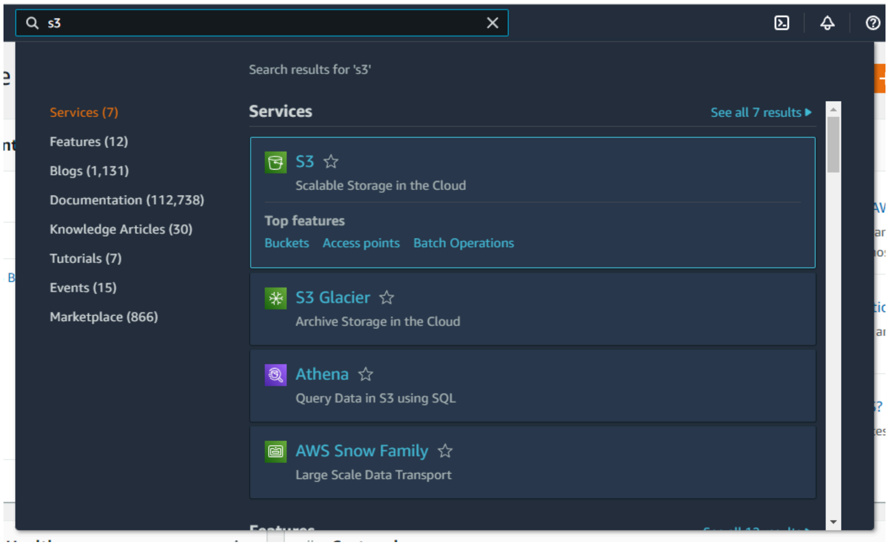
SNOWFLAKE CONTINUOUS DATA LOADING

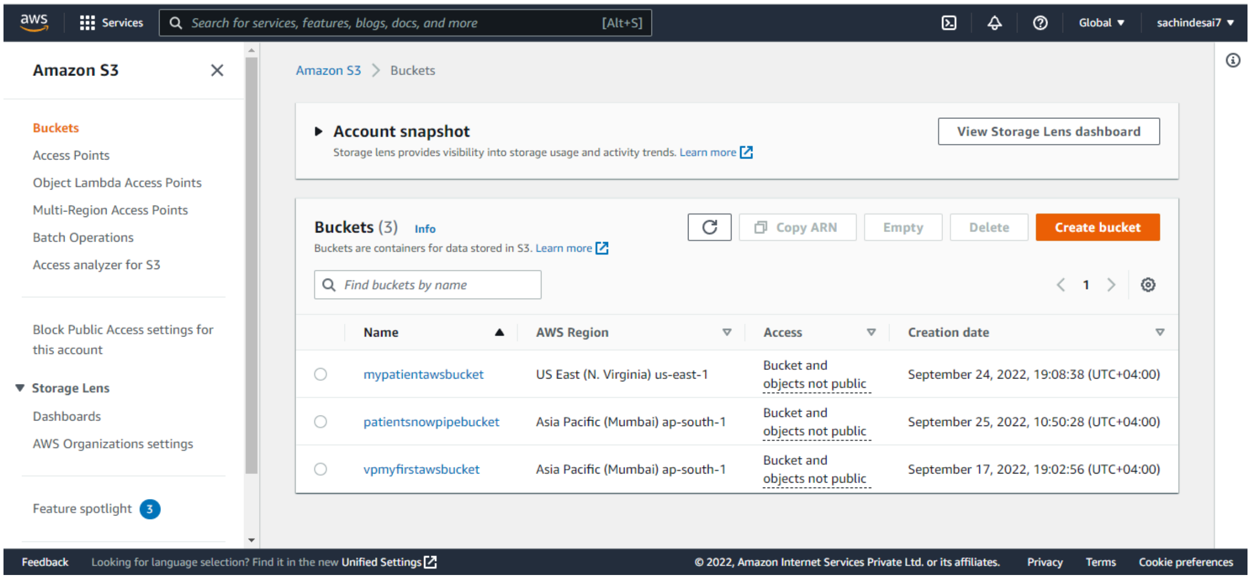
1]. Create an AWS account in aws.amazon.com

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


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
sachindesai7
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
Amazon S3 > Buckets
Account snapshot
View Storage Lens dashboard
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
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

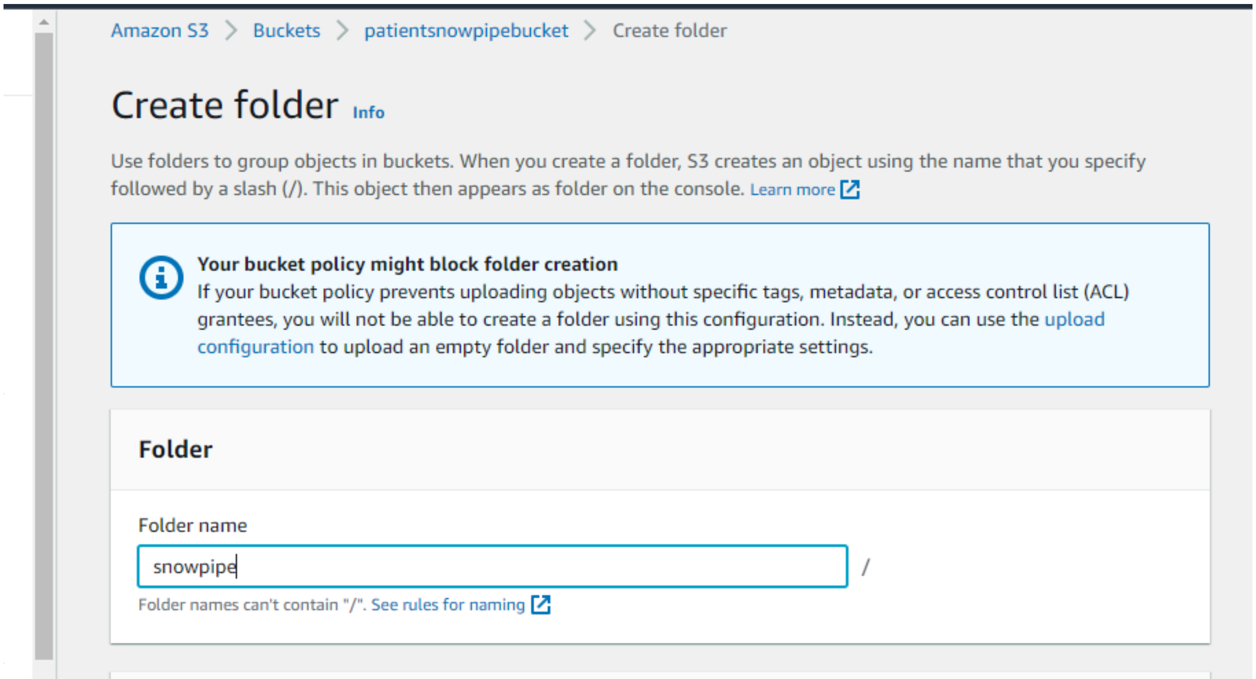
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (3) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	mypatientawsbucket	US East (N. Virginia) us-east-1	Bucket and objects not public	September 24, 2022, 19:08:38 (UTC+04:00)
○	patientsnowpipebucket	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	September 25, 2022, 10:50:28 (UTC+04:00)
○	vpmyfirstawsbucket	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	September 17, 2022, 19:02:56 (UTC+04:00)

