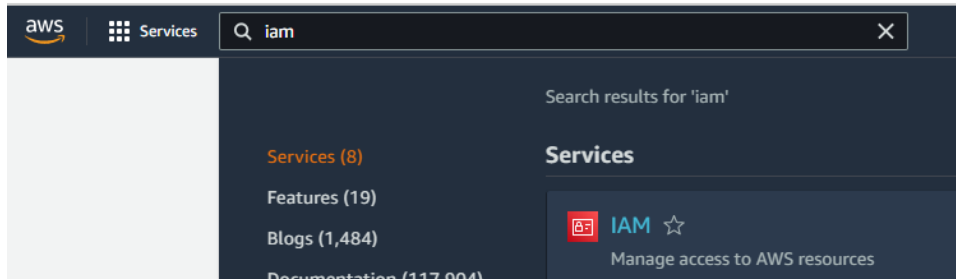


AWS IAM very important administration tool, but every developer aware of it.



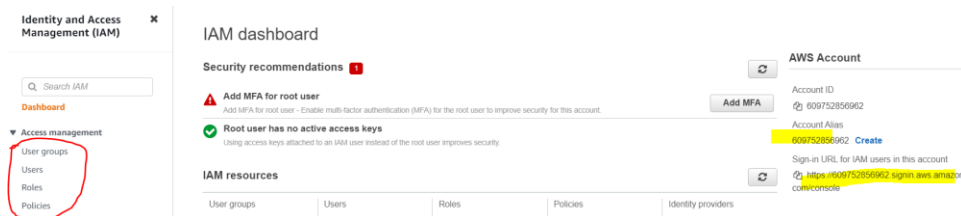
Every developer must aware these 4 services

**User groups:** it's used to assign privileges in the form of policies.

**Users:** It's fundamental component used to do anything (key pairs very important)

**IAM roles:** Very important, if u want to access aws service to another aws service use IAM roles.

**Policies:** Fundamental privileges in the form of policies.



Now right side highlighted account alias and below something URL available, it's very important.

I think u noticed when u r login, it's showing IAM 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](#)



## 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](#)

### Account ID (12 digits) or account alias

Next

By continuing, you agree to the [AWS Customer](#)

You noticed if u choose IAM user it asked 12 digits number ( you have to enter here). If you don't want this number you can rename this using **Create** button



## AWS Account



Account ID

609752856962

Account Alias

609752856962 **Create**



Sign-in URL for IAM users in this account

<https://609752856962.signin.aws.amazon.com/console>

## Quick Links

[My security credentials](#)

ions 1

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

Use

0

3 wi

to create session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs

**Create alias for AWS account 609752856962** ✕

Preferred alias

Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL

<https://pysparkpoc2023.signin.aws.amazon.com/console>

**IAM users will still be able to use the default URL containing the AWS account ID.**

Cancel **Save changes**

starting in April

**AWS Account**

Account ID

609752856962

Account Alias

609752856962 **Create**

Sign-in URL for IAM users in this account

<https://609752856962.signin.aws.amazon.com/console>

**Quick Links**

[My security credentials](#)

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

**Tools**

[Policy simulator](#)

The simulator evaluates the policies that you

## AWS Account

Account ID

609752856962

Account Alias

pysparkpoc2023 [Edit](#) | [Delete](#)

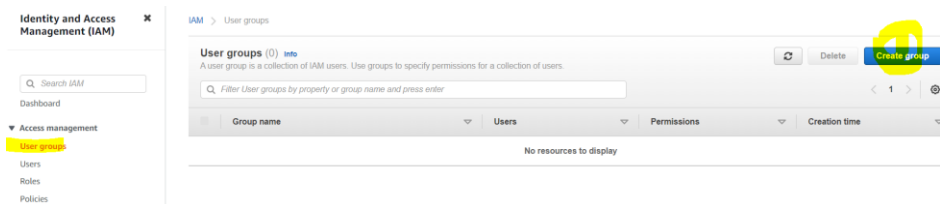
Sign-in URL for IAM users in this account

<https://pysparkpoc2023.signin.aws.amazon.com/console>

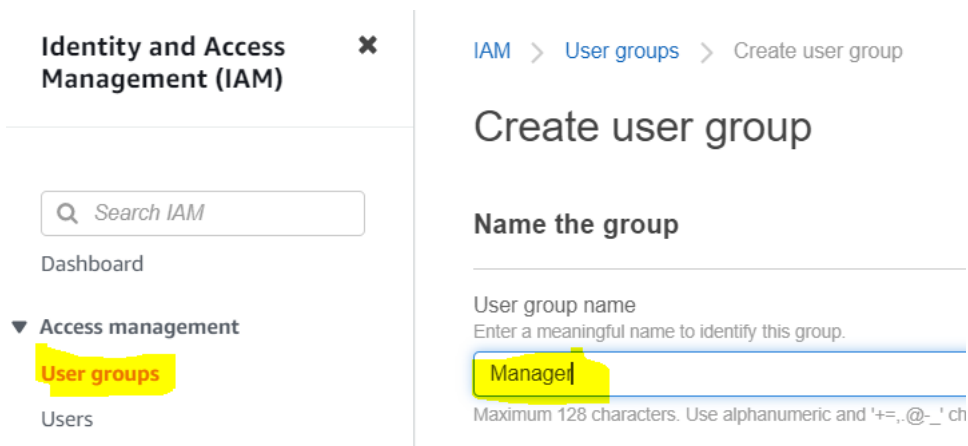
## Quick Links

In ur office 90% ur logging like this only.

## IAM User Groups



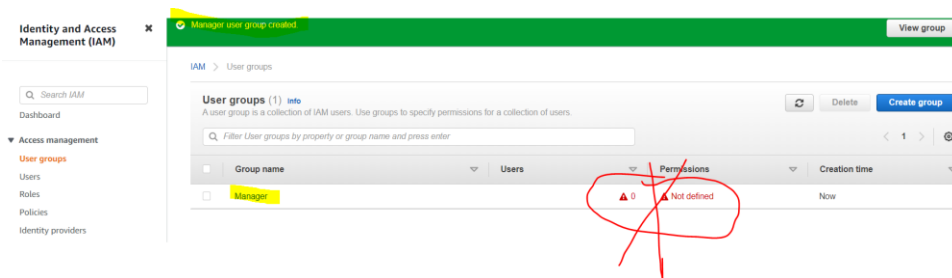
Create Group ... specify any name like “manager”



Scroll down click “create group”



Don't worry this red color highlighted things, “manager” group created. Click Manager group



Now Click on Permission tab Click on Add permission Click **Attach Policy**



Now Click on **AmazonS3FullAccess**. It means who (users) is in manager group they will get S3 full privileges. Similarly Ec2 also.

**Other permission policies (Selected 1/817)**  
You can attach up to 10 managed policies to this user group. All of the attached permissions.

