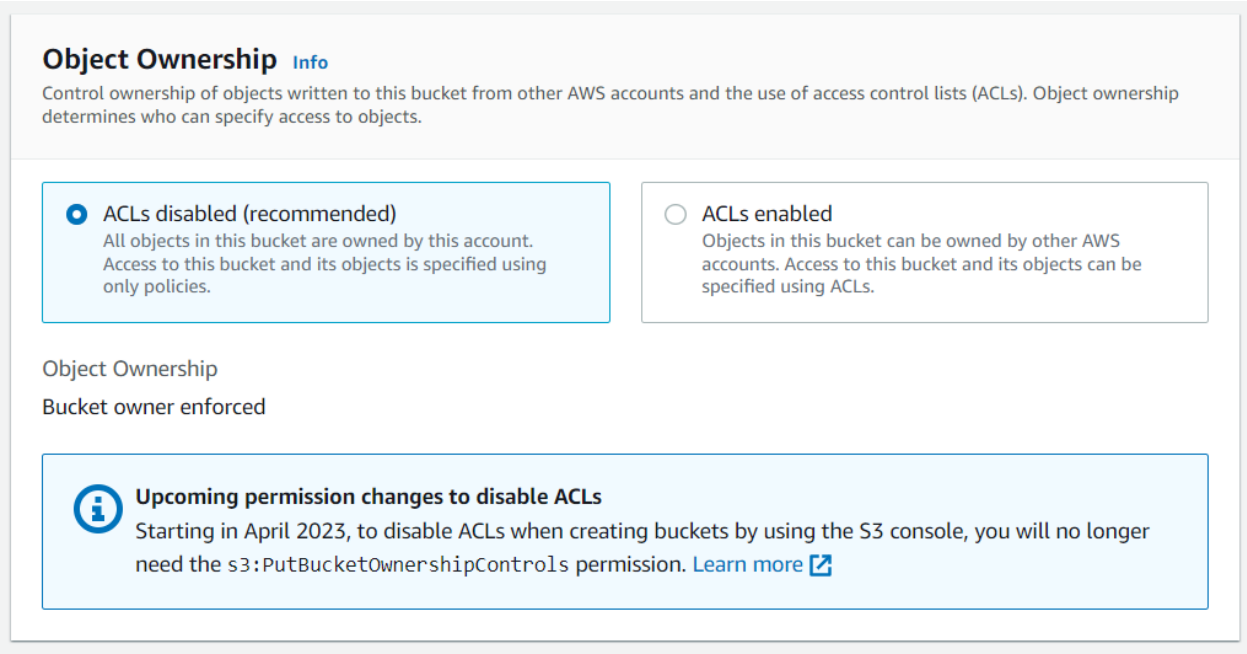


Give a name that is suitable for the project you are doing.

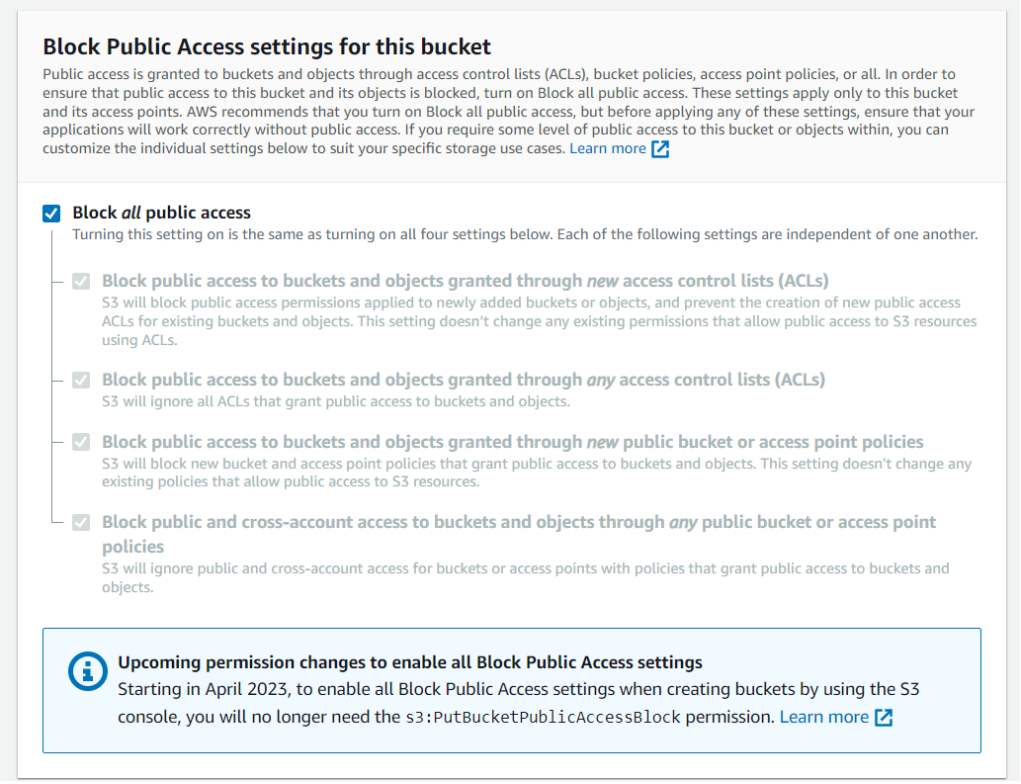
Choose Aws Region appropriatly.