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



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

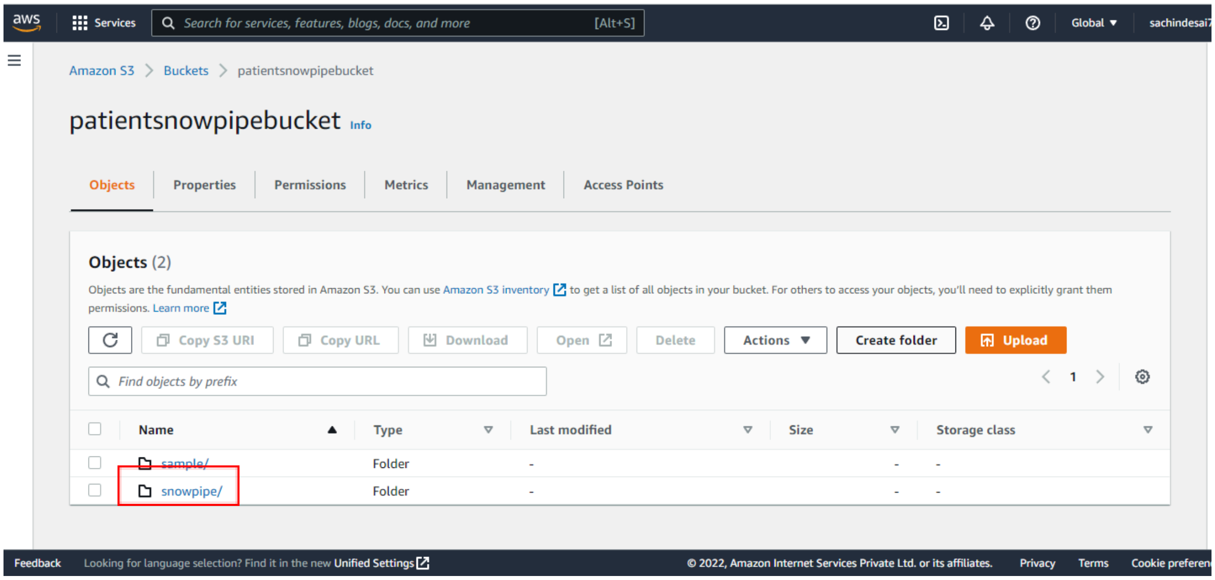
Your bucket policy might block folder creation
If your bucket policy prevents uploading objects without specific tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, you can use the upload configuration to upload an empty folder 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 ▼
sachindesai7
Amazon S3 > Buckets > patientsnowpipebucket

patientsnowpipebucket Info

Objects
Properties
Permissions
Metrics
Management
Access Points

Objects (2)

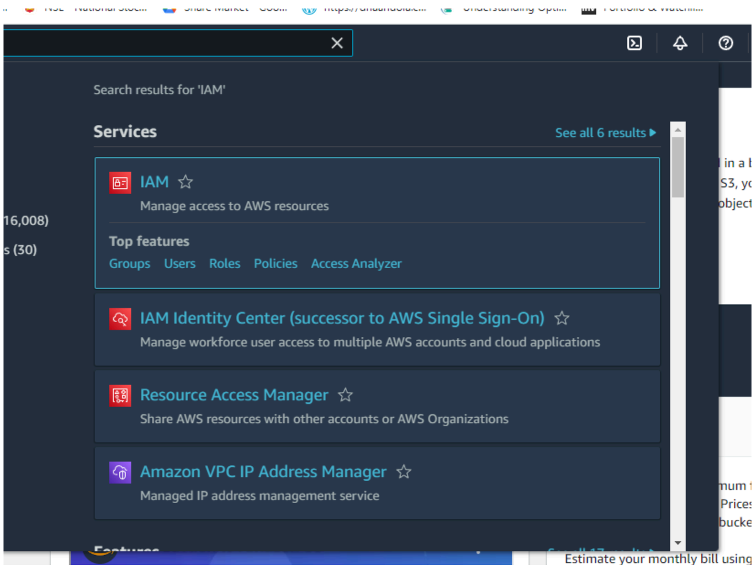
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Copy S3 URI
Copy URL
Download
Open
Delete
Actions ▼
Create folder
Upload
Find objects by prefix
1

□	Name ▲	Type	Last modified	Size	Storage class
□	sample/	Folder	-	-	-
□	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 preferen

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



Search results for 'IAM'

Services

See all 6 results ▸

IAM ☆
Manage access to AWS resources

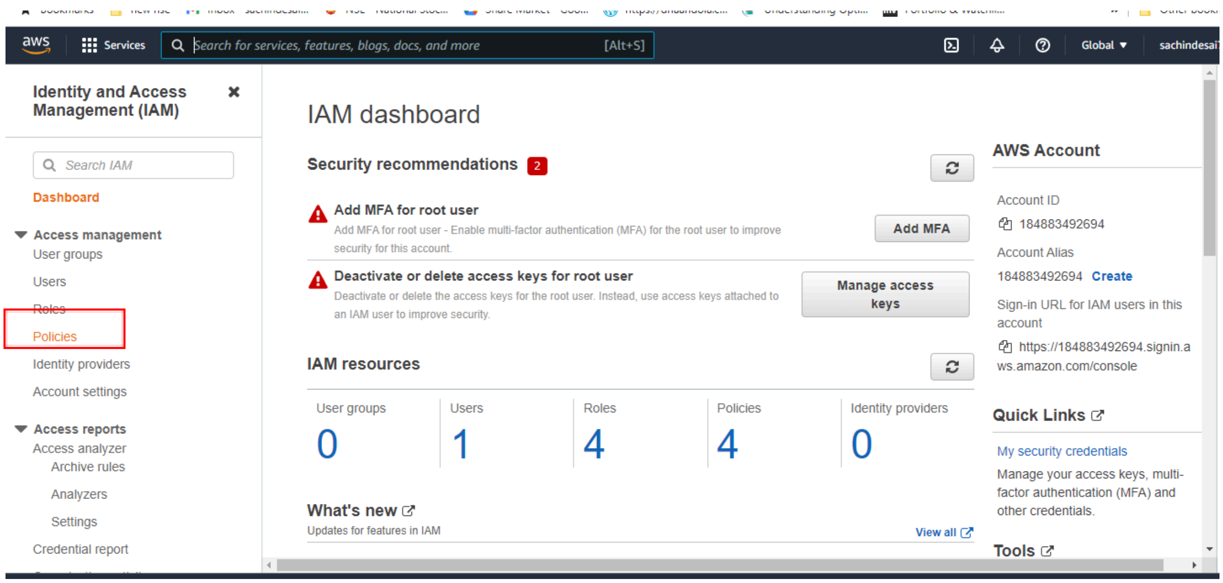
Top features
Groups Users Roles Policies Access Analyzer

IAM Identity Center (successor to AWS Single Sign-On) ☆
Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager ☆
Share AWS resources with other accounts or AWS Organizations

Amazon VPC IP Address Manager ☆
Managed IP address management service

7]. Click on the Policies from IAM Dashboard



IAM dashboard

Security recommendations 2

Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Add MFA

Deactivate or delete access keys for root user
Deactivate or delete the access keys for the root user. Instead, use access keys attached to an IAM user to improve security.

