

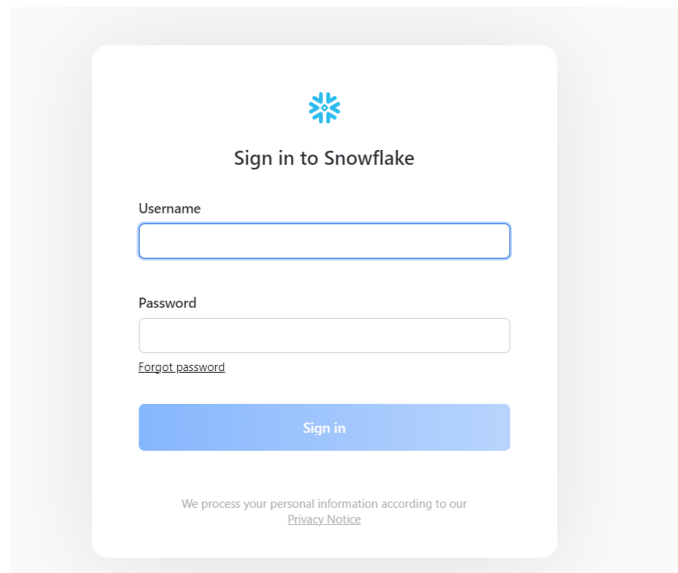
# Integration of AWS with Snowflake

Neelesh Palaparthi

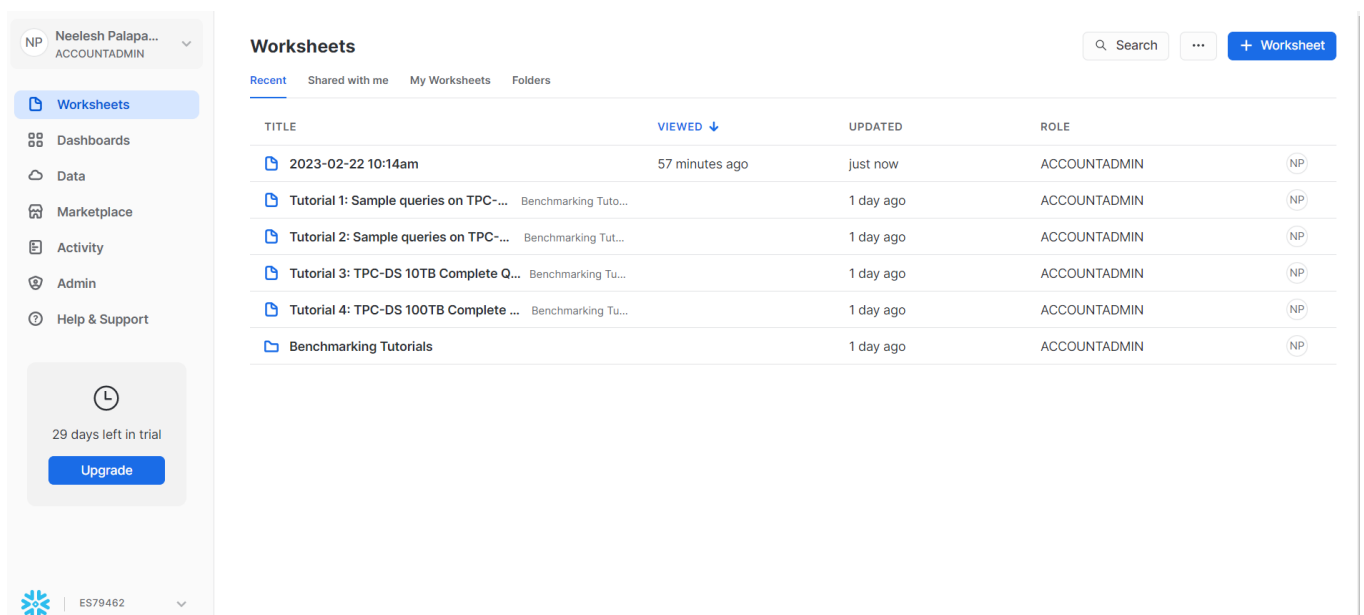
Documentation:

Step 1:

Login into snowflake account:



The image shows the Snowflake login page. At the top is the Snowflake logo, followed by the text "Sign in to Snowflake". Below this are two input fields: "Username" and "Password". There is a link for "Forgot password" below the password field. A blue "Sign in" button is positioned below the password field. At the bottom, a small text line states: "We process your personal information according to our [Privacy Notice](#)".



The image shows the Snowflake Worksheets interface. On the left is a sidebar with a user profile "Neelesh Palapa... ACCOUNTADMIN" and a list of navigation items: Worksheets, Dashboards, Data, Marketplace, Activity, Admin, and Help & Support. Below the sidebar is a trial notice: "29 days left in trial" with an "Upgrade" button. The main area is titled "Worksheets" and includes a search bar, a menu, and a "+ Worksheet" button. Below these are tabs for "Recent", "Shared with me", "My Worksheets", and "Folders". A table lists the recent worksheets:

TITLE	VIEWED ↓	UPDATED	ROLE
2023-02-22 10:14am	57 minutes ago	just now	ACCOUNTADMIN (NP)
Tutorial 1: Sample queries on TPC-... Benchmarking Tuto...		1 day ago	ACCOUNTADMIN (NP)
Tutorial 2: Sample queries on TPC-... Benchmarking Tut...		1 day ago	ACCOUNTADMIN (NP)
Tutorial 3: TPC-DS 10TB Complete Q... Benchmarking Tu...		1 day ago	ACCOUNTADMIN (NP)
Tutorial 4: TPC-DS 100TB Complete ... Benchmarking Tu...		1 day ago	ACCOUNTADMIN (NP)
Benchmarking Tutorials		1 day ago	ACCOUNTADMIN (NP)

At the bottom left, the Snowflake logo and the identifier "ES79462" are visible.