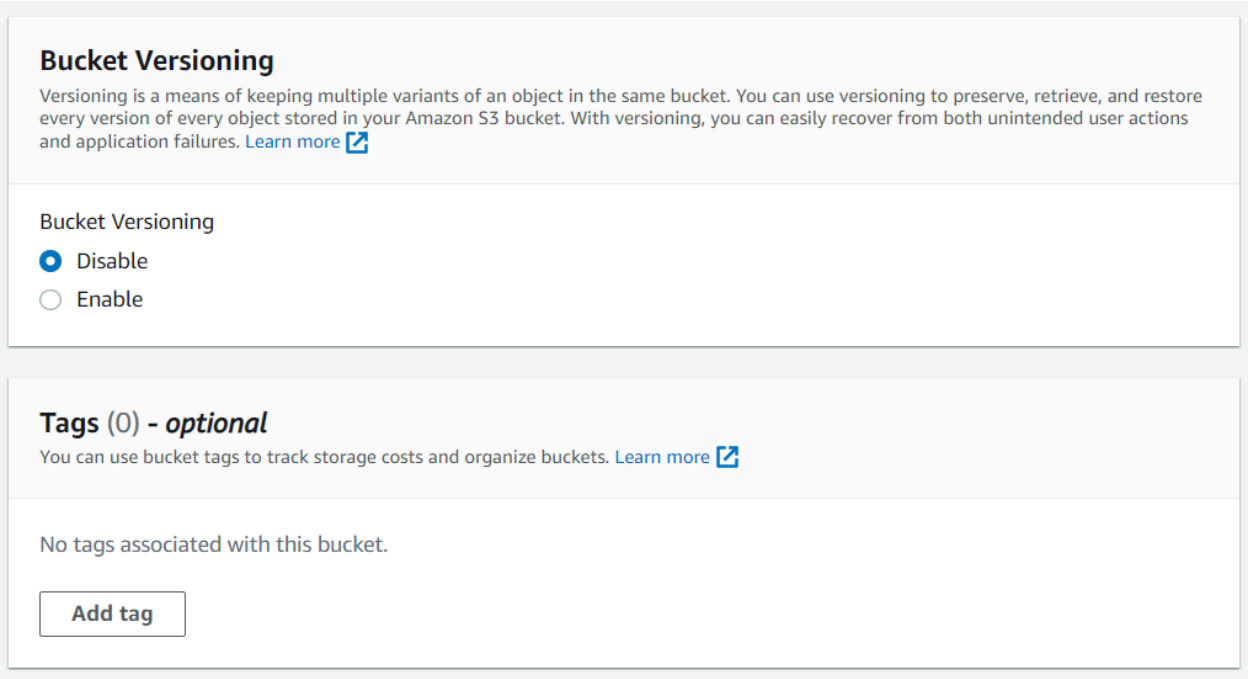
Select these options.



Block all public access.