Filter policies by property or policy name and press enter

"s3" X Clear filters

Policy name

- ☐ AWSGlueServiceRole-aug8glues3full
- ☐ AWSGlueServiceRole-awss3glue
- ☐ AWSGlueServiceRole-glueAccessS3
- ☐ AWSGlueServiceRole-GlueS3Full
- ☐ AWSGlueServiceRole-GlueS3role
- ☐ AWSQuickSightS3Policy
- ☐ AmazonDMSRedshiftS3Role
- ☒ AmazonS3FullAccess

**Other permission policies (Selected 2/817)**  
You can attach up to 10 managed policies to this user group. All of the attached permissions.

Filter policies by property or policy name and press enter

"RDS" X Clear filters

Policy name

- ☐ AWSQuickSightRDSPolicy
- ☒ AmazonRDSFullAccess
- ☐ AmazonRDSDirectoryServiceAccess

Similarly assign RDS also pls assign.

Similarly EC2 full privileges

**Other permission policies (Selected 3/817)**  
You can attach up to 10 managed policies to this user group. All of the attached permissions.

Filter policies by property or policy name and press enter

"ec2" X Clear filters

Policy name

- ☒ AmazonEC2FullAccess
- ☐ AmazonEC2RoleforSSM

Cancel Add permissions

Finally Click on Add permission

Now who is in this manager group they ll get **S3 full, Ec2 full, RDS full privileges.**

IAM > User groups > Manager

## Manager

### Summary

User group name

Manager

Users

Permissions


Access Advisor


#### Permissions policies (3) [Info](#)

You can attach up to 10 managed policies.

Filter policies by property or policy name and p

☐ Policy name [↗](#)

☒ [+](#)  AmazonRDSFullAccess

☐ [+](#)  AmazonEC2FullAccess

☐ [+](#)  AmazonS3FullAccess

Ofcourse you can revoke privileges as well like hilighted one. (Check appropriate privileges, Click Remove)

IAM > User groups > Manager

## Manager

### Summary

User group name

Manager

Creation time

January 11, 2023, 20:24 (UTC+05:30)

ARN

[↗](#) arn:aws:iam:609752856962:group/M

Users

Permissions

Access Advisor

#### Permissions policies (3) [Info](#)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.



Simulate

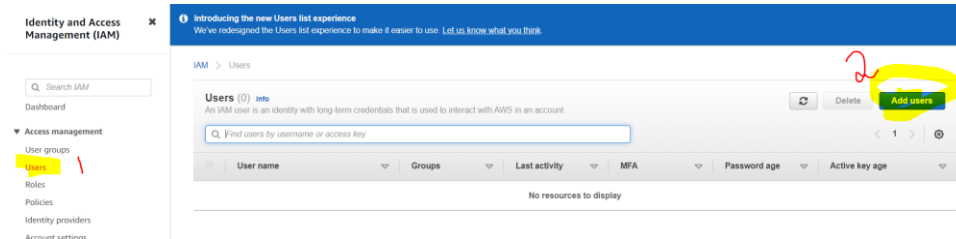
Remove

[A](#)

<input type="checkbox"/>	Policy name <a href="#">↗</a>	Type	Description
<input type="checkbox"/>	<a href="#">+</a>  AmazonRDSFullAccess	AWS managed	Provides full access to
<input type="checkbox"/>	<a href="#">+</a>  AmazonEC2FullAccess	AWS managed	Provides full access to
<input checked="" type="checkbox"/>	<a href="#">+</a>  AmazonS3FullAccess	AWS managed	Provides full access to

# IAM Users

Now explaining Users:



## Add user

1 2 3 4 5

### Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name  ✕

✕

+ Add another user

### Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Select AWS credential type\*
- ☒ Access key - Programmatic access  
Enables an **access key** ID and **secret access key** for the AWS API, CLI, SDK, and other development tools.
  - ☒ Password - AWS Management Console access  
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password\* ☐ Autogenerated password  
☒ Custom password

✕

☒ Show password

Require password reset ☒ Users must create a new password at next sign-in

\* Required

Cancel

Next: Permissions


Next





## Add user

1 2 3 4 5

### Set permissions

 Add users to group

 Copy permissions from existing user

 Attach existing policies directly

Add users to an existing group or create a new one. Using groups is a best-practice way to manage users' permissions by job functions. [Learn more](#)

### Add user to group

Create group Refresh

Q Search		Showing 1 result
Group	Attached policies	
<input checked="" type="checkbox"/> Manager	AmazonEC2FullAccess and 2 more	

### Set permissions boundary

Cancel Previous Next: Tags

## Next 3<sup>rd</sup> and 4<sup>th</sup> step optional

## Add user

1 2 3 4 5

### Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 50 more tags.

Cancel Previous Next: Review

## This step also (4<sup>th</sup> step) optional

## Add user



### Review

Review your choices. After you create the users, you can view and download autogenerated passwords and access keys.

#### User details

User names	venu and sita
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

#### Permissions summary

The users shown above will be added to the following groups.

Type	Name
Group	<a href="#">Manager</a>
Managed policy	<a href="#">IAMUserChangePassword</a>

#### Tags

[Cancel](#) [Previous](#) [Create users](#)

## Must download keys

### Add user



#### Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://pysparkpoc2023.signin.aws.amazon.com/console>

[Download .csv](#)

	User	Access key ID	Secret access key	Email login instructions
▶	venu	<del>AKIAI44QH8DHBQK3TRH49</del>	***** <a href="#">Show</a>	Send email <a href="#">↗</a>
▶	sita	<del>AKIAI44QH8DHBQK3TRH49</del>	***** <a href="#">Show</a>	Send email <a href="#">↗</a>

These keys very important Don't share these keys to anyone

Now above 2 users are members in Manager group.

#### Access management

User groups

**Users**

Roles

Policies

Identity providers

Account settings

#### Access reports

#### Users (2) Info

An IAM user is an identity with long-term credentials that is used to interact with /

Find users by username or access key

<input type="checkbox"/>	User name	Groups
<input type="checkbox"/>	sita	<a href="#">Manager</a>
<input type="checkbox"/>	venu	<a href="#">Manager</a>

Means they have full privileges to access S3, ec2, and RDS

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

IAM > User groups > Manager

## Manager

### Summary

User group name  
Manager

Users | **Permissions** | Access Advisor

#### Permissions policies (3) Info

You can attach up to 10 managed policies.

Filter policies by property or policy name and

<input type="checkbox"/>	Policy name
<input type="checkbox"/>	AmazonRDSFullAccess
<input type="checkbox"/>	AmazonEC2FullAccess
<input type="checkbox"/>	AmazonS3FullAccess

In future you can add and remove new/existing users like this. Just click on person name's check box and click Remove users.