Step 2:

Login into AWS account by using Root user:



## Sign in

☒ **Root user**

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**

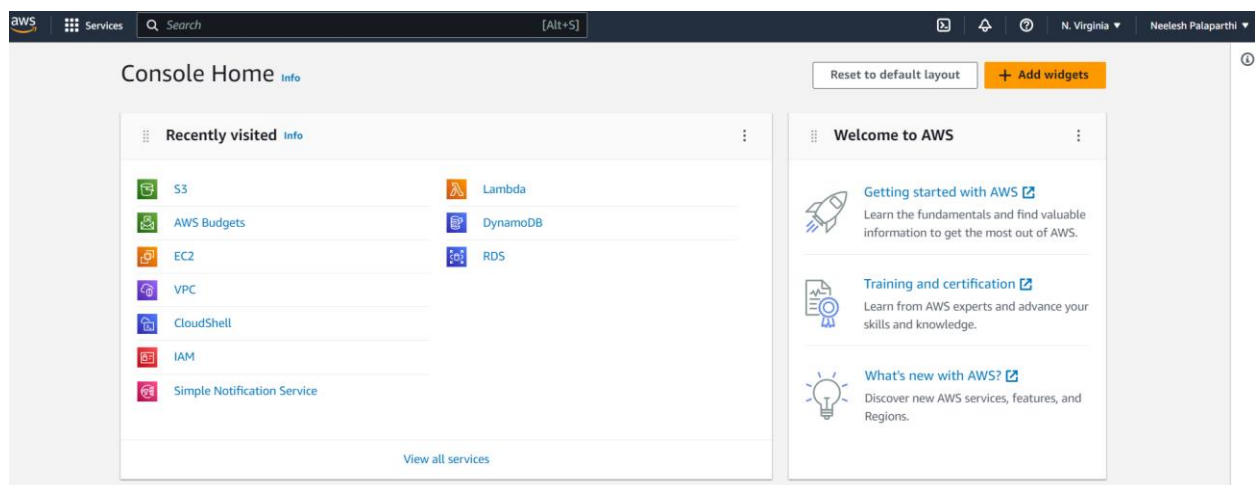
User within an account that performs daily tasks. [Learn more](#)

**Root user email address**

**Next**

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

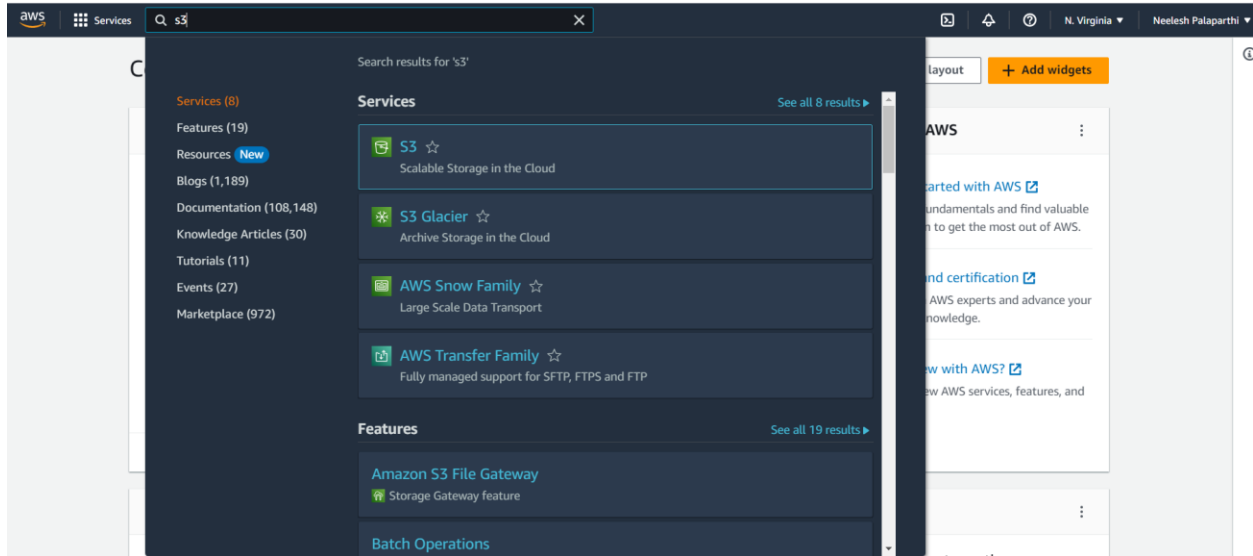
————— New to AWS? —————



2.1:

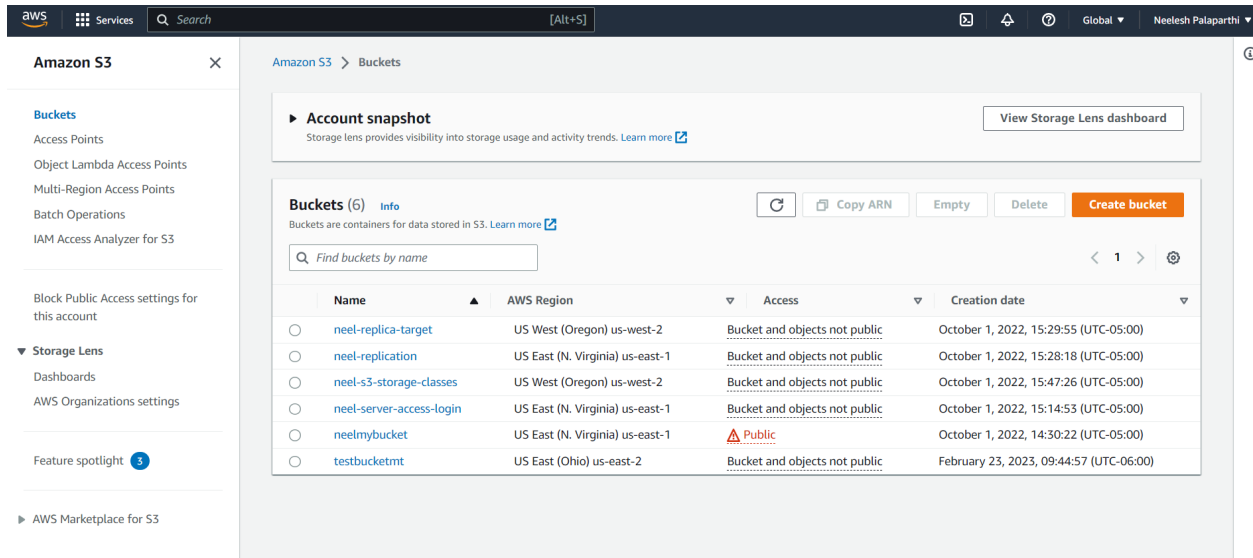
Create S3 Bucket:

Type S3 in the search bar and click on S3.



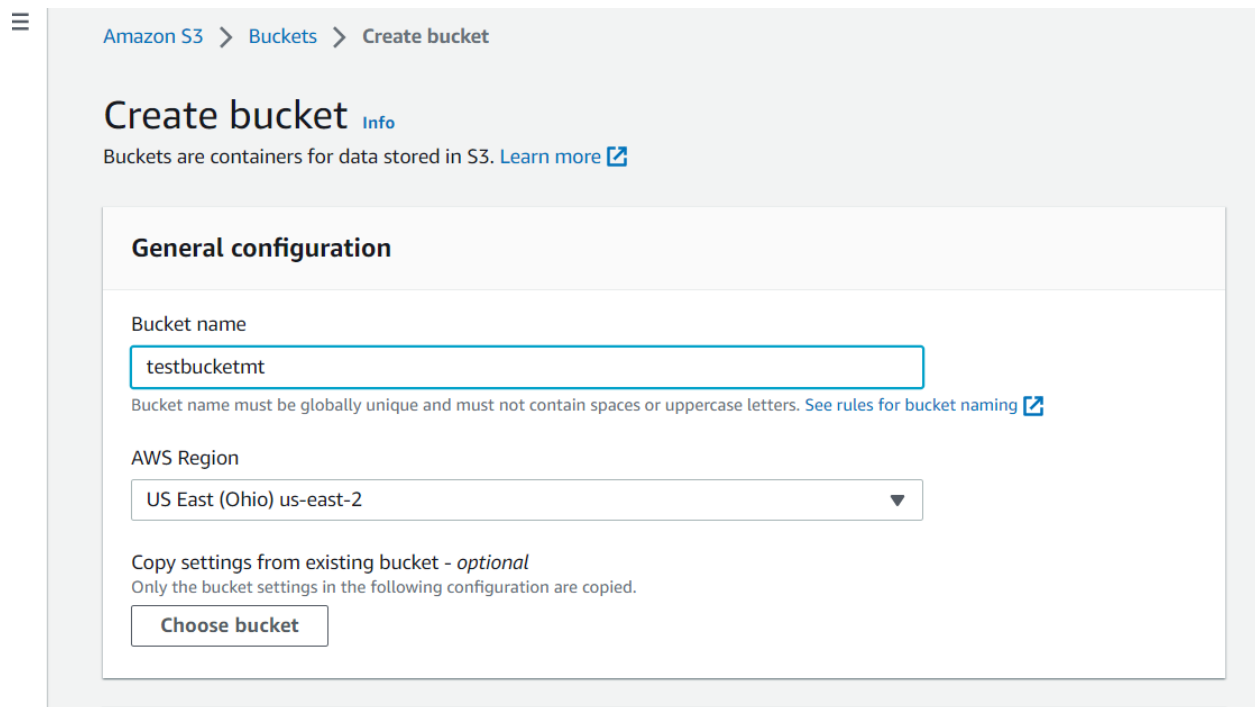
Create a new bucket:

Click on orange button to create new bucket.



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

Choose Aws Region appropriately.



The screenshot shows the 'Create bucket' page in the Amazon S3 console. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > Create bucket'. The main heading is 'Create bucket' with an 'Info' link. Below the heading, a note states 'Buckets are containers for data stored in S3. Learn more' with an external link icon. The 'General configuration' section contains a 'Bucket name' text input field with the value 'testbucketmt', a note about global uniqueness, an 'AWS Region' dropdown menu set to 'US East (Ohio) us-east-2', and a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button.