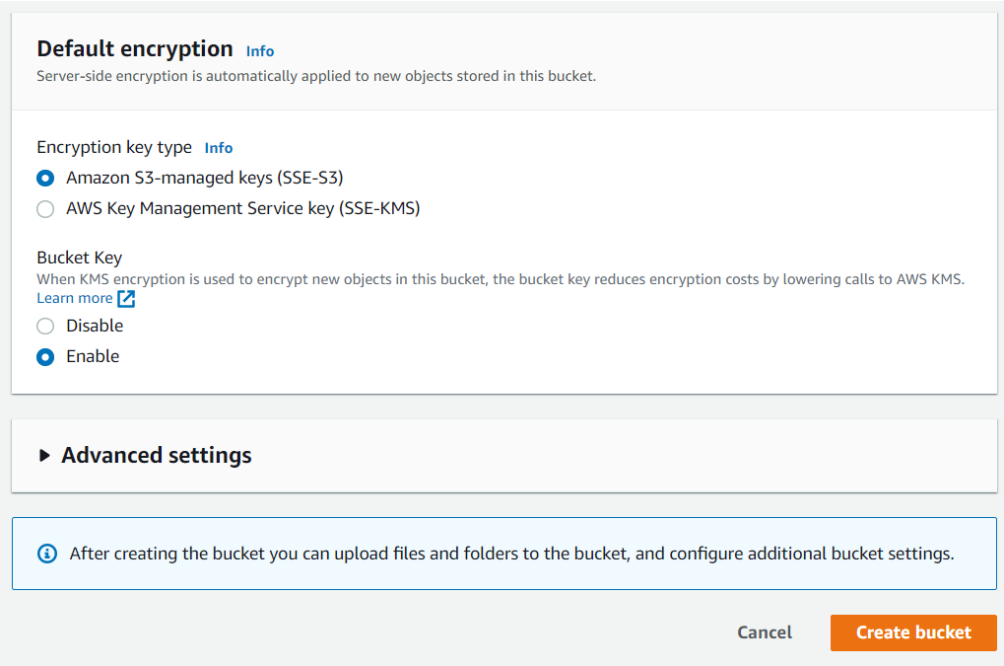


Disable bucket versioning

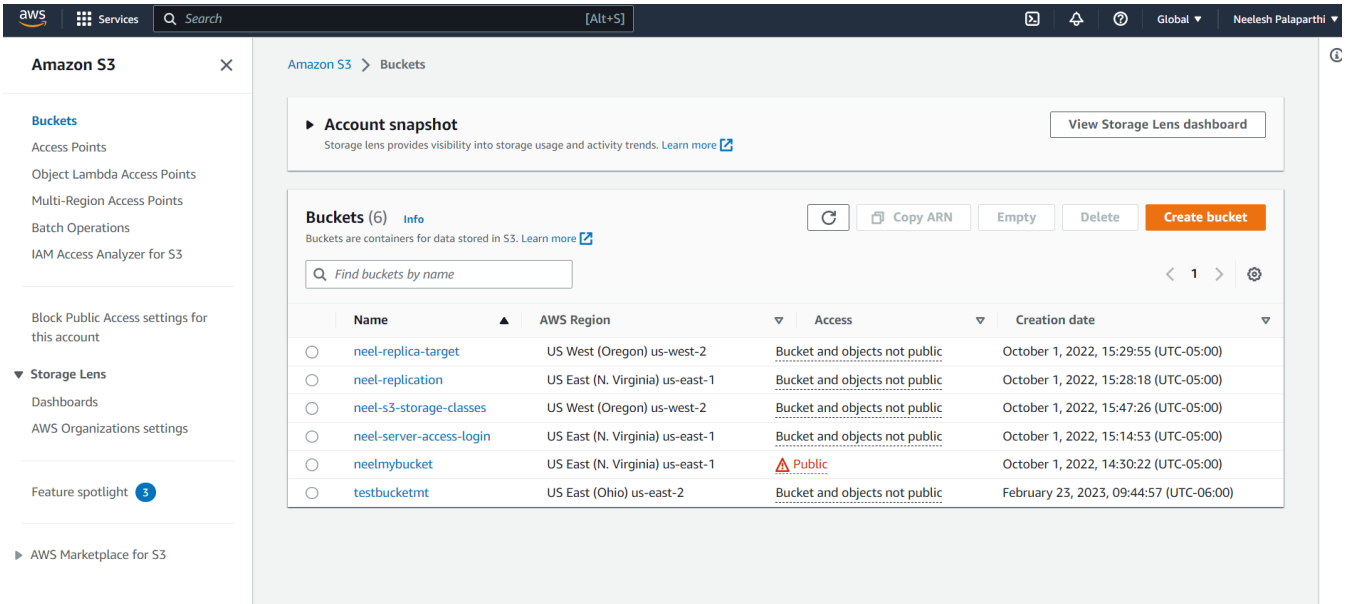


Choose encryption type and enable the bucket key.

Click on create button.



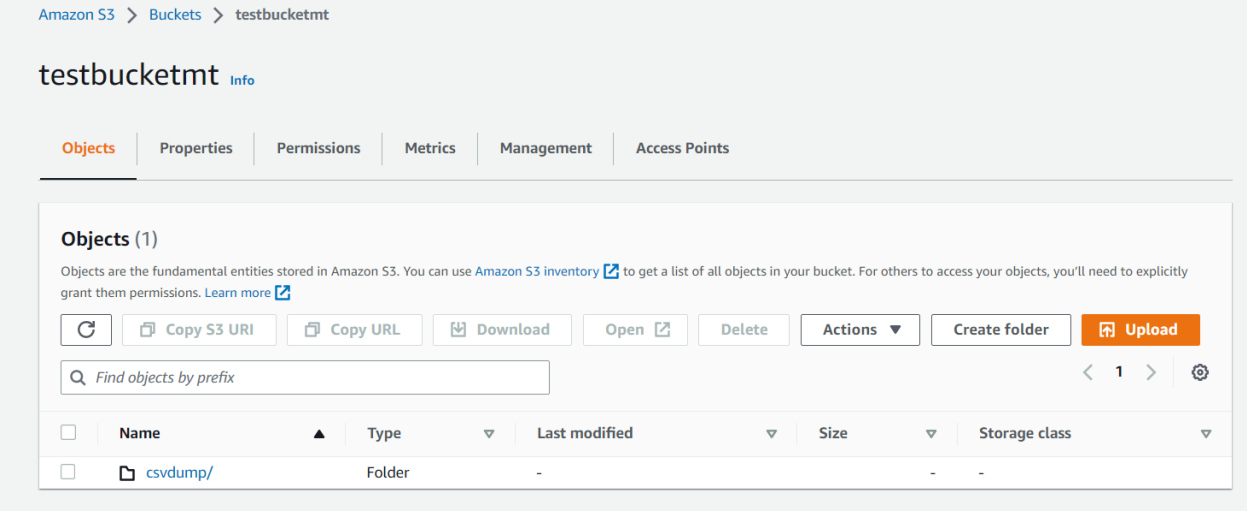
You can see the 'testbucketmt' bucket got created.