Manage access keys

IAM resources

User groups	Users	Roles	Policies	Identity providers
0	1	4	4	0

What's new
Updates for features in IAM

View all

AWS Account

Account ID
184883492694

Account Alias
184883492694 Create

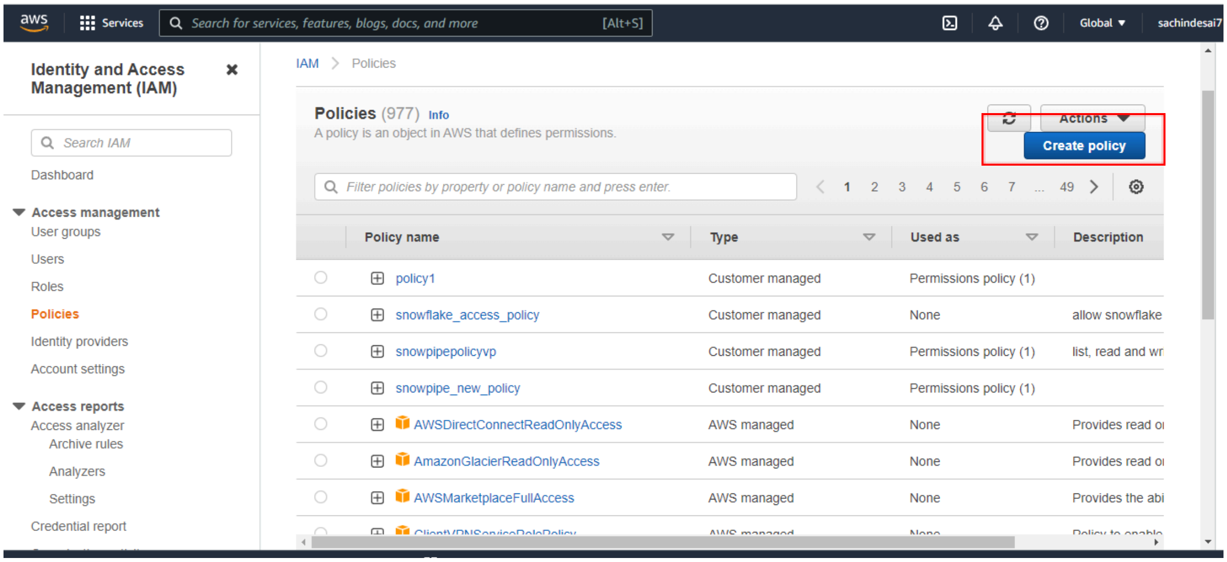
Sign-in URL for IAM users in this account
https://184883492694.signin.aws.amazon.com/console

Quick Links

My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

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



Policies (977) Info

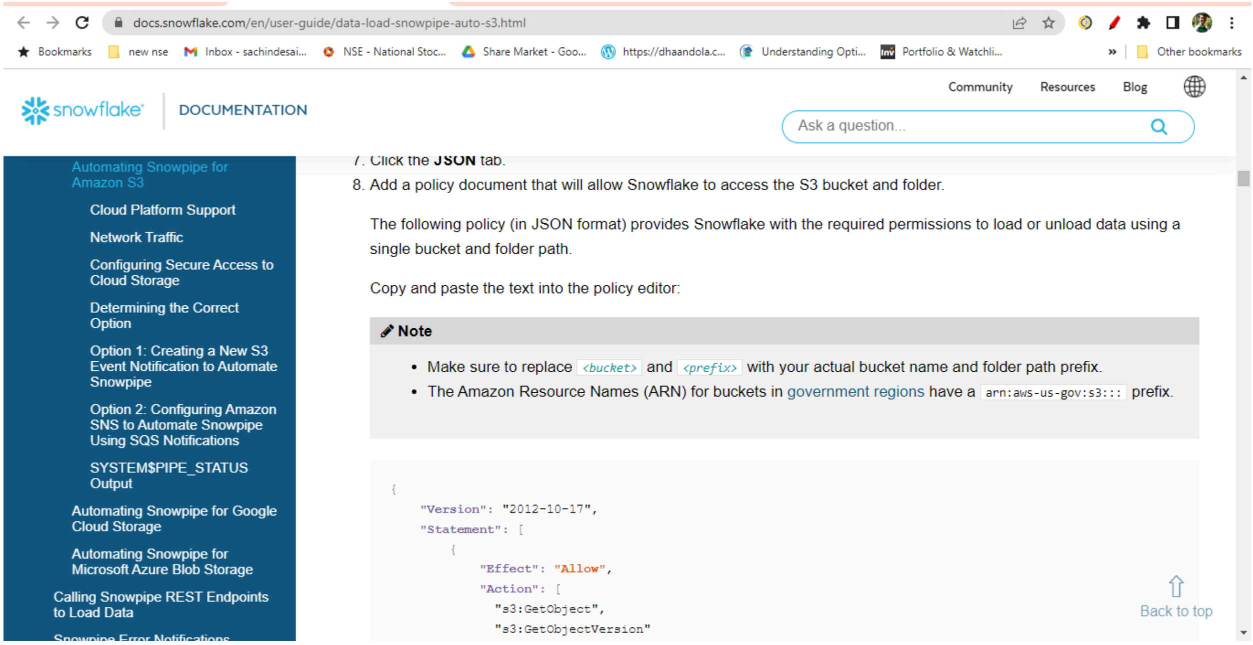
A policy is an object in AWS that defines permissions.

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
ClientVPNServiceRolePolicy	AWS managed	None	Policy to enable

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)


docs.snowflake.com/en/user-guide/data-load-snowpipe-auto-s3.html
Bookmarks
new nse
Inbox - sachindesai...
NSE - National Stoc...
Share Market - Goo...
https://dhaandola.c...
Understanding Opti...
Portfolio & Watchli...
Other bookmarks
snowflake
DOCUMENTATION
Community
Resources
Blog
Ask a question...
Automating Snowpipe for Amazon S3
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
Snowpipe Error Notifications
Back to top