Amazon S3 > Buckets > Create bucket

## Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

### General configuration

Bucket name

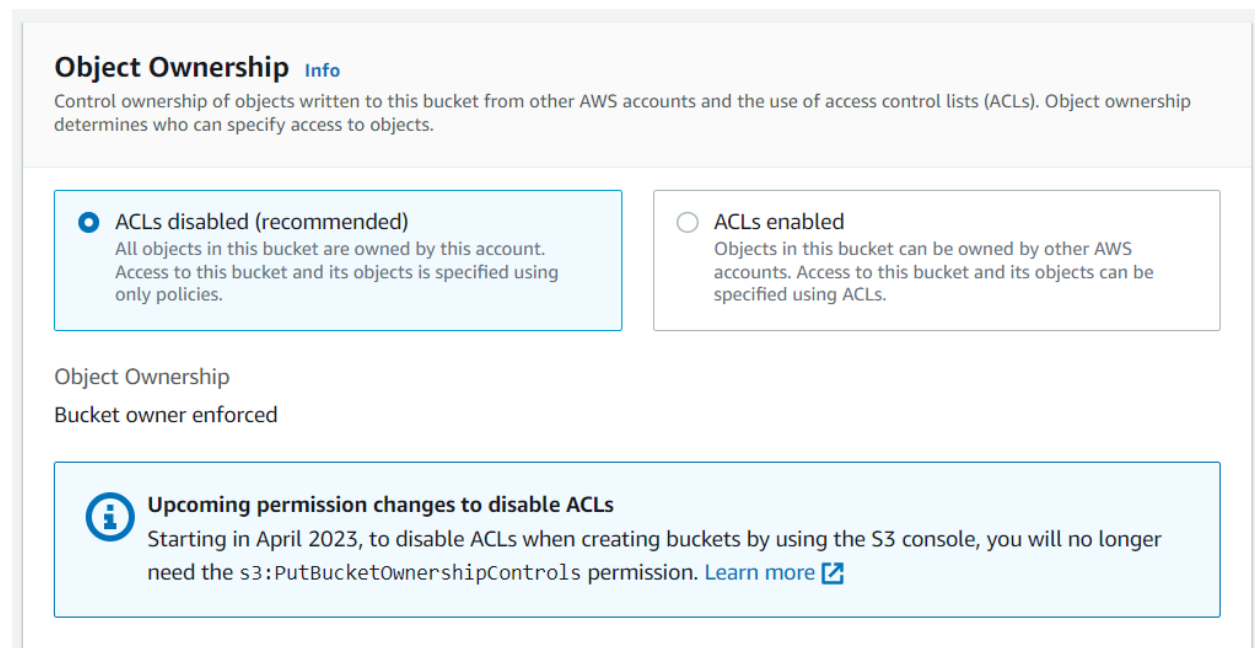
Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - *optional*  
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Select these options.



The screenshot shows the 'Object Ownership' page in the Amazon S3 console. The heading is 'Object Ownership' with an 'Info' link. A descriptive paragraph explains that object ownership controls access from other AWS accounts and ACLs. Two radio button options are presented: 'ACLs disabled (recommended)' (selected) and 'ACLs enabled'. Below these, the 'Object Ownership' section is set to 'Bucket owner enforced'. A blue information banner at the bottom announces 'Upcoming permission changes to disable ACLs', stating that starting in April 2023, the 's3:PutBucketOwnershipControls' permission will no longer be required.

## Object Ownership [Info](#)


Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

 **Upcoming permission changes to disable ACLs**  
Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you will no longer need the `s3:PutBucketOwnershipControls` permission. [Learn more](#)

## Block all public access.

### Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒

**Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☒

**Block public access to buckets and objects granted through *new* access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☒


**Block public access to buckets and objects granted through *any* access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.

☒

**Block public access to buckets and objects granted through *new* public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☒

**Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



**Upcoming permission changes to enable all Block Public Access settings**  
Starting in April 2023, to enable all Block Public Access settings when creating buckets by using the S3 console, you will no longer need the `s3:PutBucketPublicAccessBlock` permission. [Learn more](#)

## Disable bucket versioning

### Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☒ Disable

☐ Enable

### Tags (0) - optional

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

Add tag

Choose encryption type and enable the bucket key.

Click on create button.

### Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type [Info](#)

☒ Amazon S3-managed keys (SSE-S3)

☐ AWS Key Management Service key (SSE-KMS)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

☐ Disable

☒ Enable

► Advanced settings

❗ After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel [Create bucket](#)

You can see the ‘testbucketmt’ bucket got created.

aws

Services

Search

[Alt+S]

Global

Neelesh Palaparthi

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

► AWS Marketplace for S3

Amazon S3 > Buckets

► Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

Buckets (6) [Info](#)