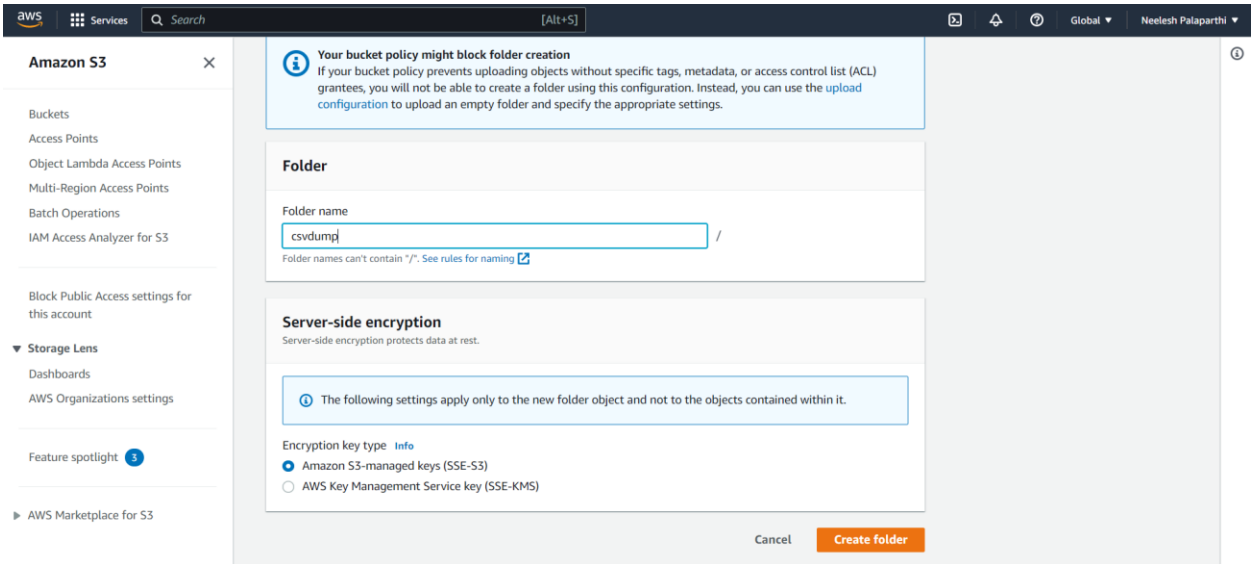
2.2 Create a folder inside s3 Bucket:

Click on the created bucket ‘testbucketmt’.

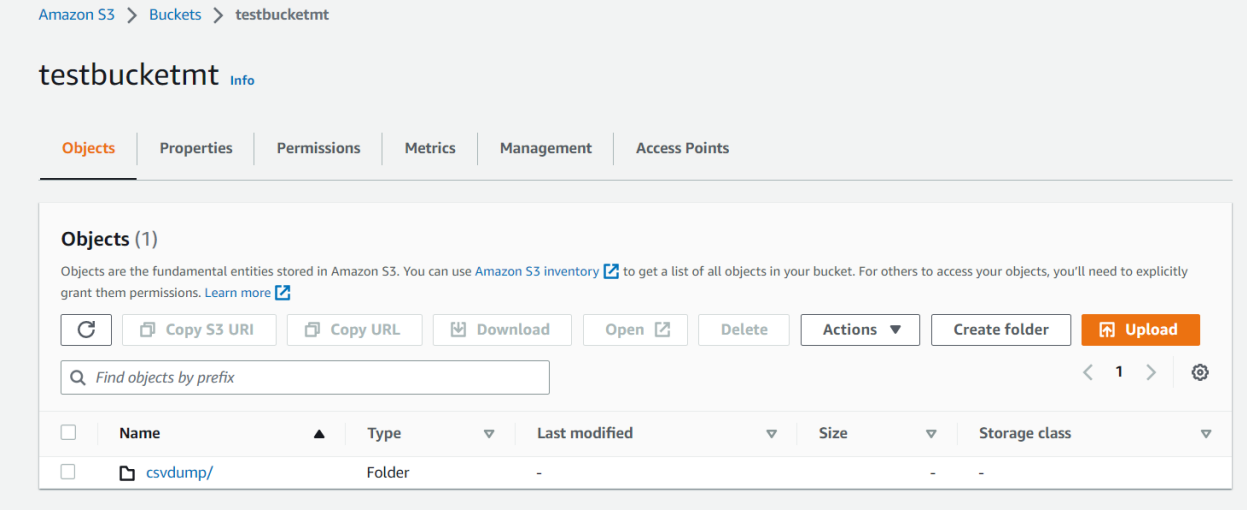
Click on create folder inside the bucket.



Write a name for the folder and choose the encryption key type and click create folder.



