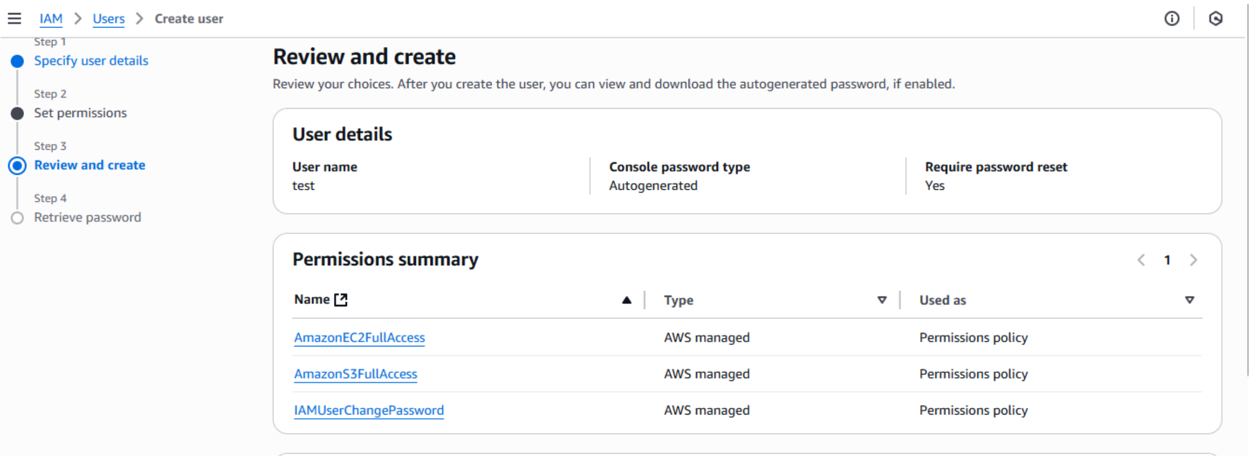
1) Create one IAM user and assign ec2, s3 full access role.



IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Review and create

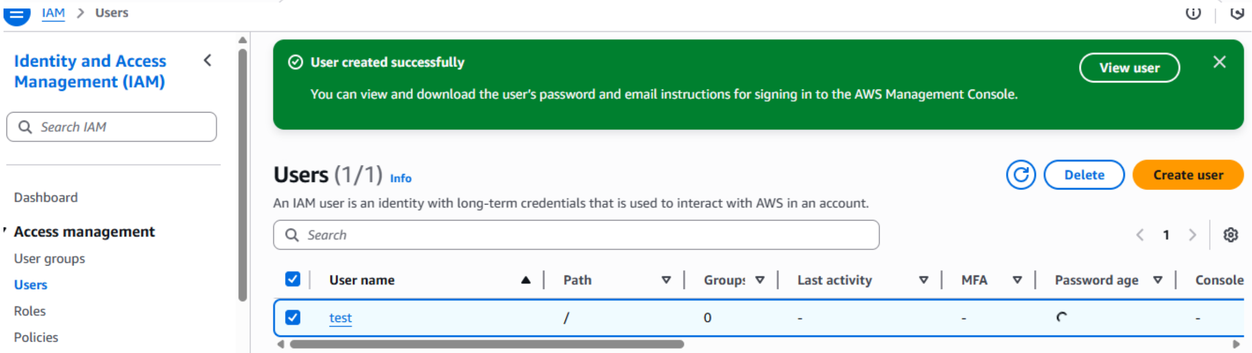
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
test	Autogenerated	Yes

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy



IAM > Users

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management
User groups
Users
Roles
Policies