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

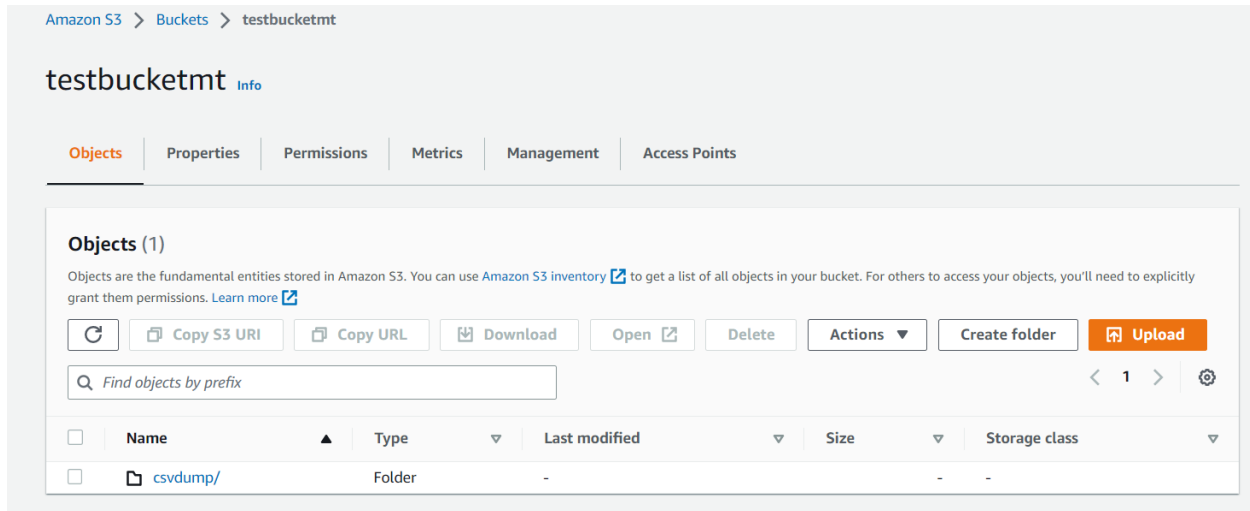
[<](#) [1](#) [>](#) [Settings](#)

	Name ▲	AWS Region ▼	Access ▼	Creation date ▼
<input type="radio"/>	neel-replica-target	US West (Oregon) us-west-2	Bucket and objects not public	October 1, 2022, 15:29:55 (UTC-05:00)
<input type="radio"/>	neel-replication	US East (N. Virginia) us-east-1	Bucket and objects not public	October 1, 2022, 15:28:18 (UTC-05:00)
<input type="radio"/>	neel-s3-storage-classes	US West (Oregon) us-west-2	Bucket and objects not public	October 1, 2022, 15:47:26 (UTC-05:00)
<input type="radio"/>	neel-server-access-login	US East (N. Virginia) us-east-1	Bucket and objects not public	October 1, 2022, 15:14:53 (UTC-05:00)
<input type="radio"/>	neelmybucket	US East (N. Virginia) us-east-1	<span>Public</span>	October 1, 2022, 14:30:22 (UTC-05:00)
<input type="radio"/>	testbucketmt	US East (Ohio) us-east-2	Bucket and objects not public	February 23, 2023, 09:44:57 (UTC-06:00)

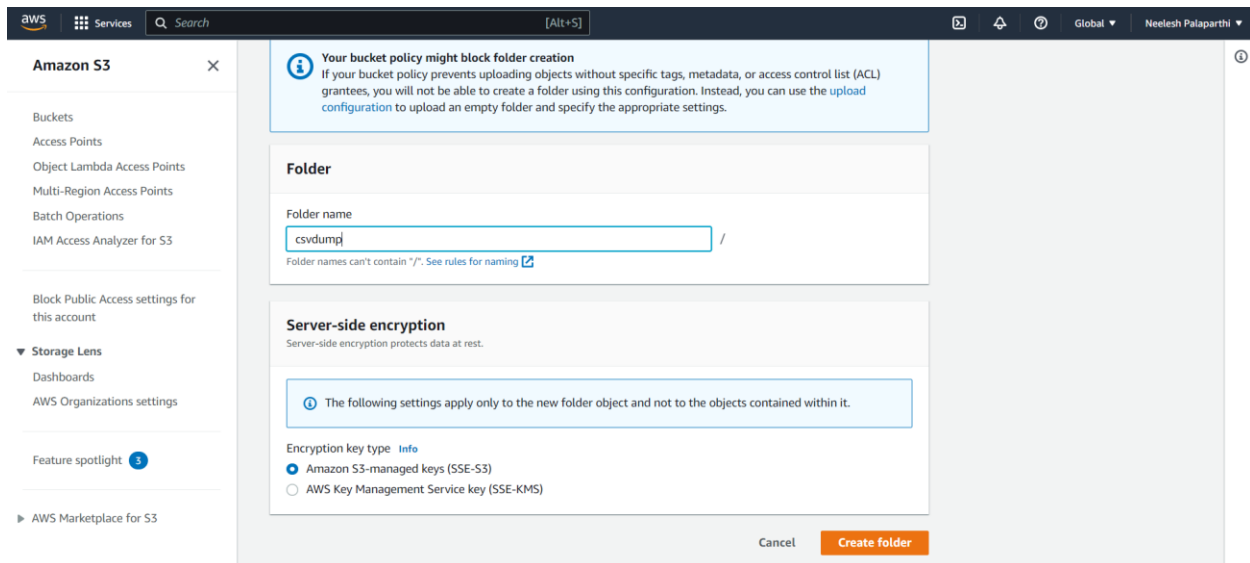
## 2.2 Create a folder inside s3 Bucket:

Click on the created bucket 'testbucketmt'.