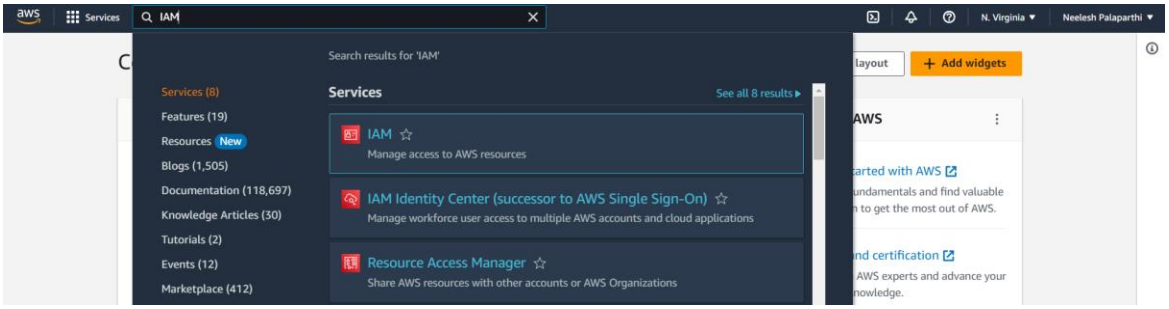
You can see folder is created in s3 bucket ‘csvdump’.



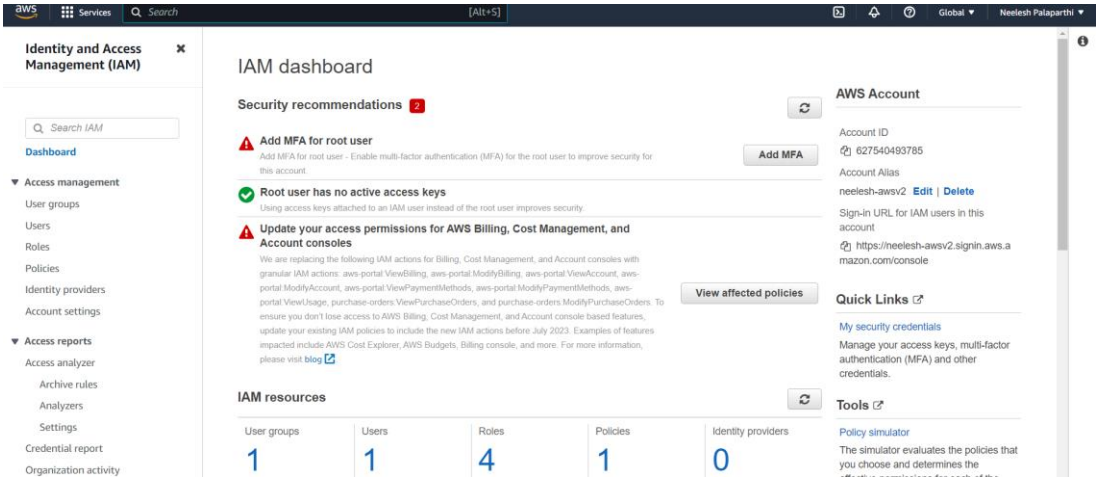
Step 3:

Creating IAM role:

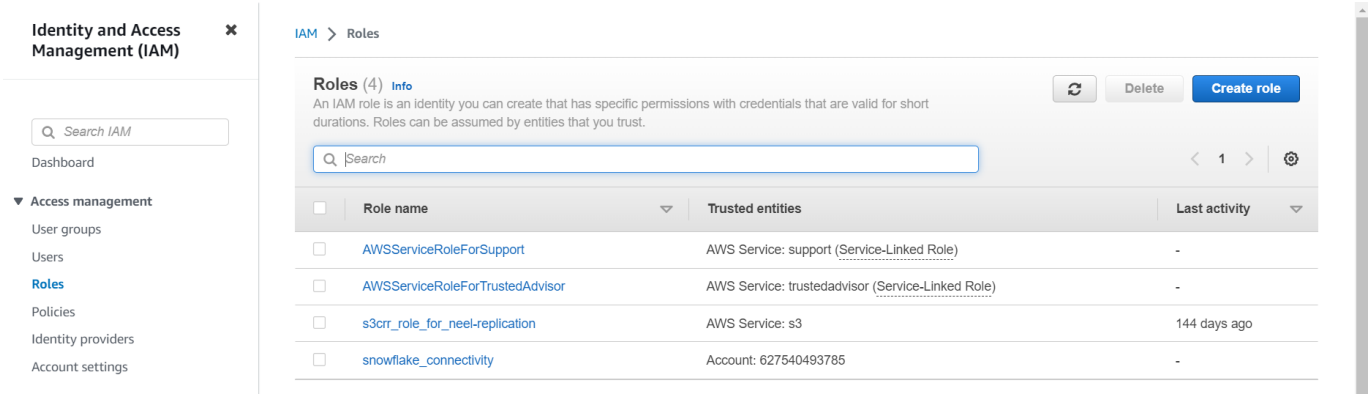
Type IAM in search bar and select IAM service.