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

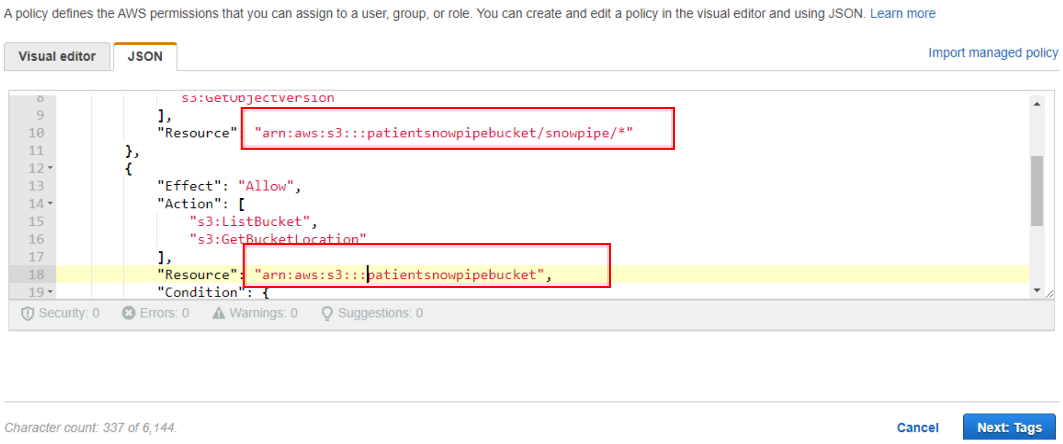
- Make sure to replace `<bucket>` and `<prefix>` with your actual bucket name and folder path prefix.
- The Amazon Resource Names (ARN) for buckets in government regions have a `arn:aws-us-gov:s3:::` prefix.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:GetObject",
              "s3:GetObjectVersion"
```

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

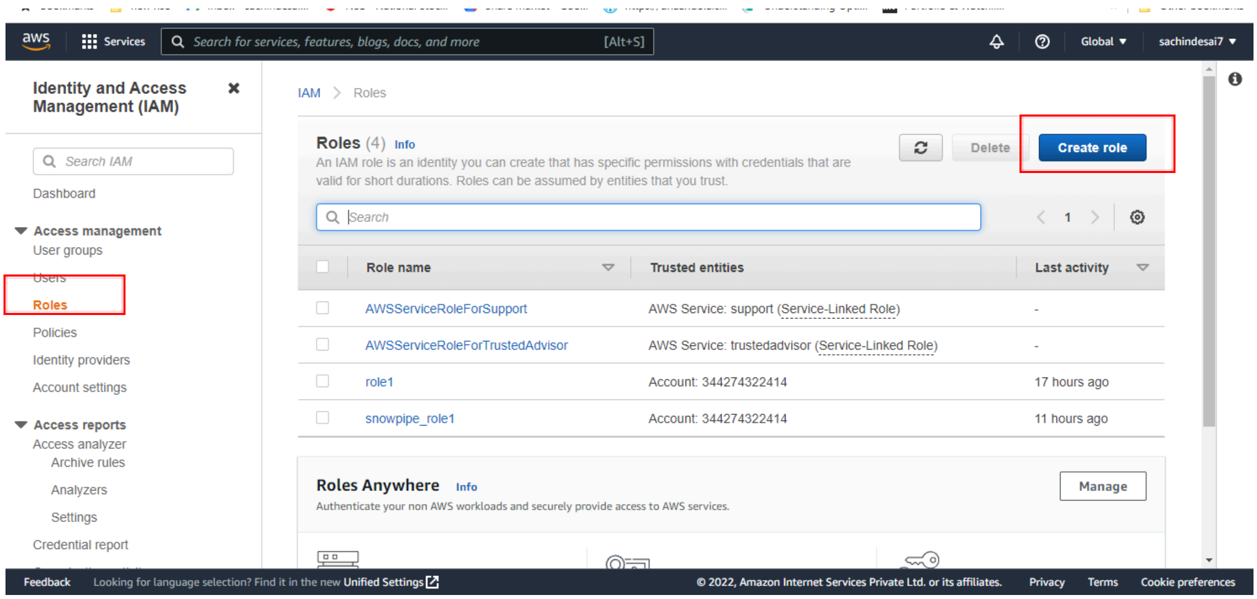
```
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::patientsnowpipebucket/snowpipe/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::patientsnowpipebucket",
            "Condition": {
```

Character count: 337 of 6,144.

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



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.

□	Role name	Trusted entities	Last activity
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
□	role1	Account: 344274322414	17 hours ago
□	snowpipe_role1	Account: 344274322414	11 hours ago

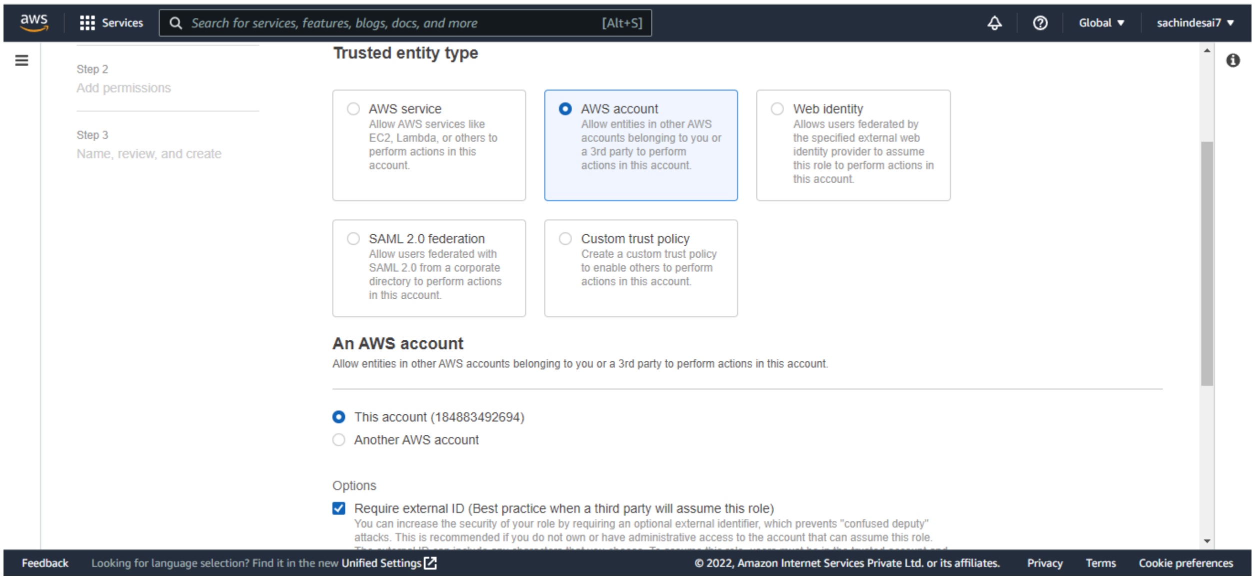
Roles Anywhere Info

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.



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.

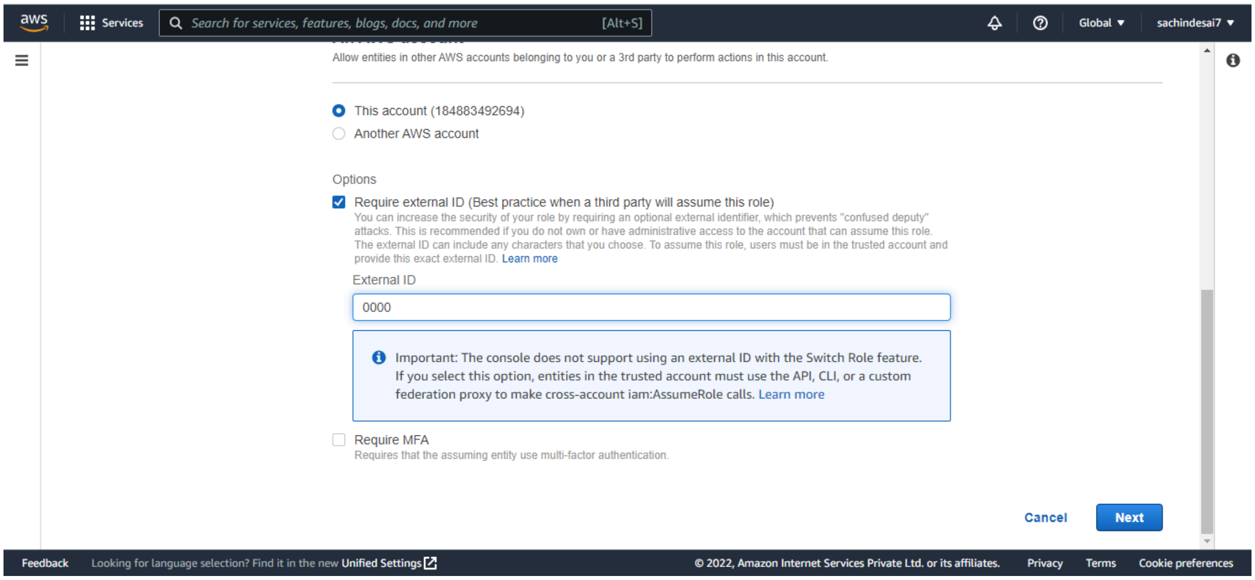
● This account (184883492694)
○ Another AWS account

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.

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

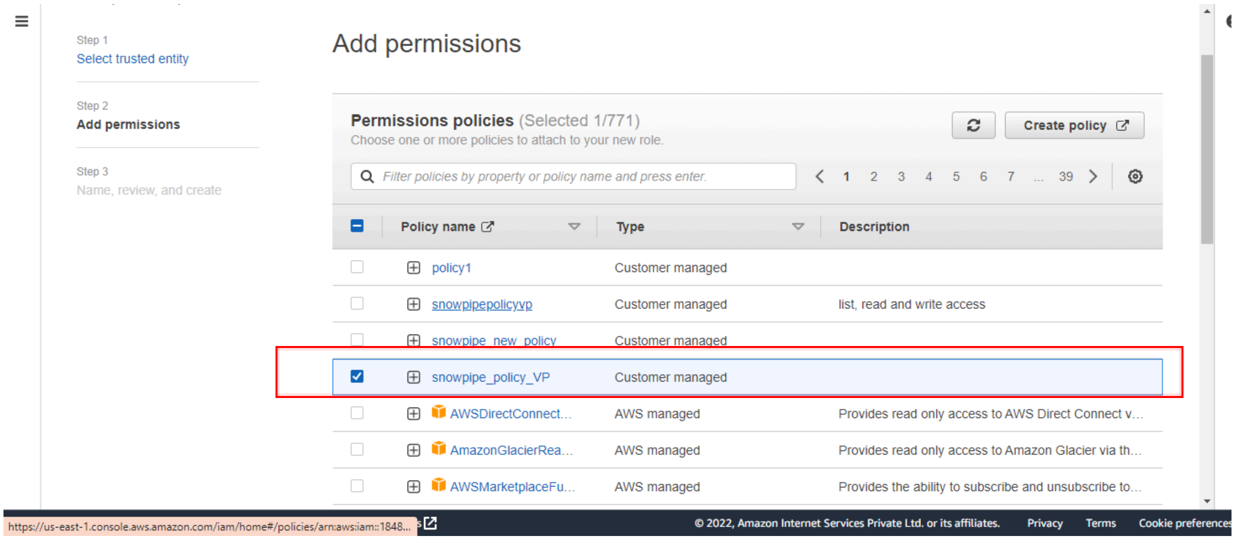
External ID
0000