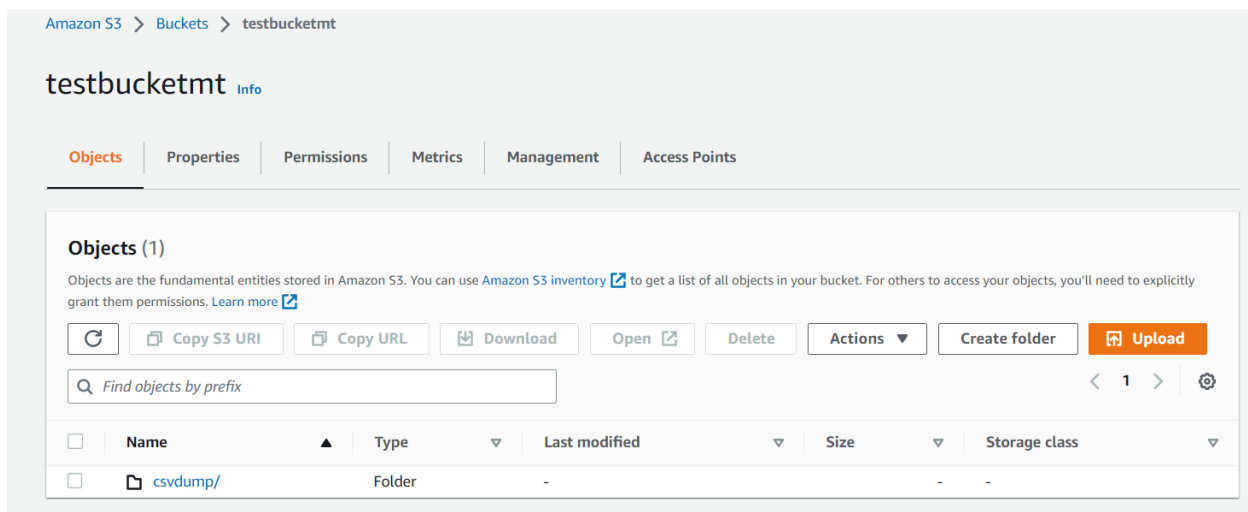
Click on create folder inside the bucket.



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



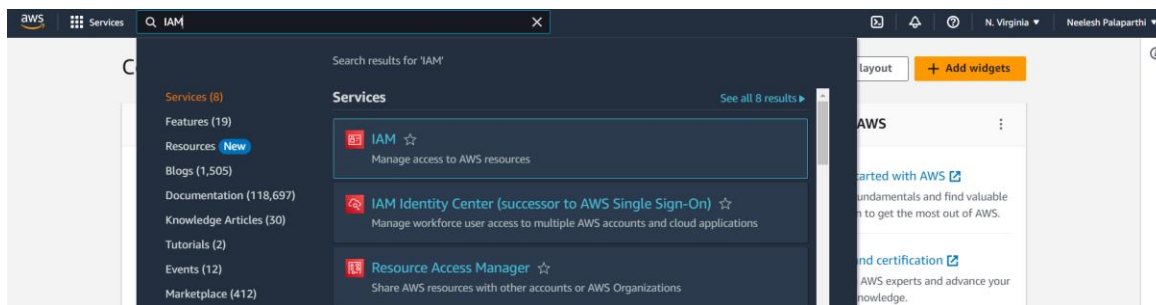
You can see folder is created in s3 bucket 'csvdump'.



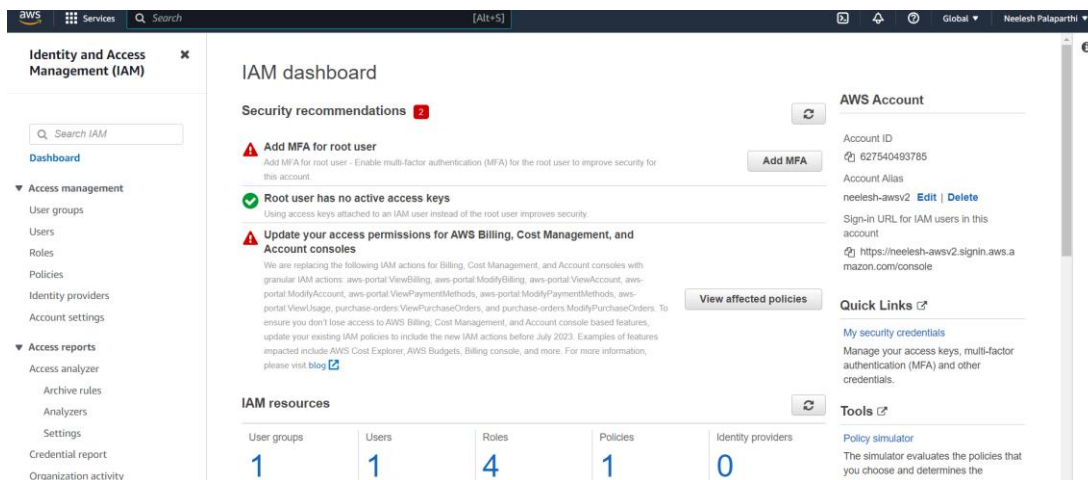
Step 3:

Creating IAM role:

Type IAM in search bar and select IAM service.

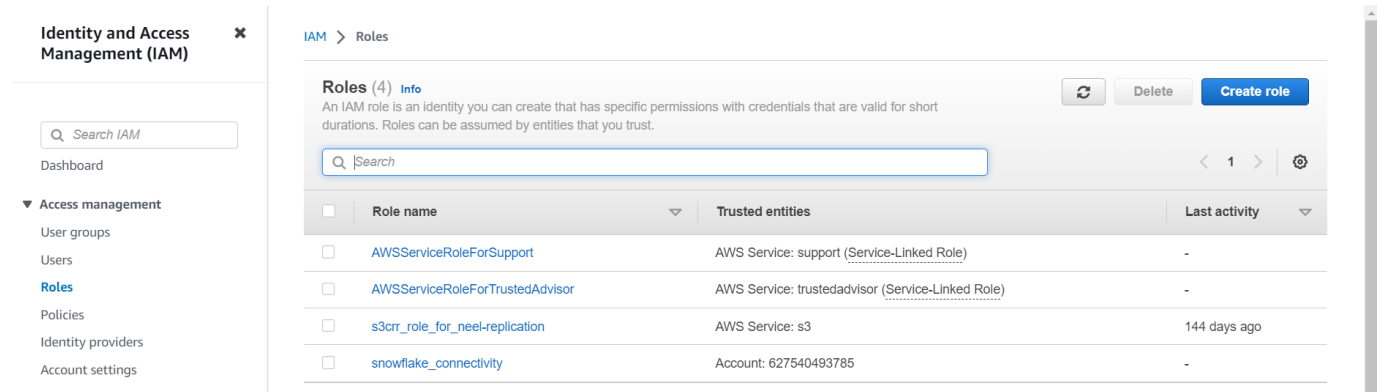


Click on the 'Roles' present on the left side.