Similarly to add .. click add users and add new users same way

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

IAM > User groups > Manager

## Manager

Summary

User group name  
Manager

Creation time  
January 11, 2024 (UTC+05:30)

ARN  
arn:aws:iam::609752856962:group/Manager

Users | **Permissions** | Access Advisor

#### Users in this group (Selected 1/2)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Remove users Add users

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input checked="" type="checkbox"/>	sda	1	None	5 minutes ago
<input type="checkbox"/>	venu	1	None	5 minutes ago

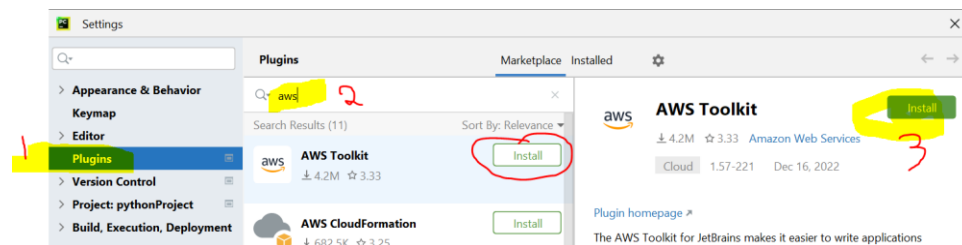
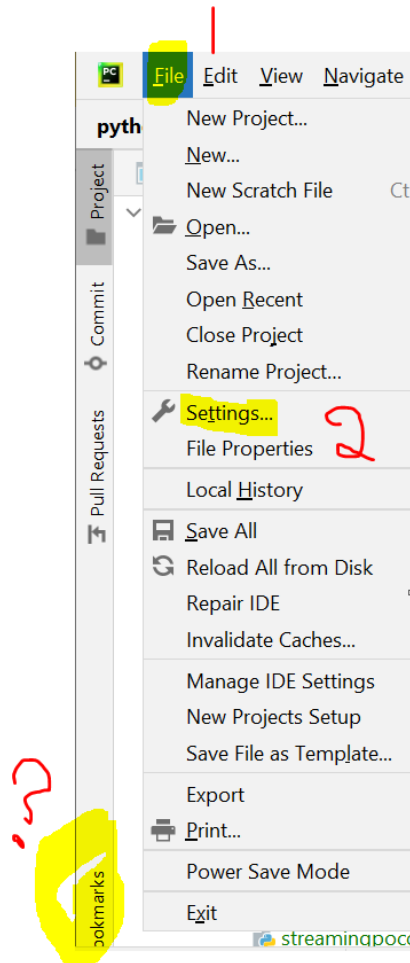
How to Access these IAM user credentials

Let eg:

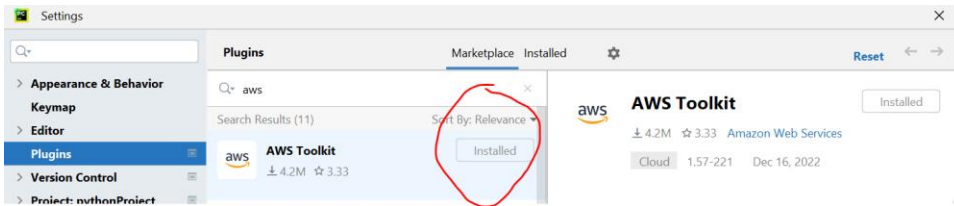
U want to access S3 from PyCharm or IntelliJ (3<sup>rd</sup> party tool) .. use these iam keys.

Now check Pycharm left side There is no aws access tab ...

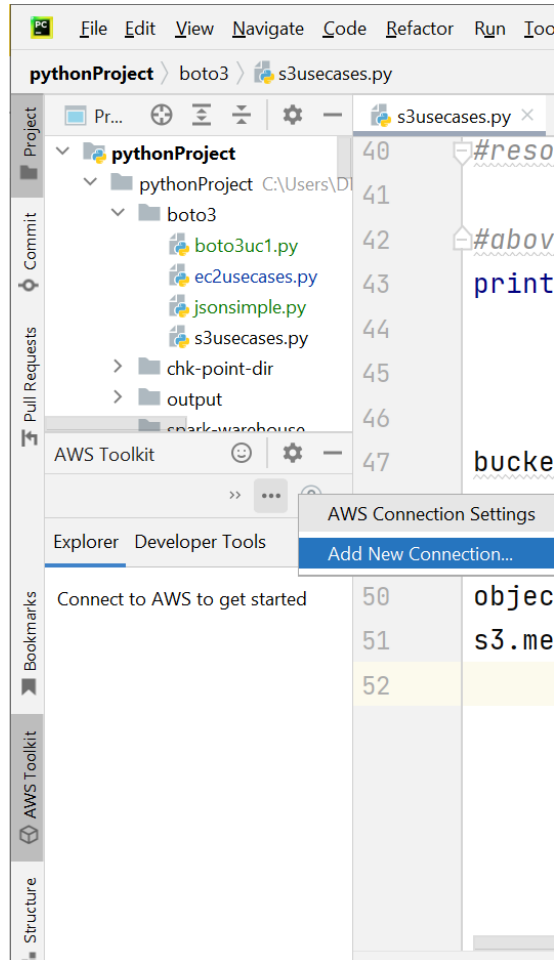
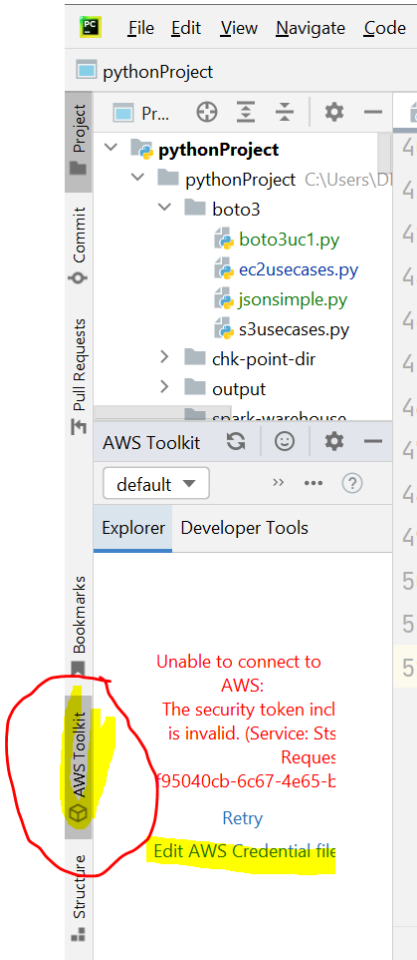
Go to File > Settings