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.

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



Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions

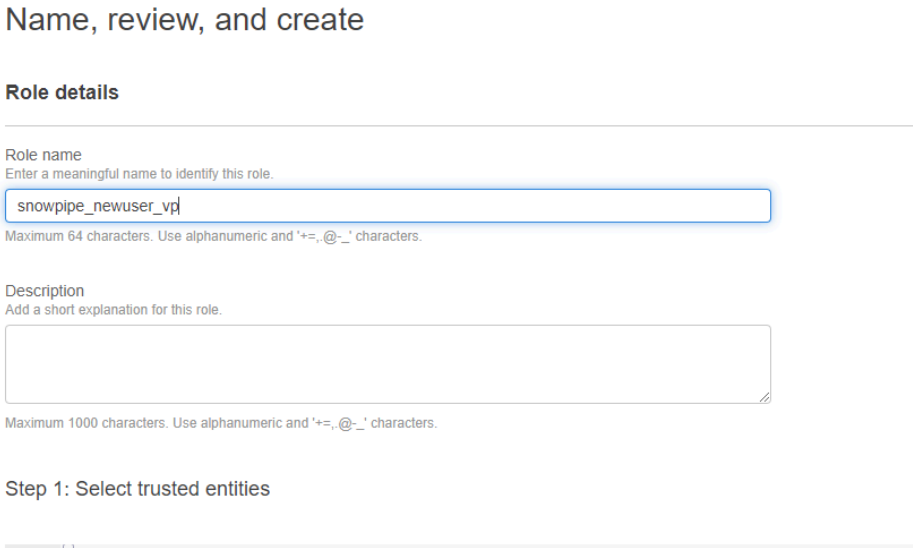
Permissions policies (Selected 1/771)
Choose one or more policies to attach to your new role.

☐	Policy name	Type	Description
☐	policy1	Customer managed	
☐	snowpipepolicyvp	Customer managed	list, read and write access
☐	snowpipe_new_policy	Customer managed	
☑	snowpipe_policy_VP	Customer managed	
☐	AWSDirectConnect...	AWS managed	Provides read only access to AWS Direct Connect v...
☐	AmazonGlacierRea...	AWS managed	Provides read only access to Amazon Glacier via th...
☐	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

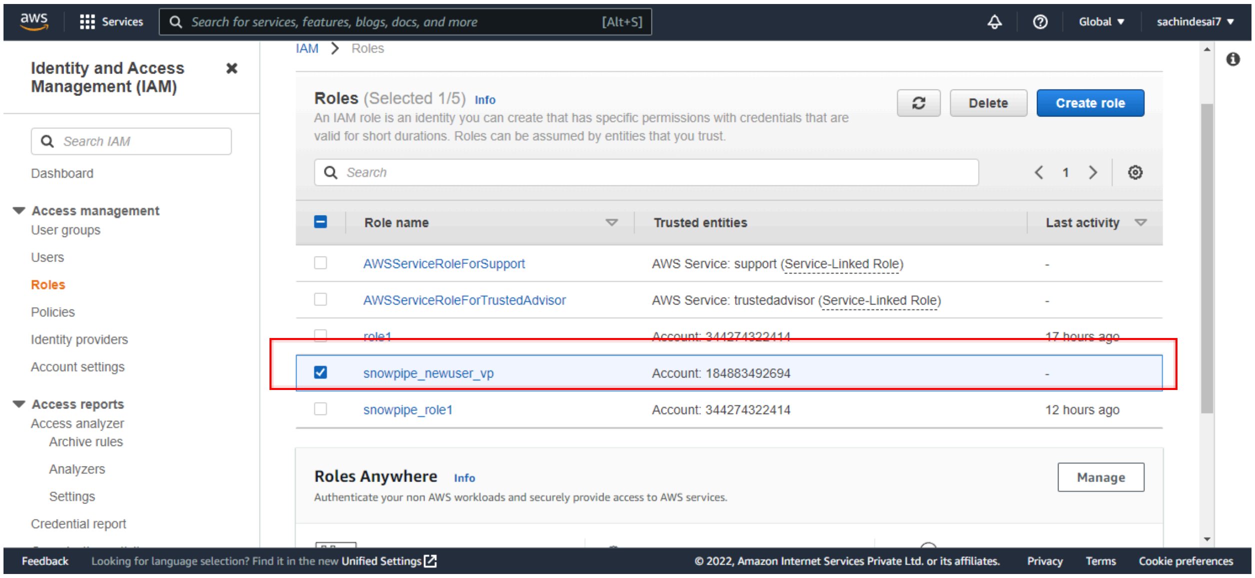
Role name
Enter a meaningful name to identify this role.
snowpipe_newuser_vp
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

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.



Roles (Selected 1/5) 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.

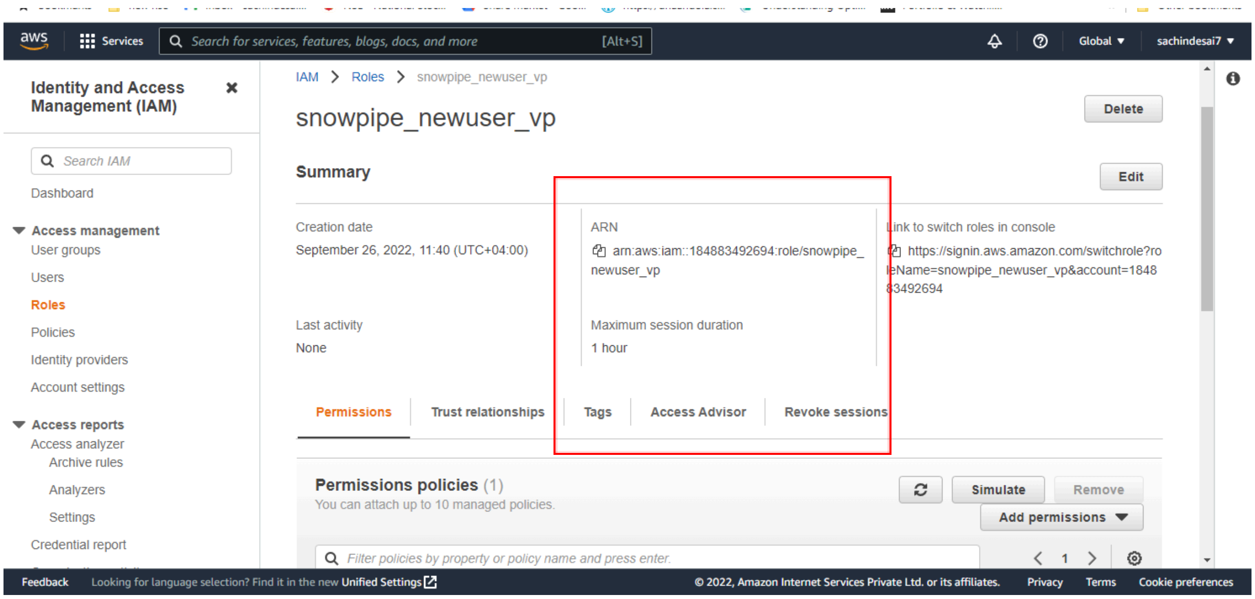
	Role name	Trusted entities	Last activity
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
□	role1	Account: 344274322414	17 hours ago
☑	snowpipe_newuser_vp	Account: 184883492694	-
□	snowpipe_role1	Account: 344274322414	12 hours ago

Roles Anywhere Info

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

You will get the following window

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