Create A new role by clicking on 'create role'.



**Identity and Access Management (IAM)**

Search IAM

Dashboard

▼ Access management

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

IAM > Roles

**Roles (4)** [Info](#)

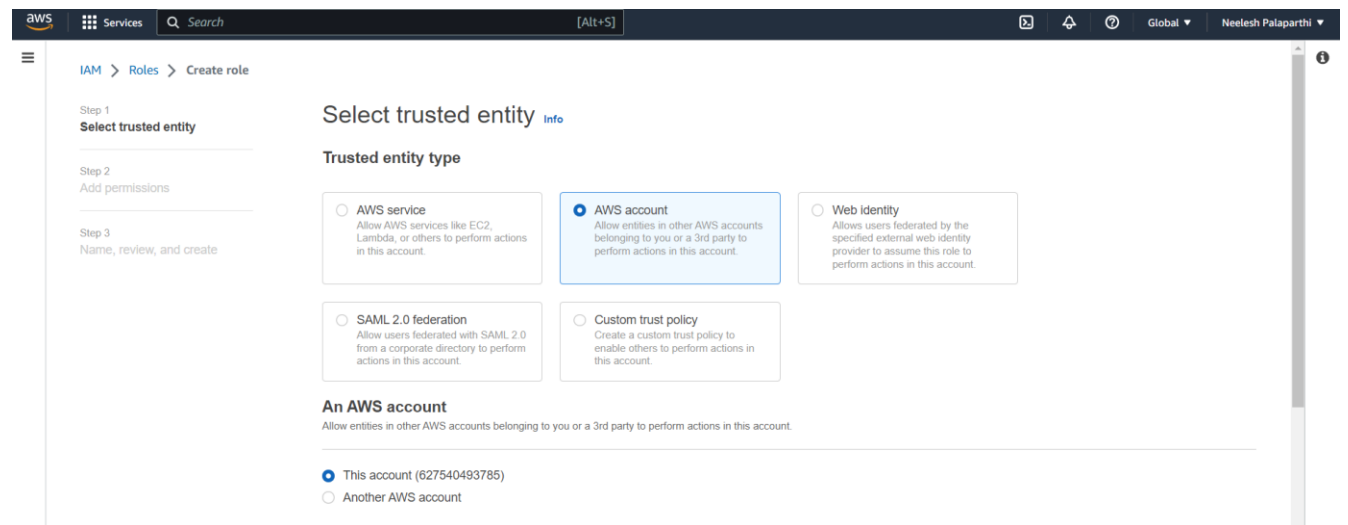
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	<a href="#">AWSServiceRoleForSupport</a>	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/>	<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor (Service-Linked Role)	-
<input type="checkbox"/>	<a href="#">s3crr_role_for_neel-replication</a>	AWS Service: s3	144 days ago
<input type="checkbox"/>	<a href="#">snowflake_connectivity</a>	Account: 627540493785	-

Buttons: Refresh, Delete, Create role

Click on AWS account and select 'this account' option.



aws Services Search [Alt+S] Global Neelesh Palaparthi

IAM > Roles > Create role

Step 1  
**Select trusted entity**

Step 2  
Add permissions

Step 3  
Name, review, and create

**Select trusted entity** [Info](#)

**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 (627540493785)**
- ☐ Another AWS account

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

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

00000

**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

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.

The screenshot shows the 'Add permissions' step in the AWS IAM console. The left sidebar indicates the current step is 'Add permissions'. The main area is titled 'Add permissions' and shows a search for 'S3' with 10 matches. A table lists several AWS managed policies, with 'AmazonS3FullAccess' selected. The table has columns for Policy name, Type, and Description.

	Policy name	Type	Description
<input type="checkbox"/>	s3curr_for_neel-replicati...	Custom...	
<input type="checkbox"/>	AmazonDMSRedshi...	AWS m...	Provides access to manage S3 settings for Redshift endpoints for DMS.
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS m...	Provides full access to all buckets via the AWS Management Console.
<input type="checkbox"/>	QuickSightAccessF...	AWS m...	Policy used by QuickSight team to access customer data produced by S3 Storage Management Analy...
<input type="checkbox"/>	AmazonS3ReadOnl...	AWS m...	Provides read only access to all buckets via the AWS Management Console.
<input type="checkbox"/>	AmazonS3Outposts...	AWS m...	Provides full access to Amazon S3 on Outposts via the AWS Management Console.
<input type="checkbox"/>	AWSBackupService...	AWS m...	Policy containing permissions necessary for AWS Backup to backup data in any S3 bucket. This inclu...

Write the role name and description.

The screenshot shows the 'Name, review, and create' step in the AWS IAM console. The left sidebar indicates the current step is 'Name, review, and create'. The main area is titled 'Name, review, and create' and shows the 'Role details' section. The 'Role name' field is filled with 'snowflake\_connectivity' and the 'Description' field is filled with 'Test'.