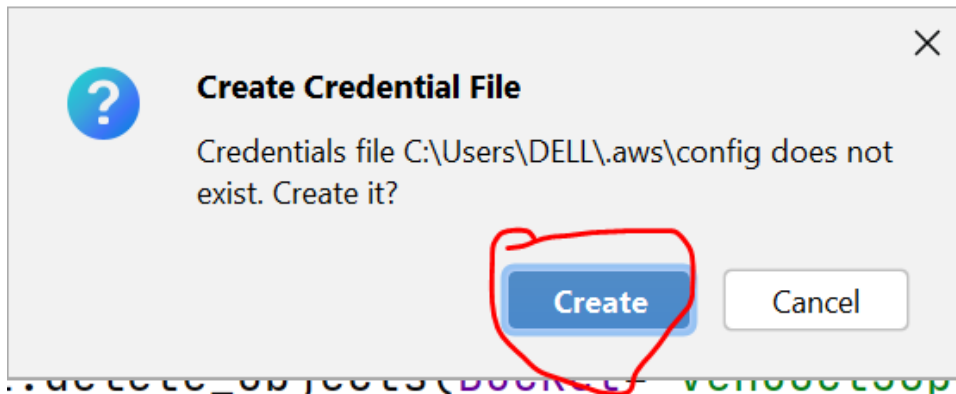
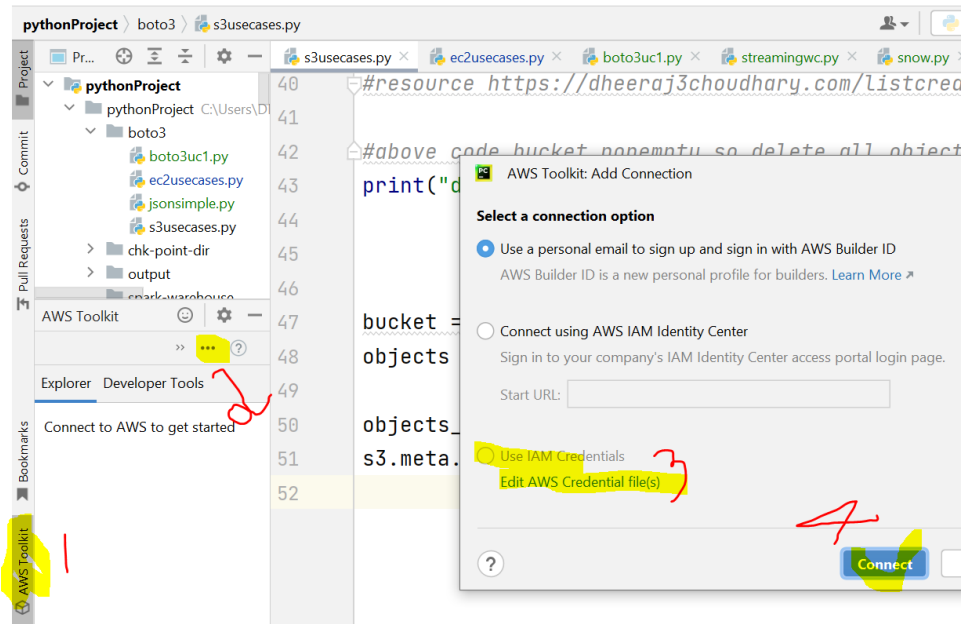


Now AWS plugin installed, (sometime it's showing restart IDE) restart pycharm for better results.

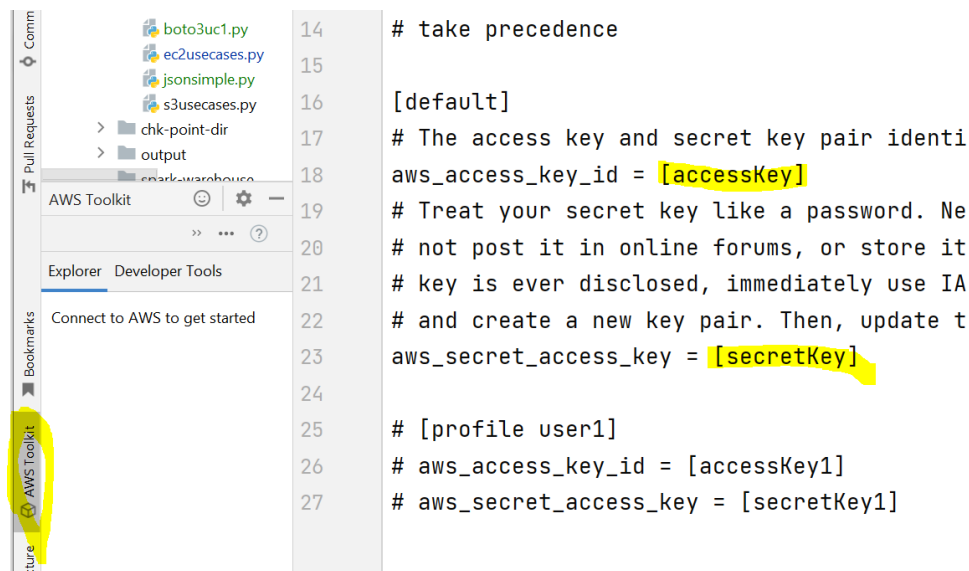


Now pls check left side U have AWS Toolkit





Click on edit AWS credentials enter IAM keys

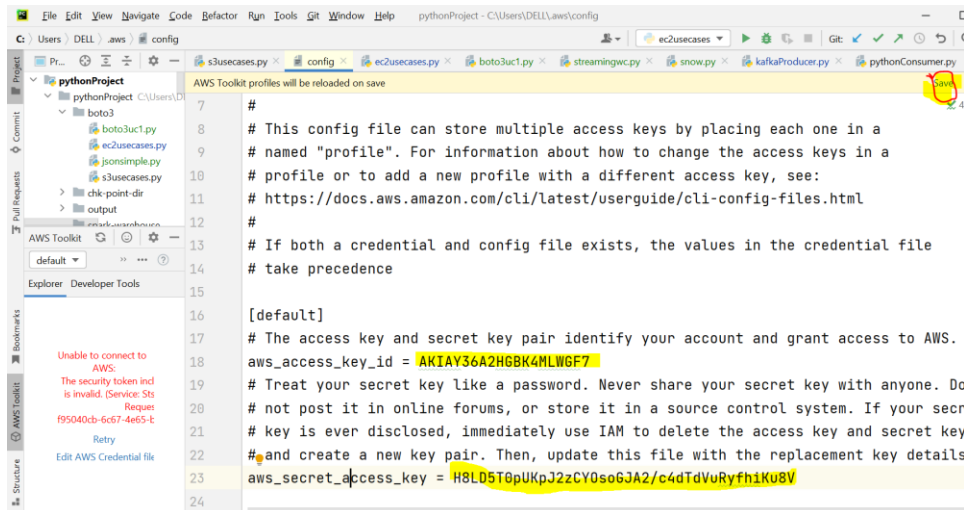


Earlier you downloaded IAM keys

User name, Password, Access key ID, Secret access key, Console login link

venu,,AKIAY36A2HGBK4MLWGF7,H8LD5T0pUKpJ2zCY0soGJA2/c4dTdVuRyfh1Ku8V,https://pysparkpoc2023.signin.aws.amazon.com/console  
sita,,AKIAY36A2HGBA2VLM4XB,bvUS0HIiC1Ij0kaHEWi1w8pieJUDIVHF2M  
+jPtTr,https://pysparkpoc2023.signin.aws.amazon.com/console