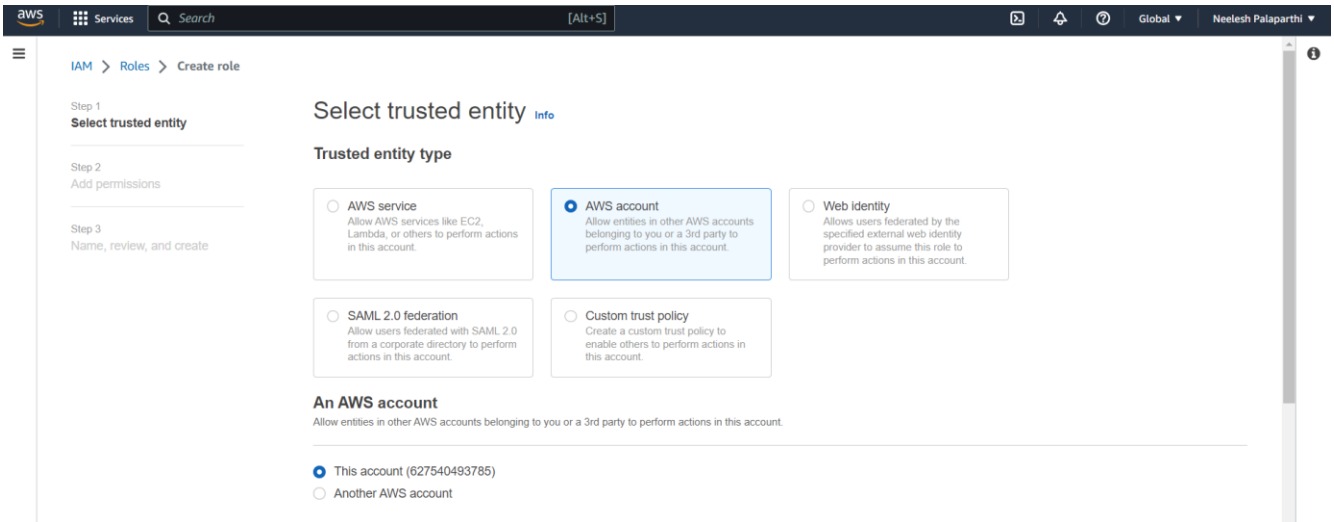
Click on the ‘Roles’ present on the left side.



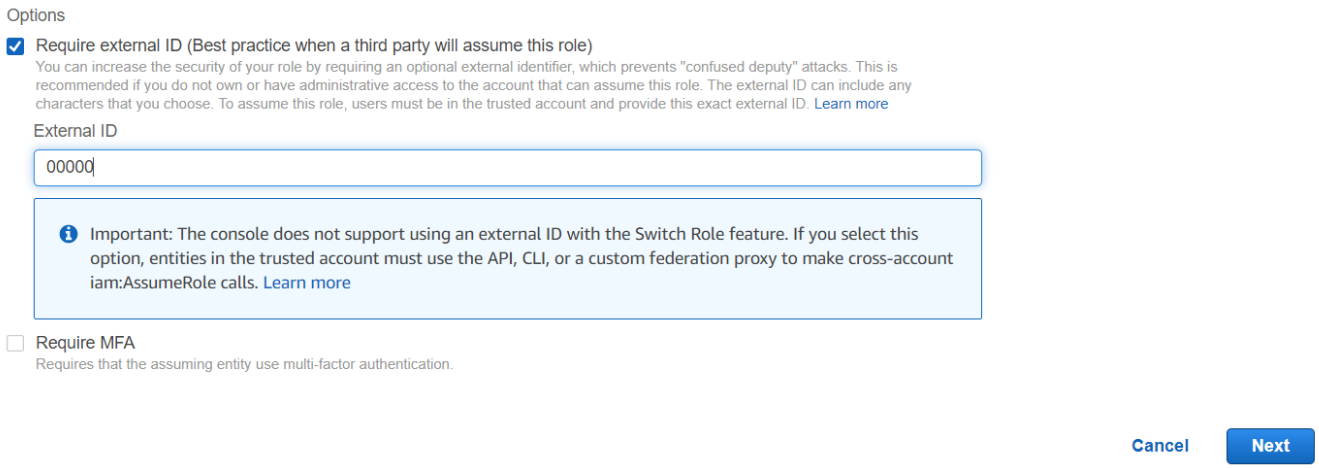
Create A new role by cliking on ‘create role’.