**Role details**

**Role name**  
Enter a meaningful name to identify this role.  
snowflake\_connectivity  
Maximum 64 characters. Use alphanumeric and '+', '@', '\_', '-' characters.

**Description**  
Add a short explanation for this role.  
Test  
Maximum 1000 characters. Use alphanumeric and '+', '@', '\_', '-' characters.

Don't change anything in the Json code.


Step 1: Select trusted entities

Edit

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": "sts:AssumeRole",  
7       "Principal": {  
8         "AWS": "627540493785"  
9       },  
10      "Condition": {  
11        "StringEquals": {  
12          "sts:ExternalId": "00000"  
13        }  
14      }  
15    }  
16  ]  
17 }
```

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.

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

-

Refresh

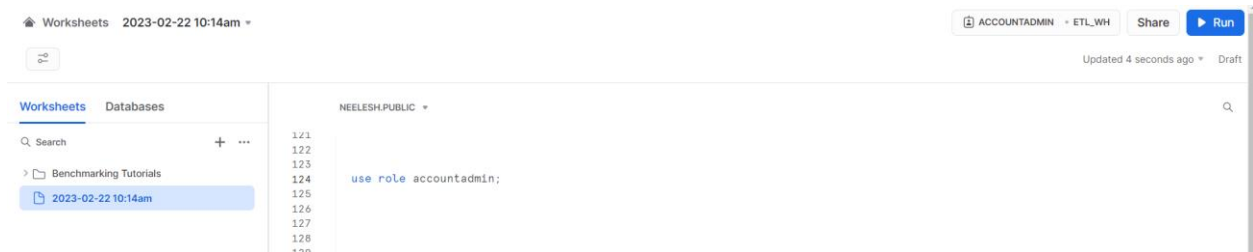
Delete

Create role

## Step 4:

### Integrating AWS with Snowflake:

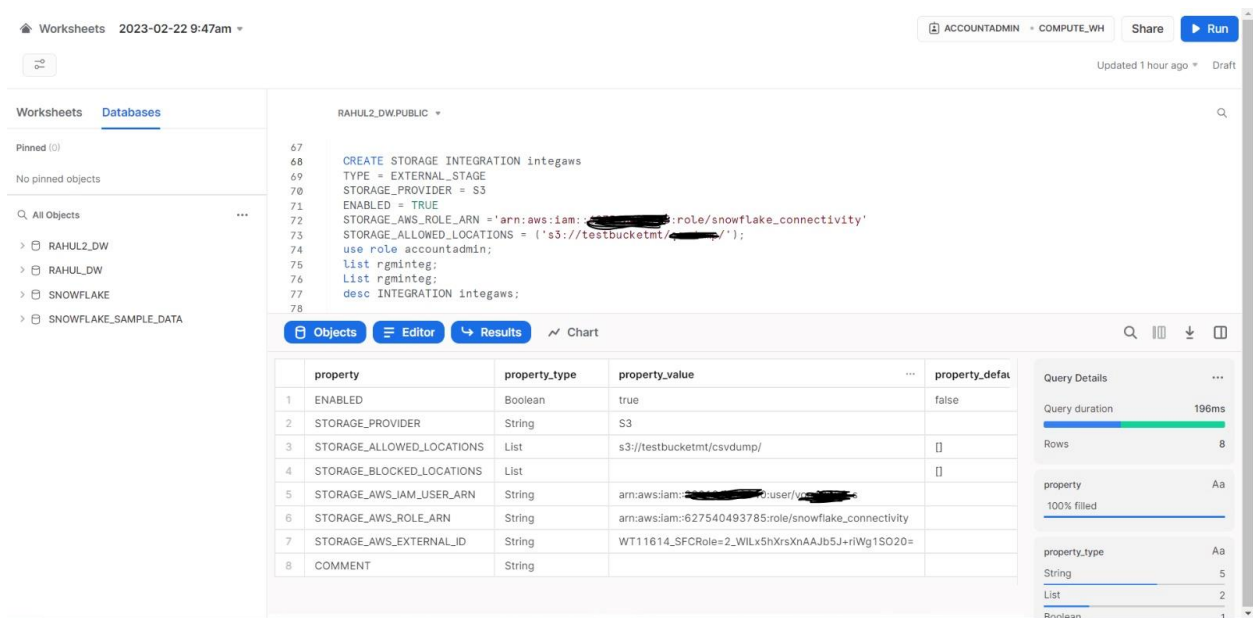
Open worksheet in snowflake and set role as account admin and run it.



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.

IAM > Roles > snowflake\_connectivity

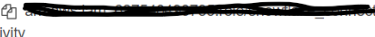
### snowflake\_connectivity

Test

Summary

Creation date  
February 23, 2023, 10:07 (UTC-06:00)

Last activity  
None

ARN  
  
ivity

Maximum session duration  
1 hour

Link to switch roles in console  
[https://signin.aws.amazon.com/switchrole?roleName=snowflake\\_connectivity&account=neelesh-awsv2](https://signin.aws.amazon.com/switchrole?roleName=snowflake_connectivity&account=neelesh-awsv2)

Permissions Trust relationships Tags Access Advisor Revoke sessions

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.










Amazon S3 > Buckets > testbucketmt

### testbucketmt


Objects Properties Permissions Metrics Management Access Points

Objects (1)

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](#)

  Copy S3 URI  Copy URL  Download  Open  Delete  Actions  Create folder  Upload

Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	 csvdump/	Folder	-	-	-