snowpipe_newuser_vp

Summary

Creation date
September 26, 2022, 11:40 (UTC+04:00)

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

Last activity
None

Maximum session duration
1 hour

Permissions policies (1)
You can attach up to 10 managed policies.

18]. Login to the Snowflake Account.

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

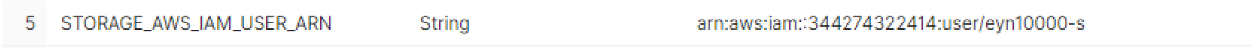
```
CREATE OR REPLACE STORAGE INTEGRATION snowpipe_integration
TYPE = external_stage
STORAGE_PROVIDER = s3
STORAGE_AWS_ROLE_ARN = 'arn:aws:iam::184883492694:role/snowpipe_newuser_vp'
ENABLED = true
STORAGE_ALLOWED_LOCATIONS = ('*');
```

19]. In Snowflake worksheet run command

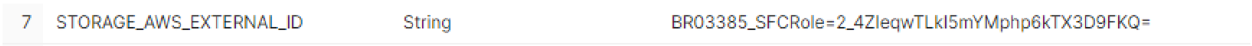
Desc integration integration_name;

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

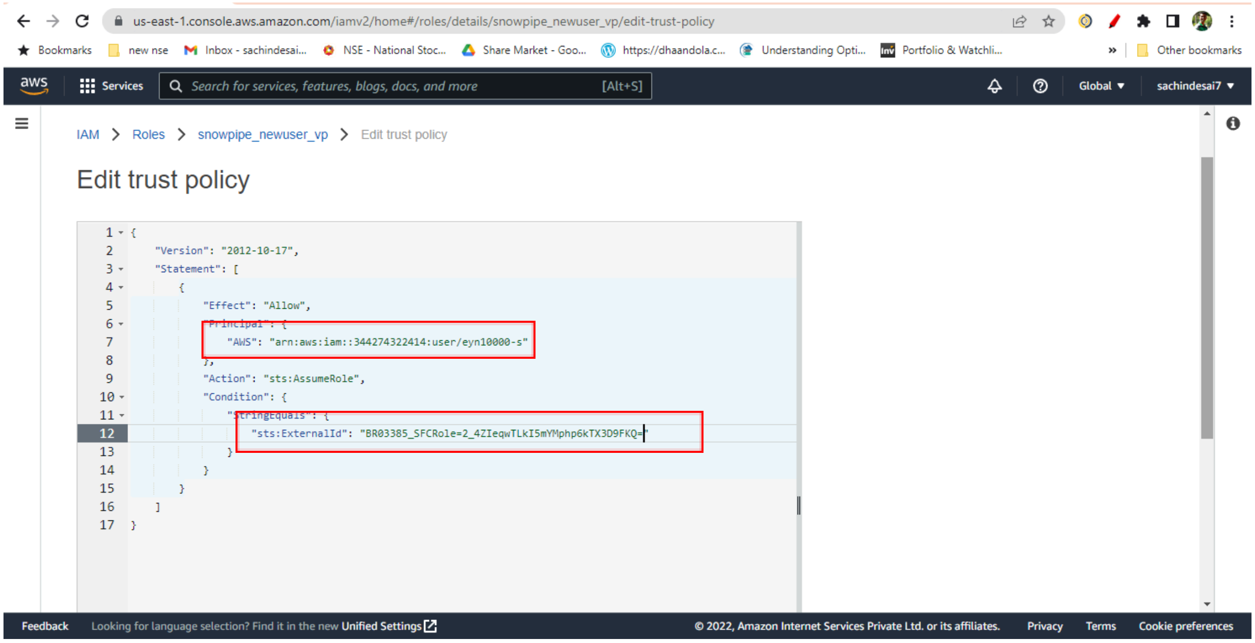
Select the role you created

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

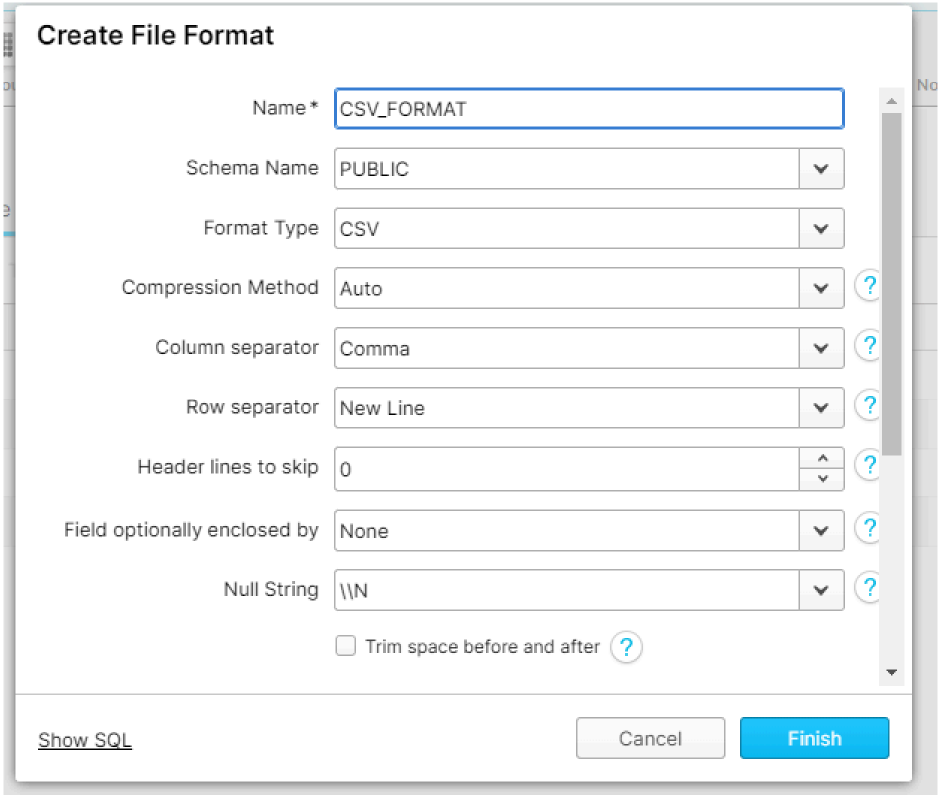


us-east-1.console.aws.amazon.com/iamv2/home#/roles/details/snowpipe_newuser_vp/edit-trust-policy
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
sachindesai7
IAM > Roles > snowpipe_newuser_vp > Edit trust policy
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

Edit trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::344274322414:user/eyn10000-s"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "BR03385_SFCRole=2_4ZIeqwTLkI5mYMphp6kTX3D9FKQ="
                }
            }
        }
    ]
}
```