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

Users (1/1) Info

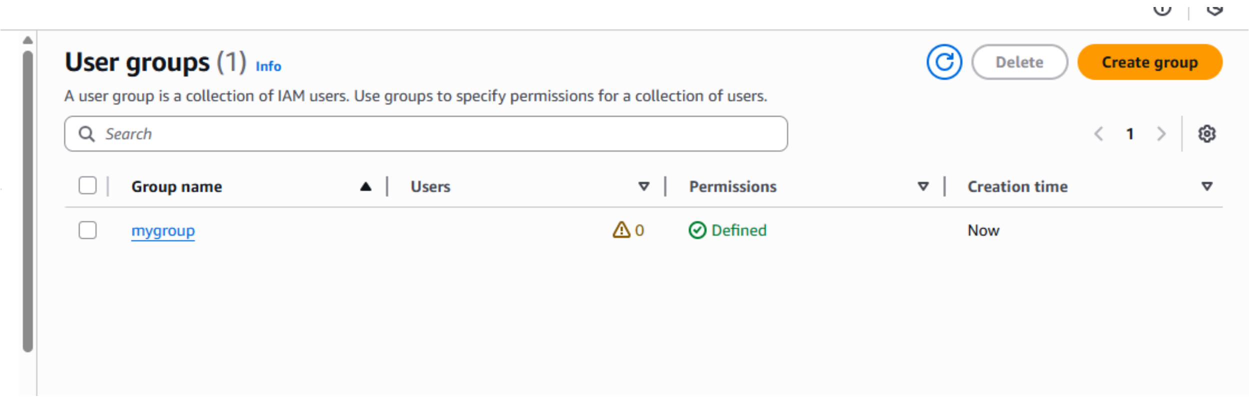
Delete | Create user

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

☑	User name	Path	Group:	Last activity	MFA	Password age	Console
☑	test	/	0	-	-		-

2) Create one Group in IAM and Assign Read access for ec2.



User groups (1) Info

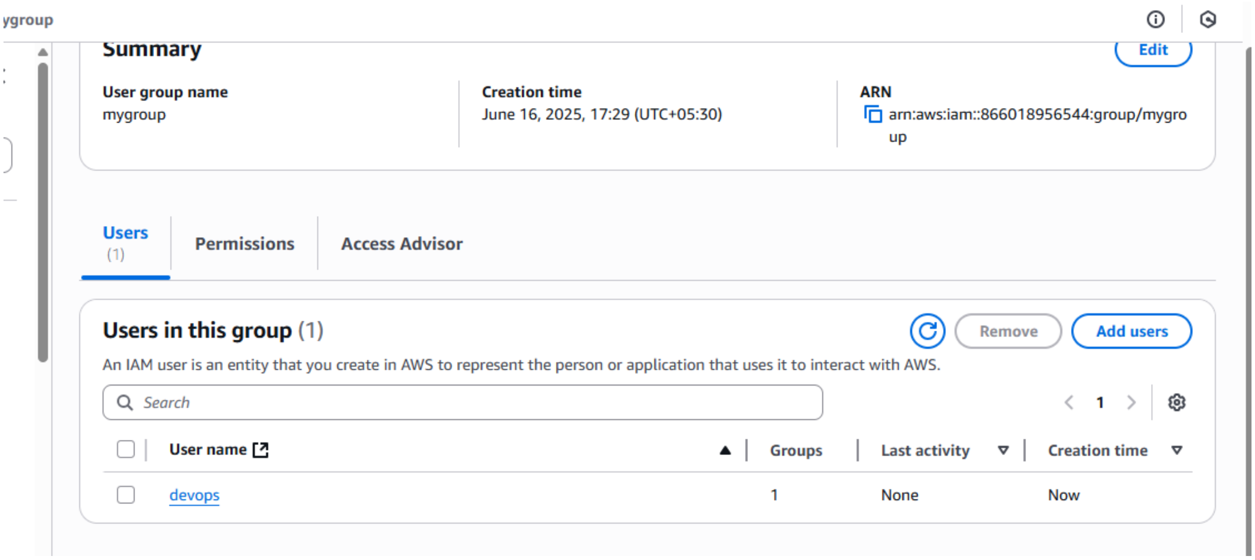
Delete | Create group

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

□	Group name	Users	Permissions	Creation time
□	mygroup	⚠ 0	✓ Defined	Now

3) Create a new user with name Devops and add to the group created in task2.



ygroup

Summary

User group name
mygroup

Creation time
June 16, 2025, 17:29 (UTC+05:30)