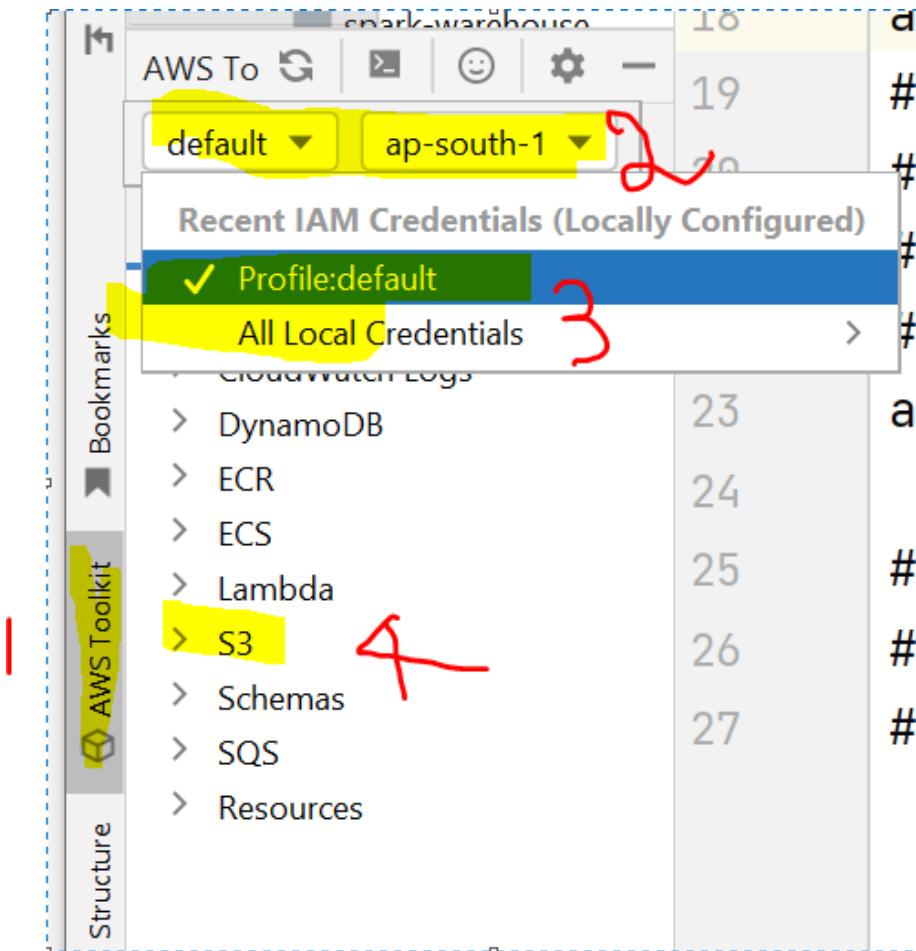
Just copy anyone user details here.



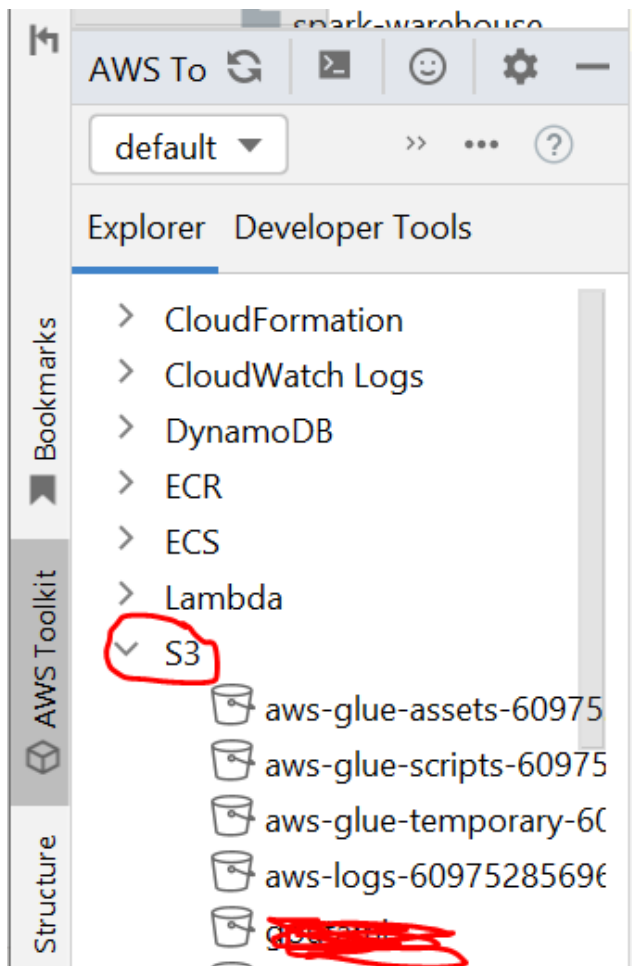
```
7 #
8 # This config file can store multiple access keys by placing each one in a
9 # named "profile". For information about how to change the access keys in a
10 # profile or to add a new profile with a different access key, see:
11 # https://docs.aws.amazon.com/cli/latest/userguide/cli-config-files.html
12 #
13 # If both a credential and config file exists, the values in the credential file
14 # take precedence
15
16 [default]
17 # The access key and secret key pair identify your account and grant access to AWS.
18 aws_access_key_id = AKIAY36A2HGBK4MLWGF7
19 # Treat your secret key like a password. Never share your secret key with anyone. Do
20 # not post it in online forums, or store it in a source control system. If your secret
21 # key is ever disclosed, immediately use IAM to delete the access key and secret key
22 # and create a new key pair. Then, update this file with the replacement key details
23 aws_secret_access_key = H8LD5T0pUKpJ2zCY0soGJA2/c4dTdVuRyfh1Ku8V
24
```

Unable to connect to AWS:  
The security token included is invalid. (Service: sts, Status: 400, RequestID: f95040cb-6c67-4e65-b...

Secret







You have S3 full privileges so you have full privileges to do anything in s3.. Pls find IAM privileges from iam group

**Identity and Access Management (IAM)**

Search IAM

Dashboard

▼ **Access management**

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

▼ **Access reports**

- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

[IAM](#) > [User groups](#) > [Manager](#)

## Manager

### Summary

User group name  
Manager

**Users** | **Permissions** | Access Advisor

### Permissions policies (3) [Info](#)

You can attach up to 10 managed policies.

Filter policies by property or policy name and pres

<input type="checkbox"/>	Policy name <a href="#">↗</a>
<input type="checkbox"/>	<a href="#">+ AmazonRDSFullAccess</a>
<input type="checkbox"/>	<a href="#">+ AmazonEC2FullAccess</a>
<input type="checkbox"/>	<a href="#">+ AmazonS3FullAccess</a>

So 3<sup>rd</sup> party tool like Pycharm, IntelliJ, Snowflake, Databricks want to access AWS resources, use IAM user credentials (Iam keys)

How to connect these IAM keys from Snowflake and databricks explained in another document pls follow.

## IAM Roles

If you want to access AWS access from another AWS service use IAM roles.

