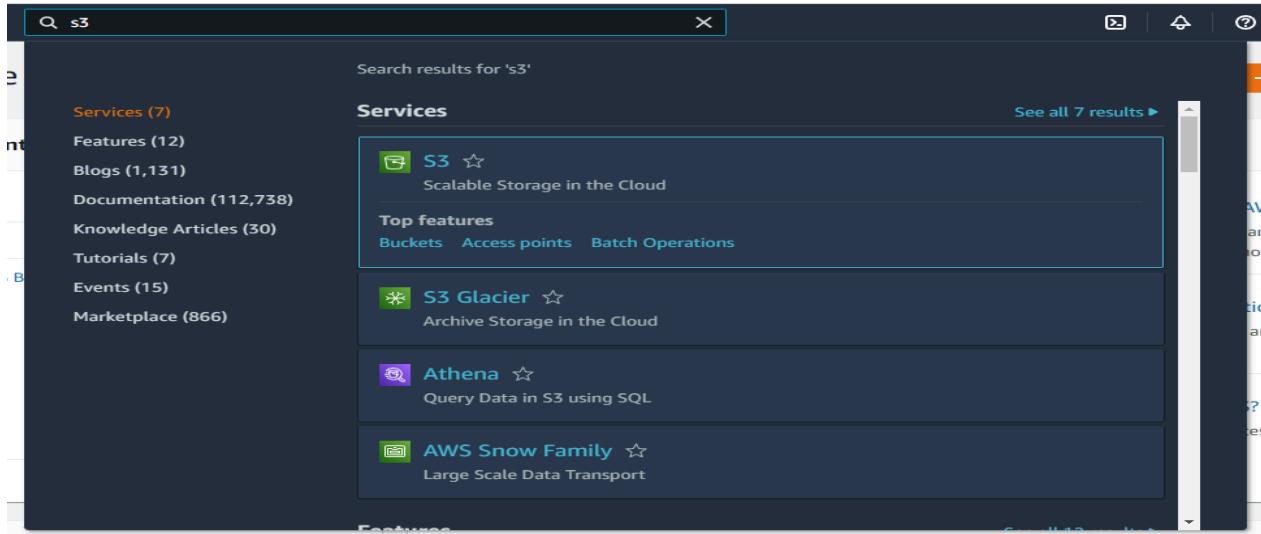


SNOWFLAKE CONTINUOUS DATA LOADING

- 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

A screenshot of the Amazon S3 Buckets page. The top navigation bar shows 'Amazon S3 > Buckets'. On the left, there is a sidebar with options like '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', and 'AWS Organizations settings'. The main content area displays an 'Account snapshot' section with a 'View Storage Lens dashboard' button. Below it is a table titled 'Buckets (3) Info' with a 'Create bucket' button. The table lists three buckets: 'mypatientawsbucket' (US East (N. Virginia) us-east-1), 'patientsnowpipebucket' (Asia Pacific (Mumbai) ap-south-1), and 'vpmyfirstawsbucket' (Asia Pacific (Mumbai) ap-south-1). Each row in the table includes columns for Name, AWS Region, Access, and Creation date.

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

Amazon S3 > Buckets > patientsnowpipebucket > Create folder

Amazon S3 > Buckets > patientsnowpipebucket

patientsnowpipebucket Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (2)

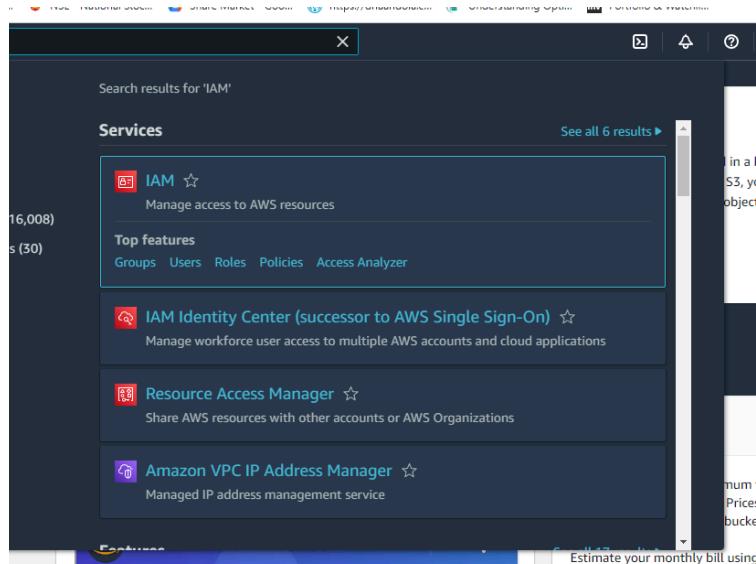
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