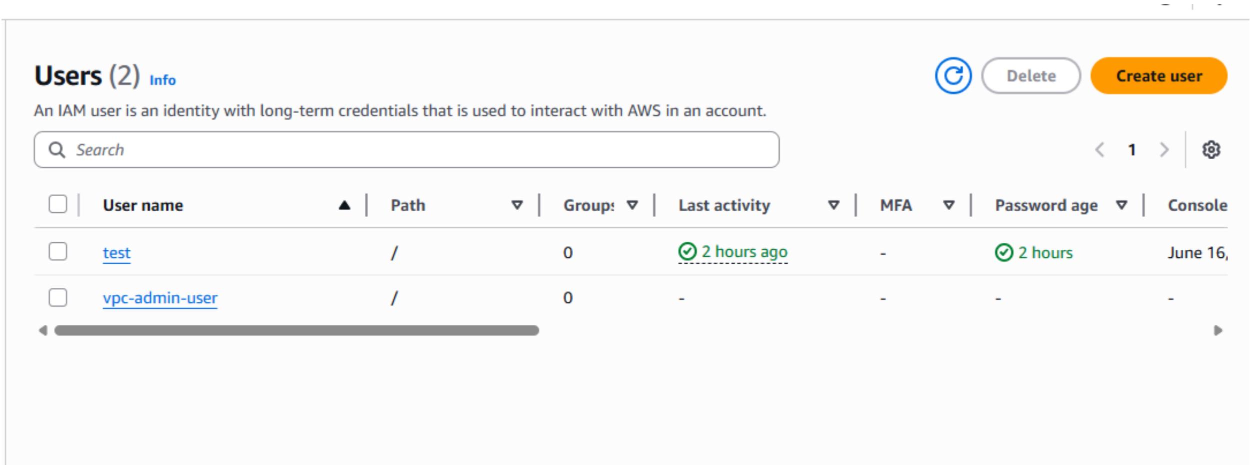
ARN
arn:aws:iam::866018956544:group/mygroup

Users in this group (1)

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

□	User name	Groups	Last activity	Creation time
□	devops	1	None	Now

4) Write a bash script to create a IAM user with VPC full access.

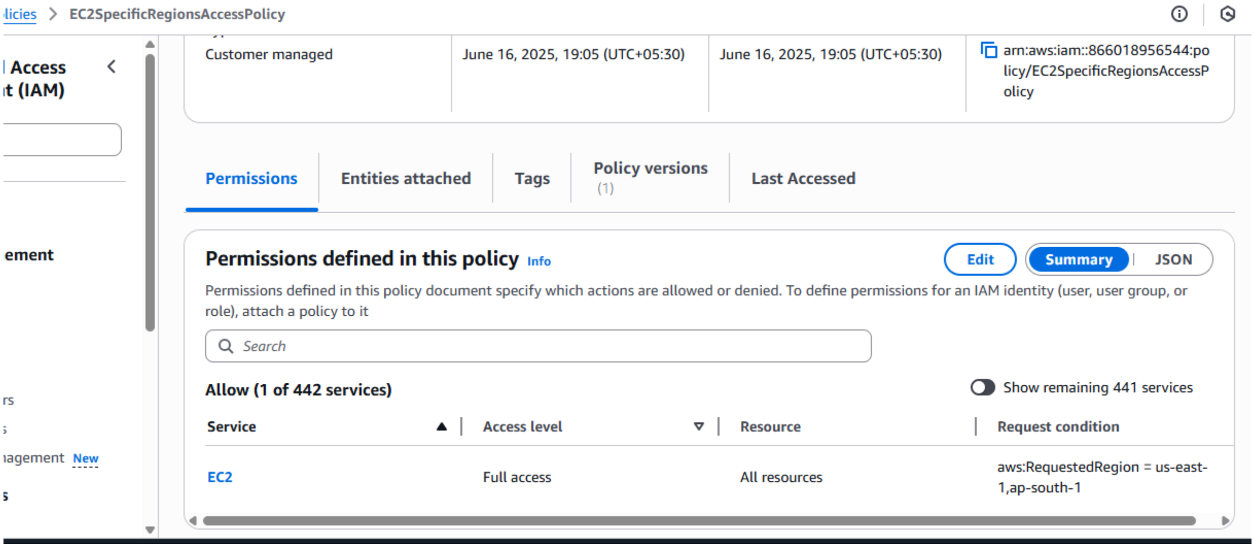


Users (2) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Path	Group:	Last activity	MFA	Password age	Console
□	test	/	0	✓ 2 hours ago	-	✓ 2 hours	June 16,
□	vpc-admin-user	/	0	-	-	-	-

5) Create a IAM policy to access ec2 for a specific user in specific regions only.



licies > EC2SpecificRegionsAccessPolicy

Customer managed	June 16, 2025, 19:05 (UTC+05:30)	June 16, 2025, 19:05 (UTC+05:30)	arn:aws:iam::866018956544:policy/EC2SpecificRegionsAccessPolicy