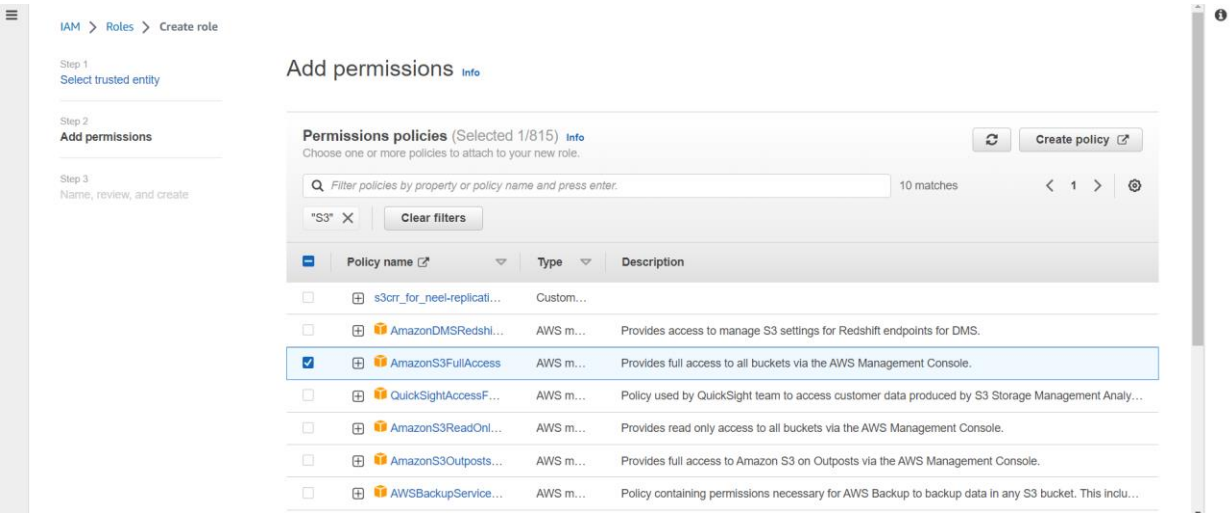
Click on AWS account and select ‘this account’ option.



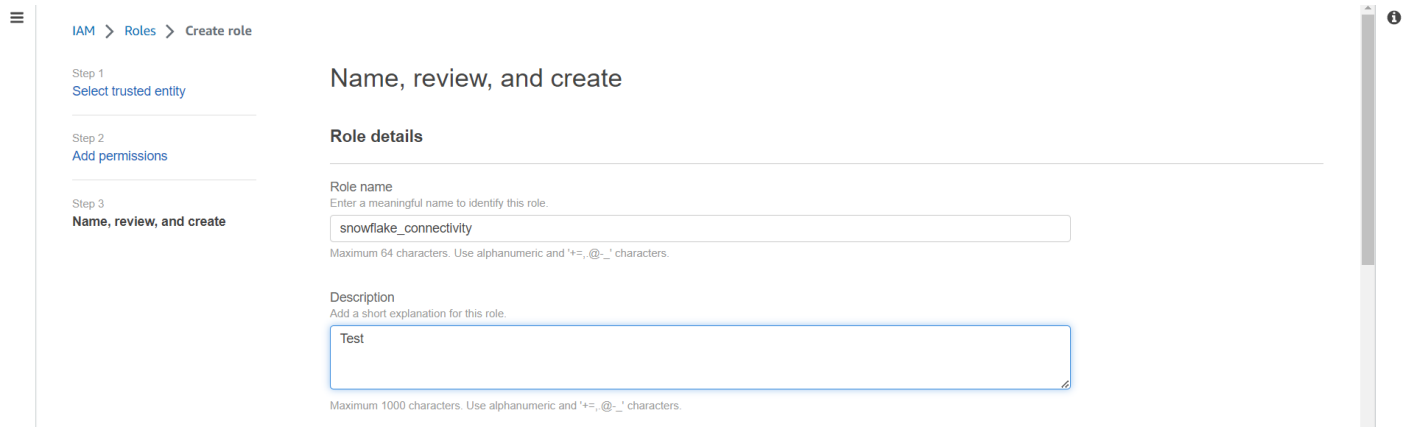
Click on Require external ID and write 5 zero’s ‘00000’ and click next.



As we want to use S3 bucket with IAM service so we need to add permissions. click on space bar and type s3 and choose ‘Amazon s3 full access option’ and click next.



Write the role name and description.



Don’t change anything in the Json code.