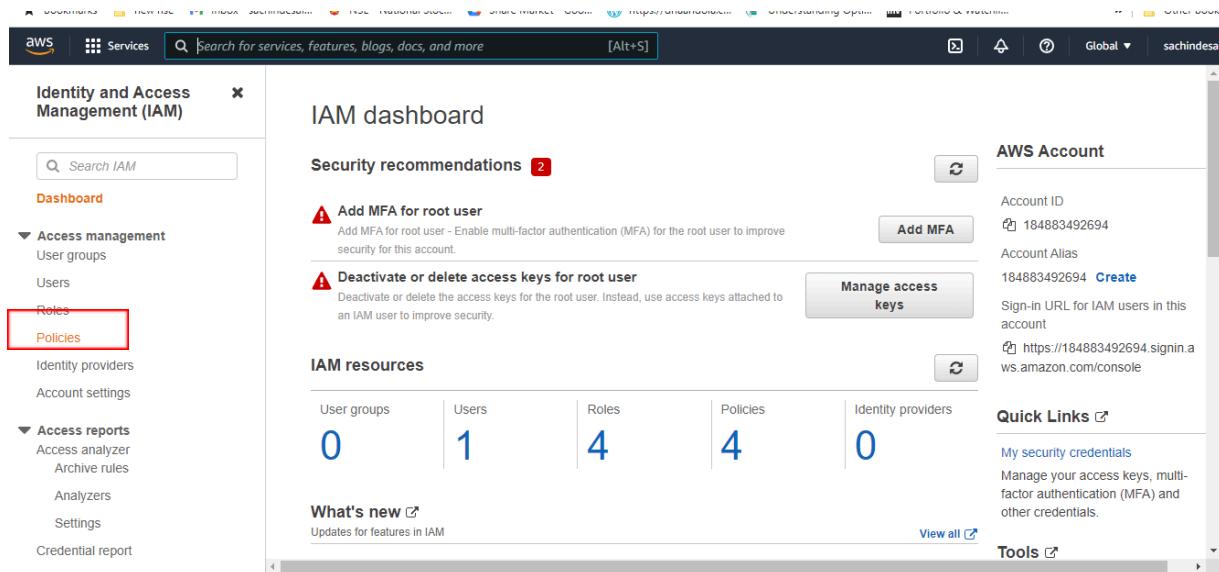
<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class	<input type="checkbox"/>
<input type="checkbox"/>	sample/	Folder	-	-	-	<input type="checkbox"/>
<input type="checkbox"/>	snowpipe/	Folder	-	-	-	<input type="checkbox"/>

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

The screenshot shows the AWS IAM Policies page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. The main area displays a table of policies. A red box highlights the 'Actions' dropdown menu and the 'Create policy' button at the top right of the table header. The table columns are 'Policy name', 'Type', 'Used as', and 'Description'. Some policies listed include 'policy1', 'snowflake_access_policy', 'snowpipepolicyvp', 'snowpipe_new_policy', and several AWS managed policies like 'AWSMarketplaceFullAccess'.

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)

The screenshot shows a browser window displaying the Snowflake documentation for 'Automating Snowpipe for Amazon S3'. The left sidebar has a navigation tree with items like 'Cloud Platform Support', 'Network Traffic', 'Configuring Secure Access to Cloud Storage', etc. The main content area has a heading '1. Click the JSON tab.' followed by instructions to add a policy document. Below this is a note section with a bullet list: 'Make sure to replace <bucket> and <prefix> with your actual bucket name and folder path prefix.' and 'The Amazon Resource Names (ARN) for buckets in government regions have a arn:aws-us-gov:s3::: prefix.' At the bottom, there's a code block containing a JSON policy document:

```
{
  "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](#)

The screenshot shows the AWS IAM Policy Editor interface. At the top, there are tabs for "Visual editor" and "JSON", with "JSON" being selected. Below the tabs, the policy document is displayed in JSON format. Two specific lines of the JSON code are highlighted with red boxes:

```
    "Effect": "Allow",  
    "Action": [  
        "s3>ListBucket",  
        "s3:GetBucketLocation"  
    ],  
    "Resource": "arn:aws:s3:::patientsnowpipebucket",  
    "Condition": {}
```

Below the JSON code, there are status indicators: Security: 0, Errors: 0, Warnings: 0, and Suggestions: 0. At the bottom right, there are buttons for "Cancel", "Next: Tags", and "Create policy".

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

The screenshot shows the AWS IAM Roles page. On the left, there is a navigation sidebar with "Identity and Access Management (IAM)" selected. Under "Access management", the "Roles" tab is selected, indicated by a red box. The main area displays a table of existing roles:

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

At the top right of the table header, there is a "Create role" button, which is also highlighted with a red box. Other buttons visible include "Search" and "Manage".

13]. Select AWS Account from Trusted Entity Type.

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

Trusted entity type

Step 2 Add permissions

Step 3 Name, review, and create

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.

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.

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.

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

The screenshot shows the 'Add permissions' step in the AWS IAM console. On the left, a sidebar lists three steps: Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). Step 2 is currently selected. The main area is titled 'Add permissions' and contains a table titled 'Permissions policies (Selected 1/771)'. The table has columns for Policy name, Type, and Description. One row is highlighted with a red border, indicating it is selected. The selected policy is 'snowpipe_policy_VP', which is Customer managed and provides read-only access to AWS Direct Connect. Other policies listed include 'policy1', 'snowpipepolicyvp', 'snowpipe_new_policy', 'AWSDirectConnect...', 'AmazonGlacierRea...', and 'AWSMarketplaceFu...'. A search bar at the top of the table allows filtering by policy name.

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.

The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with navigation links like Dashboard, User groups, Users, Roles (which is selected and highlighted in orange), Policies, Identity providers, Account settings, Access analyzer, Archive rules, Analyzers, Settings, and Credential report. The main content area shows a table of roles:

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

Below the table, there's a section titled "Roles Anywhere" with a "Manage" button. At the bottom of the page, there are links for Feedback, Unified Settings, Copyright notice (© 2022, Amazon Internet Services Private Ltd. or its affiliates.), Privacy, Terms, and Cookie preferences.

You will get the following window

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

The screenshot shows the AWS IAM Role details page for 'snowpipe_newuser_vp'. The left sidebar is identical to the previous screenshot. The main content area has a "Summary" section with fields like Creation date (September 26, 2022, 11:40 (UTC+04:00)), Last activity (None), ARN (arn:aws:iam::184883492694:role/snowpipe_newuser_vp), and Maximum session duration (1 hour). Below the summary, there are tabs for Permissions, Trust relationships, Tags, Access Advisor, and Revoke sessions. The "Permissions policies (1)" section shows a single policy attached. At the bottom, there are buttons for Simulate, Remove, and Add permissions. The ARN of the role is highlighted with a red box.

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_SFRole=2_4ZleqwTLki5mYMphp6kTX3D9FKQ=

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]

IAM > Roles > snowpipe_newuser_vp > Edit trust policy

Edit trust policy

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Principal": "$",  
7             "ARN": "arn:aws:iam::344274322414:user/eyn10000-s"  
8         },  
9         {  
10            "Action": "sts:AssumeRole",  
11            "Condition": {  
12                "StringEquals": {  
13                    "sts:ExternalId": "BR03385_SFCRole=2_4ZIeqwTlkI5mYmpb6kTX3D9FKQ+"  
14                }  
15            }  
16        }  
17    ]
```

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

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.

The screenshot shows the 'Create event notification' page in the Amazon S3 console. At the top, the navigation path is: Amazon S3 > Buckets > patientsnowpipebucket > Create event notification. The main title is 'Create event notification'. Below it, a sub-instruction reads: '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.' A 'General configuration' section is shown, containing fields for 'Event name' (set to 'demo1_notification'), 'Prefix - optional' (set to 'images/'), and 'Suffix - optional' (set to '.jpg').

Check All Object create Events

The screenshot shows the 'Event types' configuration page. It instructs the user to '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.' Under the 'Object creation' section, there are three checkboxes: 'All object create events s3:ObjectCreated:' (checked), 'Put s3:ObjectCreated:Put' (unchecked), and 'Post s3:ObjectCreated:Post' (unchecked).

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())));
```