As a bigdata developer, 90% you are using IAM roles most frequently. Let eg:

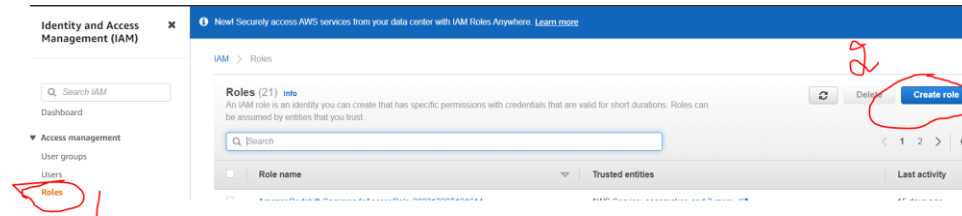
Glue want to access s3

Redshift want to access s3

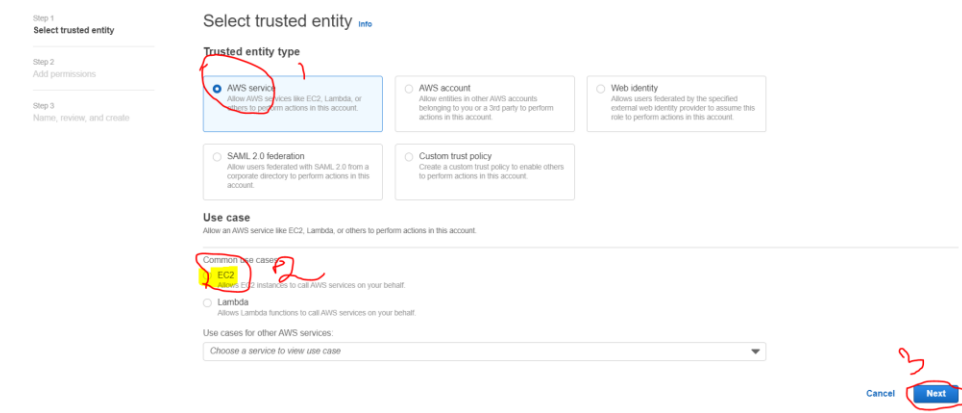
Lambda want to access glue

Ec2 want to access s3

Use IAM roles in these scenario. The main reason EC2 , redshift, Glue, lambda and s3 are aws services.  
So aws service want to access another aws service use **IAM Roles**



Next



Type S3 .. choose s3 full privileges ... it means Ec2 want to access S3

At that time Ec2 had full privileges to access S3.

Step 1  
[Select trusted entity](#)

Step 2  
**Add permissions**

Step 3  
[Name, review, and create](#)

## Add permissions [Info](#)

### Permissions policies (820) [Info](#)

Choose one or more policies to attach to your new role.

[Filter policies by property or policy name and press](#)

"s3"



[Clear filters](#)

<input type="checkbox"/>	Policy name <a href="#">↗</a>
<input type="checkbox"/>	<a href="#">+ AWSGlueServiceRole-aug8glues3full</a>
<input type="checkbox"/>	<a href="#">+ AWSGlueServiceRole-awss3glue</a>
<input type="checkbox"/>	<a href="#">+ AWSGlueServiceRole-glueAccessS3</a>
<input type="checkbox"/>	<a href="#">+ AWSGlueServiceRole-GlueS3Full</a>
<input type="checkbox"/>	<a href="#">+ AWSGlueServiceRole-GlueS3role</a>
<input type="checkbox"/>	<a href="#">+ AWSQuickSightS3Policy</a>
<input type="checkbox"/>	<a href="#">+  AmazonDMSRedshiftS3Role</a>

20

[+ AmazonS3FullAccess](#)

Give any name to that role (relevant name highly recommended)

Step 1  
[Select trusted entity](#)

Step 2  
[Add permissions](#)

Step 3  
**Name, review, and create**

## Name, review, and create

### Role details

Role name

Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+', '=', '@', '-', '\_'

Cancel

Previous

Create role

## Verify IAM roles

<input type="checkbox"/>	<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor (Service-Linked Role)
<input type="checkbox"/>	<a href="#">EC2AccessS3</a>	AWS Service: ec2
<input type="checkbox"/>	<a href="#">ec2access3data</a>	AWS Service: ec2
<input type="checkbox"/>	<a href="#">EMR_AutoScaling_DefaultRole</a>	AWS Service: application-autoscaling, and 1 more
<input type="checkbox"/>	<a href="#">EMR_DefaultRole</a>	AWS Service: elasticmapreduce
<input type="checkbox"/>	<a href="#">EMR_EC2_DefaultRole</a>	AWS Service: ec2
<input type="checkbox"/>	<a href="#">GlueAccessS3</a>	AWS Service: glue

## Now testing purpose create ec2

aws

Services

Search

New EC2 Experience  
Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

► Images

Resources

You are using the following Amazon

Instances (running)

Instances

Placement groups

Volumes

ⓘ Easily size, configure, and c

Learn more

Launch instance

To get started, launch an Amazon EC2

Launch instance ▼

M

EC2 > Instances > Launch an instance

## Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. following the simple steps below.


### Name and tags [Info](#)

Name

ubuntu

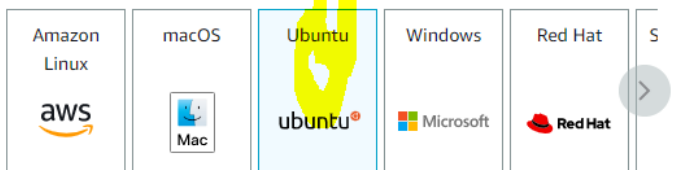
### ▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

 Search our full catalog including 1000s of application and OS images

Recents


Quick Start





When you are creating emr below Advanced option available. Click and choose IAM role choose (EC2AccessS3) Finally click **launch instance**

#### ▼ Advanced details [Info](#)

**Purchasing option [Info](#)**  
☐ Request Spot Instances  
Request Spot Instances at the Spot price, capped at the On-Demand price

**Domain join directory [Info](#)**  
Select  Create new directory

**IAM instance profile [Info](#)**  
Select  Create new IAM profile  
Search:   
Select   
EC2AccessS3  
arn:aws:iam::609752856962:instance-profile/EC2AccessS3  
ec2access3data  
arn:aws:iam::609752856962:instance-profile/ec2access3data  
EMR\_EC2\_DefaultRole  
arn:aws:iam::609752856962:instance-profile/EMR\_EC2\_DefaultRole

**Instance auto-recovery [Info](#)**  
Select

**Shutdown behavior [Info](#)**  
Stop

#### Summary



**Number of instances [Info](#)**  
1

**Software Image (AMI) [Info](#)**  
Canonical, Ubuntu, 22.04 LTS, ...read more  
ami-0f69bc5520884278e

**Virtual server type (instance type) [Info](#)**  
t2.micro

**Firewall (security group) [Info](#)**  
New security group

**Storage (volumes) [Info](#)**  
1 volume(s) - 8 GiB

 **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. 

Cancel **Launch instance**

Pic Name: IAM-role-assign

If u face any problem to connect ec2 follow ec2 document

Or follow this video to connect ec2 using putty

<https://www.youtube.com/watch?v=Nu8u79o7qVI>

sudo apt update .... its highly recommended

aws s3 ls is commonly used aws s3 command to display s3 buckets.