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

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');
```

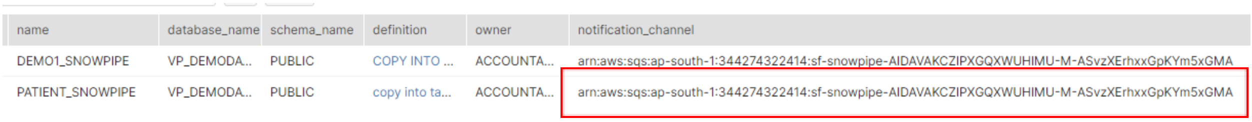
23]. Now Create auto-ingest pipe.

```
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

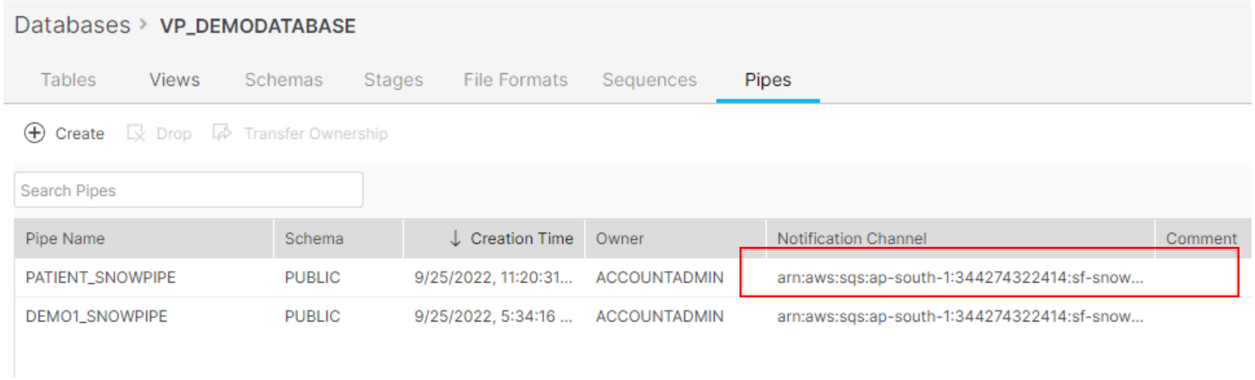
Show pipes;



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.