Step 1: Select trusted entities

Edit

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": "627540493785"
            },
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "00000"
                }
            }
        }
    ]
}
```

Step 2: Add permissions

Edit

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

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

You can see a role is created ‘snowflake_connectivity’.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

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.

Delete Create role

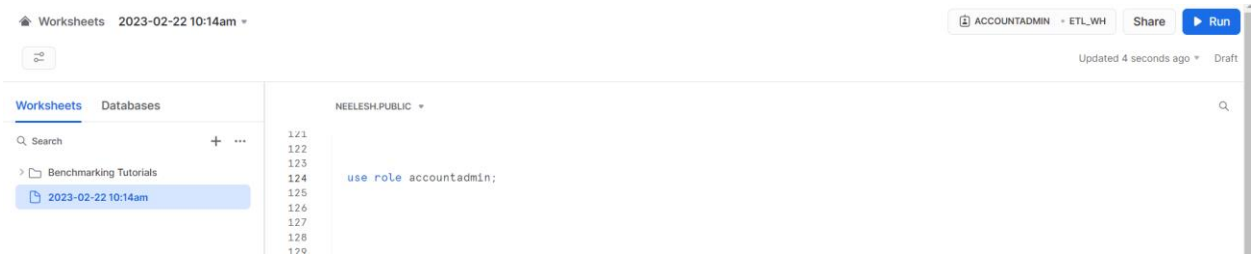
Search

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
s3crr_role_for_neel-replication	AWS Service: s3	145 days ago
snowflake_connectivity	Account: 627540493785	-

Step 4:

Integrating AWS with Snowflake:

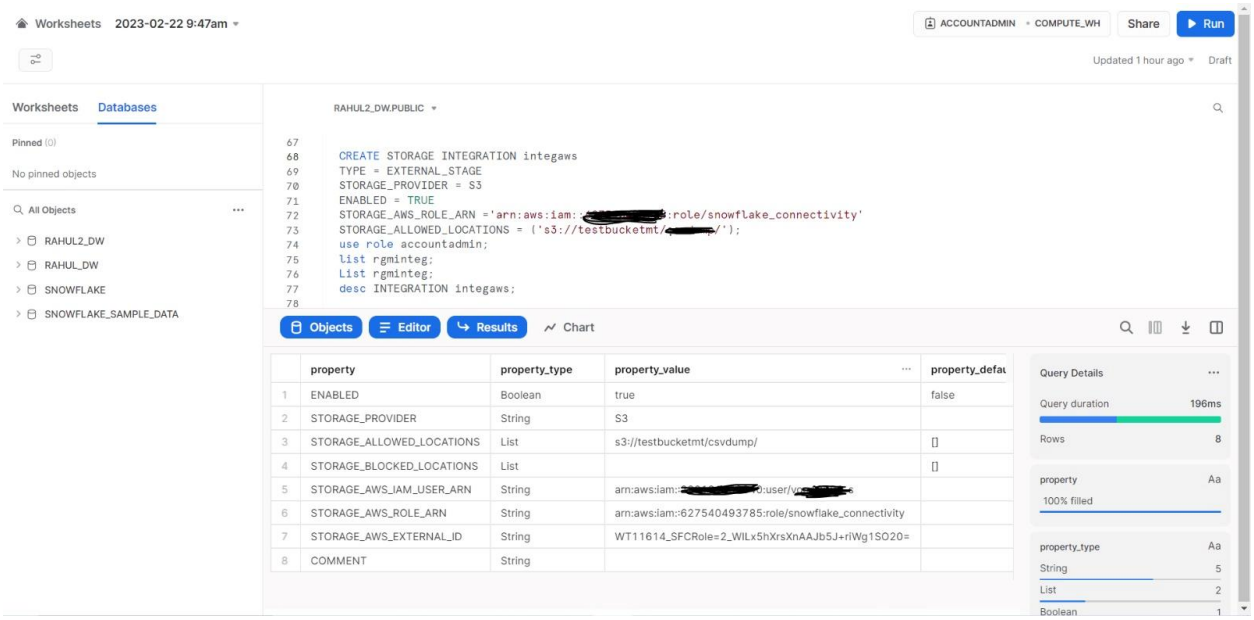
Open worksheet in snowflake and set role as account admin and run it.



Type the following command in worksheet and run it.

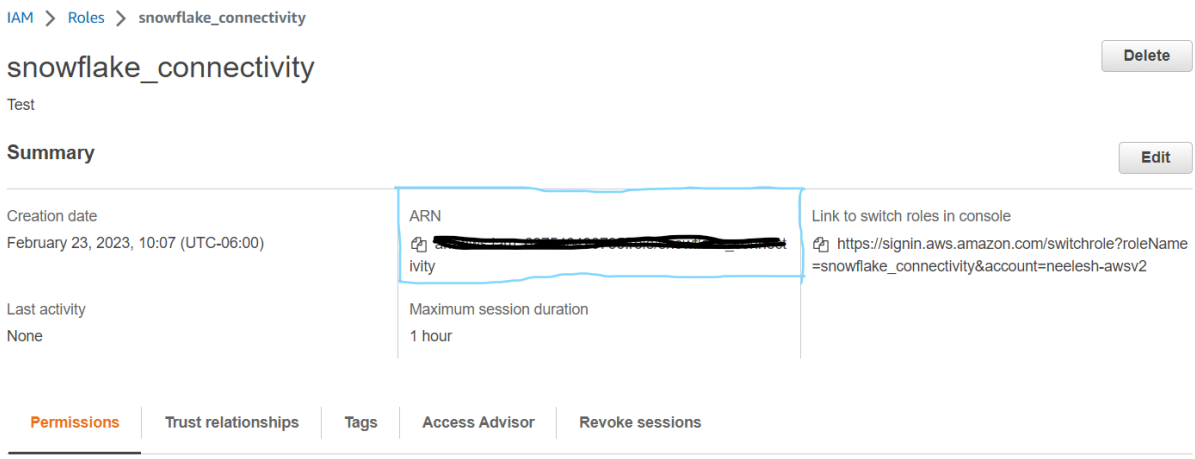
CREATE STORAGE INTEGRATION name
TYPE = EXTERNAL_STAGE
STORAGE_PROVIDER = S3
ENABLED = TRUE
STORAGE_AWS_ROLE_ARN = ’ ‘
STORAGE_ALLOWED_LOCATIONS = (' ');

After running you can see the output which will be similar to the image below.



STORAGE_AWS_ROLE_ARN = ’ ‘

For this, go to IAM service and select the created role and there copy that ARN and paste it in above quotations.



STORAGE_ALLOWED_LOCATIONS = (' ');

For this click the s3 bucket and go inside folder and select folder and there,

Copy the url in highlighted blue box and paste it inside the above command.