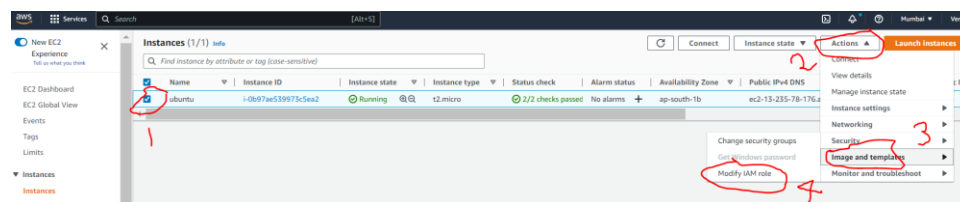
sudo apt install awscli ... used to run any command using command line interface.

```
ubuntu@ip-172-31-12-41: ~  
ubuntu@ip-172-31-12-41:~$ #sudo apt update  
ubuntu@ip-172-31-12-41:~$ aws s3 ls  
Command 'aws' not found, but can be installed with:  
sudo snap install aws-cli # version 1.15.58, or  
sudo apt install awscli # version 1.22.34-1  
See 'snap info aws-cli' for additional versions.  
ubuntu@ip-172-31-12-41:~$ sudo apt install awscli
```

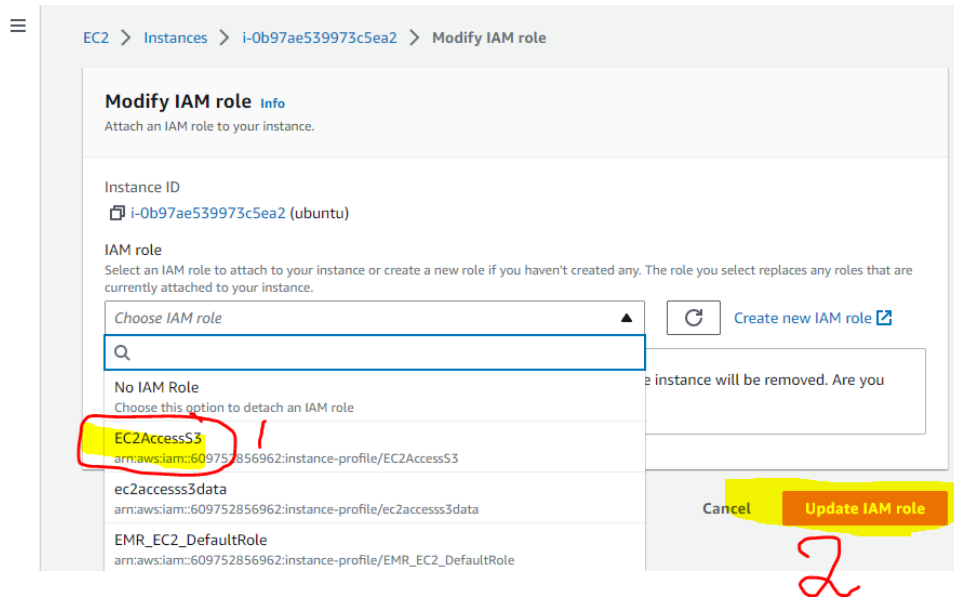
Now if you execute s3 commands it's not working. You will get access denied access or like this

**Unable to locate credentials. You can configure credentials by running "aws configure".** it means you don't have privileges to access. Ofcourse you can use IAM keys also but not recommended.

```
ubuntu@ip-172-31-12-41:~$ aws s3 ls  
Unable to locate credentials. You can configure credentials by running "aws configure".  
ubuntu@ip-172-31-12-41:~$
```



Above you created IAM Role .. modify and assign to this ec2 server. At that time automatically this EC2 having all privileges to access S3.. Update with this.



Pls note: if you assign iam role (Pic Name: IAM-role-assign) earlier this step no need.

```
ubuntu@ip-172-31-12-41:~$ aws s3 ls
Unable to locate credentials. You can
configure".
ubuntu@ip-172-31-12-41:~$ aws s3 ls
2022-07-16 06:01:35 aws-glue-assets-6
2021-08-01 02:25:33 aws-glue-scripts-
2021-08-01 02:25:34 aws-glue-temporar
2020-11-03 15:30:19 aws-logs-60975285
```

Now check you have full privileges to access S3 after assign IAM role...

Similarly Redshift access S3 explained in another document pls follow

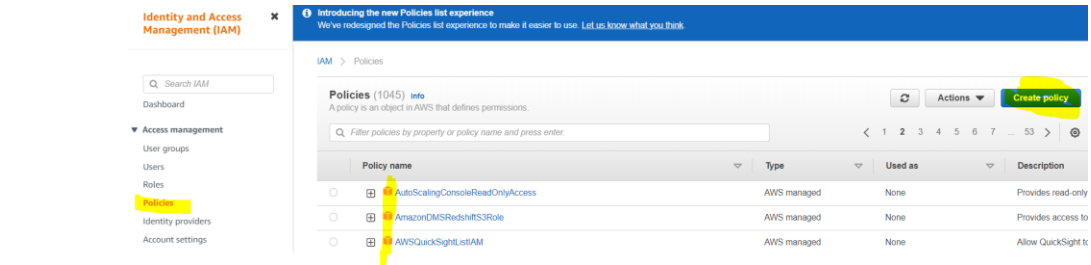
Similarly Lambda access S3, glue explained in another document pls follow

Similarly Glue access S3 explained in another document pls follow

## IAM Policy

Policy nothing but collection of privileges to access different AWS Services. Hilgited yellow color box means by default aws assigned privileges .





If you want to create ur own privileges click Create policy

## Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a p

**Visual editor** **JSON**

[Expand all](#) | [Collapse all](#)

▼ Select a service

▼ Service Select a service below

close

Q s3

S3 ⓘ S3 Object Lan

**Actions** Choose a service before defining actions

**Resources** Choose actions before applying resources

**Request conditions** Choose actions before specifying conditions

Now choose different privileges and uncheck appropriate

▼ Actions Specify the actions allowed in S3 [Switch to deny permissions](#) ⓘ

[close](#)

Q Filter actions

Manual actions (add actions)

☐ All S3 actions (s3:\*)

Access level [Expand all](#) | [Collapse all](#)

☒ List (10 selected)

☒ Read (53 selected)

☒ Tagging (10 selected)

☐ Write (38 selected)