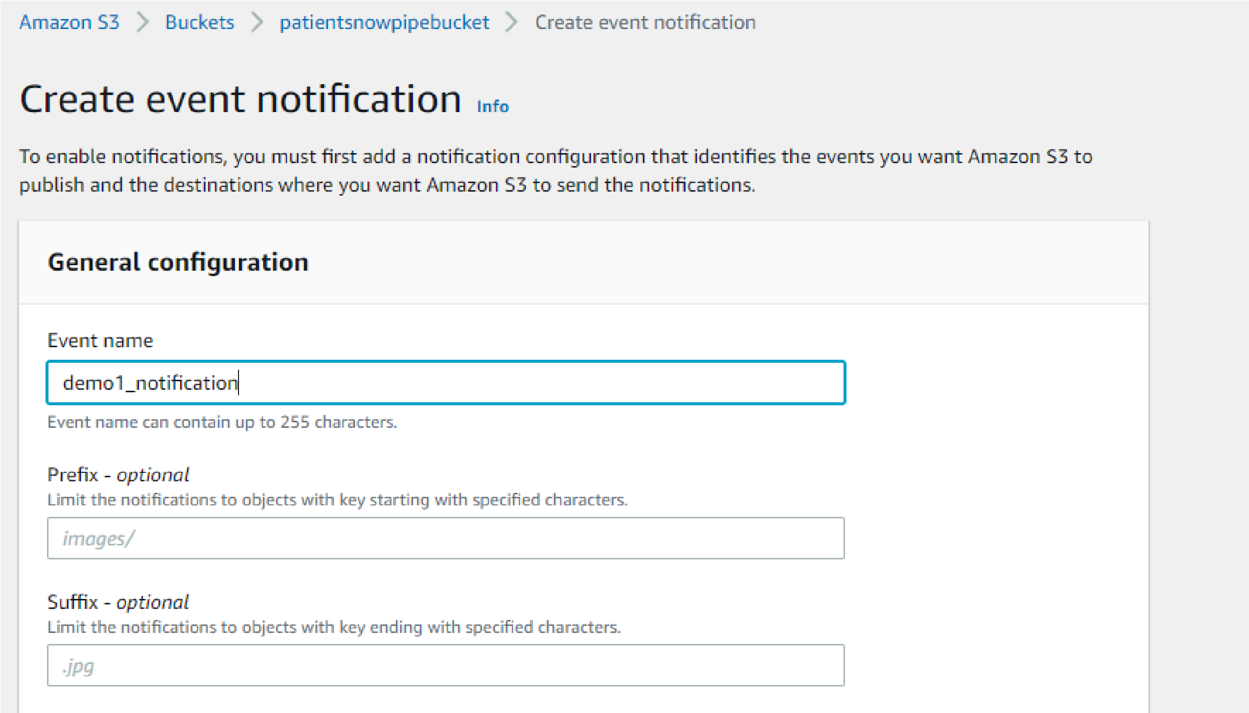


Pipe Name	Schema	↓ Creation Time	Owner	Notification Channel	Comment
PATIENT_SNOWPIPE	PUBLIC	9/25/2022, 11:20:31...	ACCOUNTADMIN	arn:aws:sqs:ap-south-1:344274322414:sf-snow...	
DEMO1_SNOWPIPE	PUBLIC	9/25/2022, 5:34:16 ...	ACCOUNTADMIN	arn:aws:sqs:ap-south-1:344274322414:sf-snow...	

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

demo1_notification

Event name can contain up to 255 characters.

Prefix - *optional*

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

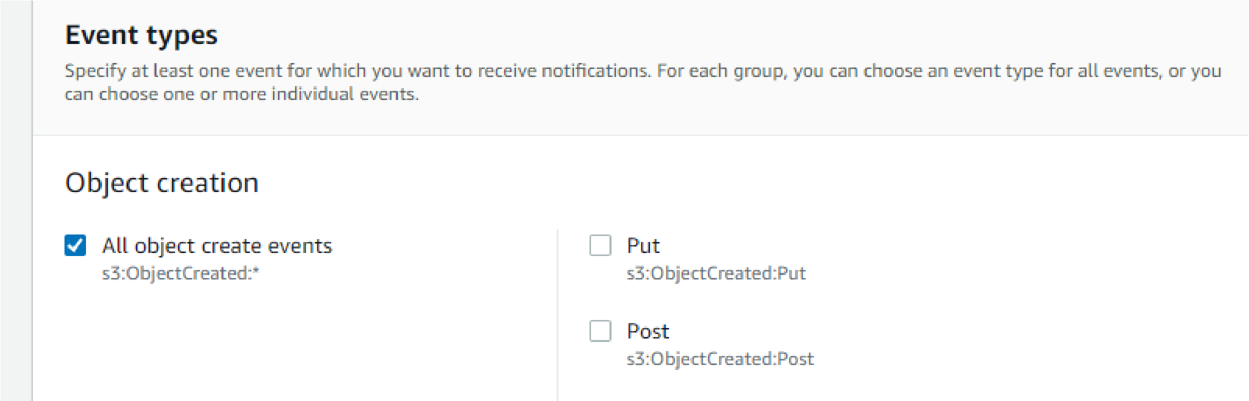
images/

Suffix - *optional*

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

.jpg

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

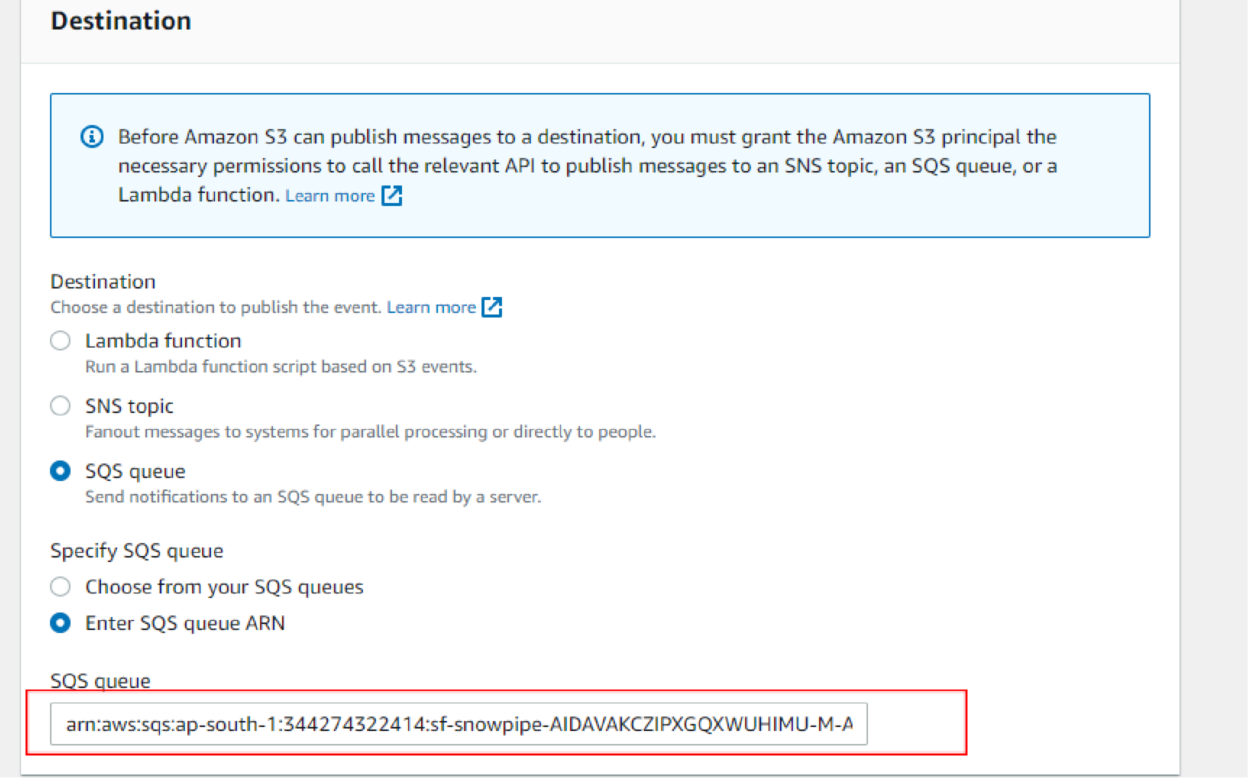
☑ All object create events
s3:ObjectCreated:*

☐ 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())));