<input checked="" type="checkbox"/> AbortMultipartUpload ⓘ	<input checked="" type="checkbox"/> InitiateReplication ⓘ	<input checked="" type="checkbox"/> PutInventoryConfiguration ⓘ
<input checked="" type="checkbox"/> CreateAccessPoint ⓘ	<input checked="" type="checkbox"/> PutAccelerateConfiguration ⓘ	<input checked="" type="checkbox"/> PutLifecycleConfiguration ⓘ
<input checked="" type="checkbox"/> CreateAccessPointForObjectLam... ⓘ	<input checked="" type="checkbox"/> PutAccessPointConfigurationFor... ⓘ	<input checked="" type="checkbox"/> PutMetricsConfiguration ⓘ
<input checked="" type="checkbox"/> CreateBucket ⓘ	<input checked="" type="checkbox"/> PutAnalyticsConfiguration ⓘ	<input checked="" type="checkbox"/> PutObject ⓘ
<input checked="" type="checkbox"/> CreateJob ⓘ	<input checked="" type="checkbox"/> PutBucketCORS ⓘ	<input checked="" type="checkbox"/> PutObjectLegalHold ⓘ
<input checked="" type="checkbox"/> CreateMultiRegionAccessPoint ⓘ	<input checked="" type="checkbox"/> PutBucketLogging ⓘ	<input checked="" type="checkbox"/> PutObjectRetention ⓘ
<input checked="" type="checkbox"/> DeleteAccessPoint ⓘ	<input checked="" type="checkbox"/> PutBucketNotification ⓘ	<input checked="" type="checkbox"/> PutReplicationConfiguration ⓘ
<input checked="" type="checkbox"/> DeleteAccessPointForObjectLam... ⓘ	<input checked="" type="checkbox"/> PutBucketObjectLockConfiguration ⓘ	<input checked="" type="checkbox"/> PutStorageLensConfiguration ⓘ
<input type="checkbox"/> DeleteBucket ⓘ	<input checked="" type="checkbox"/> PutBucketOwnershipControls ⓘ	<input checked="" type="checkbox"/> ReplicateDelete ⓘ
<input type="checkbox"/> DeleteBucketWebsite ⓘ	<input checked="" type="checkbox"/> PutBucketRequestPayment ⓘ	<input checked="" type="checkbox"/> ReplicateObject ⓘ
<input type="checkbox"/> DeleteMultiRegionAccessPoint ⓘ	<input checked="" type="checkbox"/> PutBucketVersioning ⓘ	<input checked="" type="checkbox"/> RestoreObject ⓘ
<input type="checkbox"/> DeleteObject ⓘ	<input checked="" type="checkbox"/> PutBucketWebsite ⓘ	<input checked="" type="checkbox"/> SubmitMultiRegionAccessPointR... ⓘ
<input type="checkbox"/> DeleteObjectVersion ⓘ	<input checked="" type="checkbox"/> PutEncryptionConfiguration ⓘ	<input checked="" type="checkbox"/> UpdateJobPriority ⓘ

[Cancel](#) [Next: Tags](#)

Now choose **All resources** (all aws services access this policies)

▼ Resources [close](#)

☐ Specific

☒ All resources

As a best practice, define permissions for only specific resources in specific accounts. Alternatively, you can grant least privilege using condition keys. [Learn more](#)

[Request conditions](#) Specify request conditions (optional)

Item count: 3,712 of 6,144.

[Cancel](#) [Next: Tags](#)

Tags always optional pls ignore

[Cancel](#) [Previous](#) [Next: Review](#)

Now

## Create policy

1 2 3

### Review policy

Name\* **S3NoDeletePolicyTest**

Use alphanumeric and "+", "@", "\_" characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and "+", "@", "\_" characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 363 services) <a href="#">Show remaining 362</a>			
S3	Full: List, Read, Permissions management, Tagging Limited: Write	All resources	None

Tags

Key	Value
-----	-------

No tags associated with the resource.

\* Required

Cancel

Previous

Create policy

Dashboard

#### ▼ Access management

User groups

Users

Roles

**Policies**

Identity providers

Account settings

#### ▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

"s3" X

Clear filters

Policy name

- ☐ [AWSGlueServiceRole-aug8glues3full](#)
- ☐ [AWSGlueServiceRole-awss3glue](#)
- ☐ [AWSGlueServiceRole-glueAccessS3](#)
- ☐ [AWSGlueServiceRole-GlueS3Full](#)
- ☐ [AWSGlueServiceRole-GlueS3role](#)
- ☐ [AWSQuickSightS3Policy](#)
- ☐ [S3NoDeletePolicyTest](#)
- ☐ [AmazonDMSRedshiftS3Role](#)
- ☐ [AmazonS3FullAccess](#)

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups > Manager

Manager

Summary

User group name: Manager

Creation time: January 11, 2023, 20:24 (UTC+05:30)

ARN: arn:aws:iam:609752856962:group/Manager

Users

Permissions

Access Advisor

Permissions policies (3)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

Policy name	Type	Description
AmazonRDSFullAccess	AWS managed	Provides full access to Amazon RDS via the AWS Management Console.
AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Management Console.
AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Management Console.

Like above add this customized privileges to this group

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups > Manager > Add permissions

Attach permission policies to Manager

Current permissions policies (3)

Other permission policies (Selected 1/818)

You can attach up to 10 managed policies to this user group. All of the attached permissions.

Filter policies by property or policy name and press enter.

"s3" X Clear filters

Policy name
<input type="checkbox"/> AWSGlueServiceRole-aug8glues3full
<input type="checkbox"/> AWSGlueServiceRole-awss3glue
<input type="checkbox"/> AWSGlueServiceRole-glueAccessS3
<input type="checkbox"/> AWSGlueServiceRole-GlueS3Full
<input type="checkbox"/> AWSGlueServiceRole-GlueS3role
<input type="checkbox"/> AWSQuickSightS3Policy
<input checked="" type="checkbox"/> S3NoDeletePolicyTest

Cancel

Add permissions

Now try to delete existing s3full privileges and add customized new privileges.

Manager

Summary

User group name: Manager  
Creation time: January 11, 2023, 20:24 (UTC+05:30)  
ARN: arn:aws:iam:609752856962:group/Manager

Users | **Permissions**

**Remove AmazonS3FullAccess?**

All the users in this group will lose the permissions defined in this policy.

Cancel Delete

Permissions policies (Selected)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

	Policy name	Type	Description
<input type="checkbox"/>	S3NoDeletePolicyTest	Customer managed	
<input type="checkbox"/>	AmazonRDSFullAccess	AWS managed	Provides full access to Amazon RDS resources.
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 resources.
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to Amazon S3 resources.

Now pls check new privileges

Users | **Permissions** | Access Advisor

**Permissions policies (3)** [Info](#)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

	Policy name
<input type="checkbox"/>	<input checked="" type="checkbox"/> S3NoDeletePolicyTest
<input type="checkbox"/>	<input checked="" type="checkbox"/> AmazonRDSFullAccess
<input type="checkbox"/>	<input checked="" type="checkbox"/> AmazonEC2FullAccess

Now who is in manager group all employees have s3 full privileges except delete object privileges.

Notice? No yellow color box means it's user defined policy.