Permissions defined in this policy Info

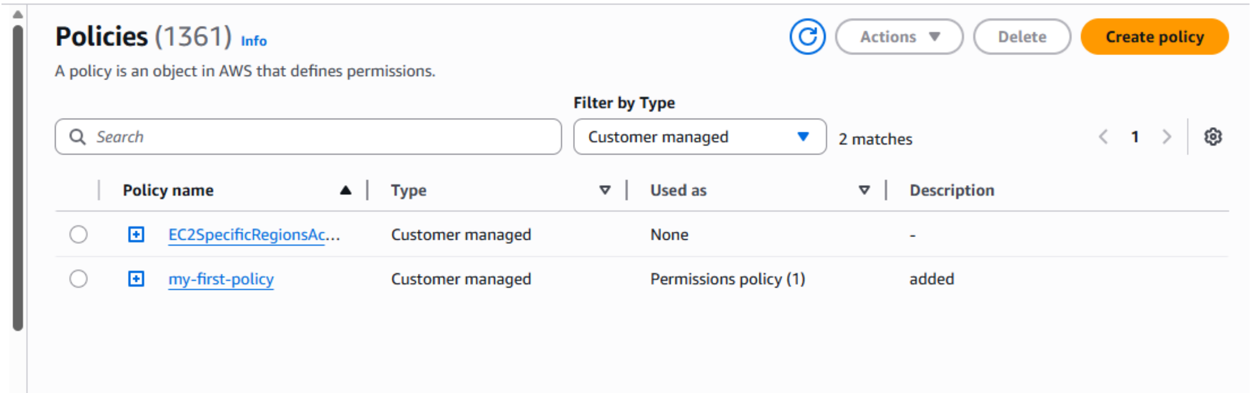
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (1 of 442 services)

Show remaining 441 services

Service	Access level	Resource	Request condition
EC2	Full access	All resources	aws:RequestedRegion = us-east-1,ap-south-1



Policies (1361) Info

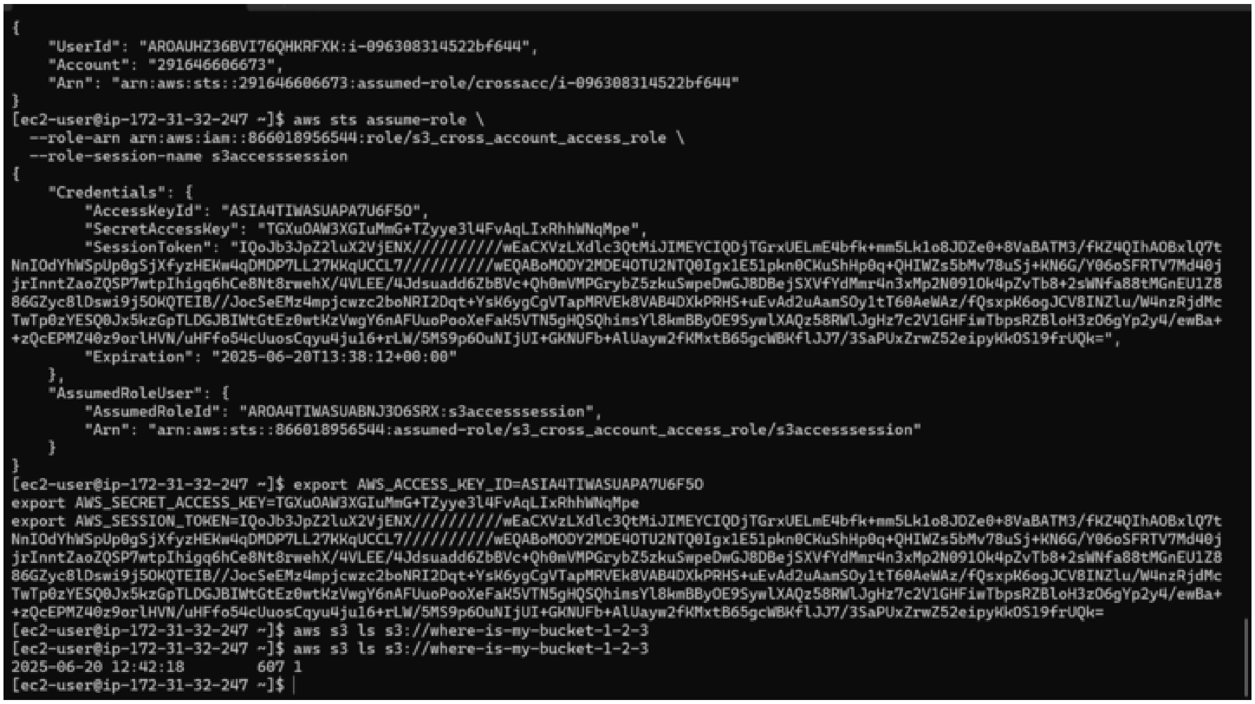
A policy is an object in AWS that defines permissions.

Filter by Type: Customer managed

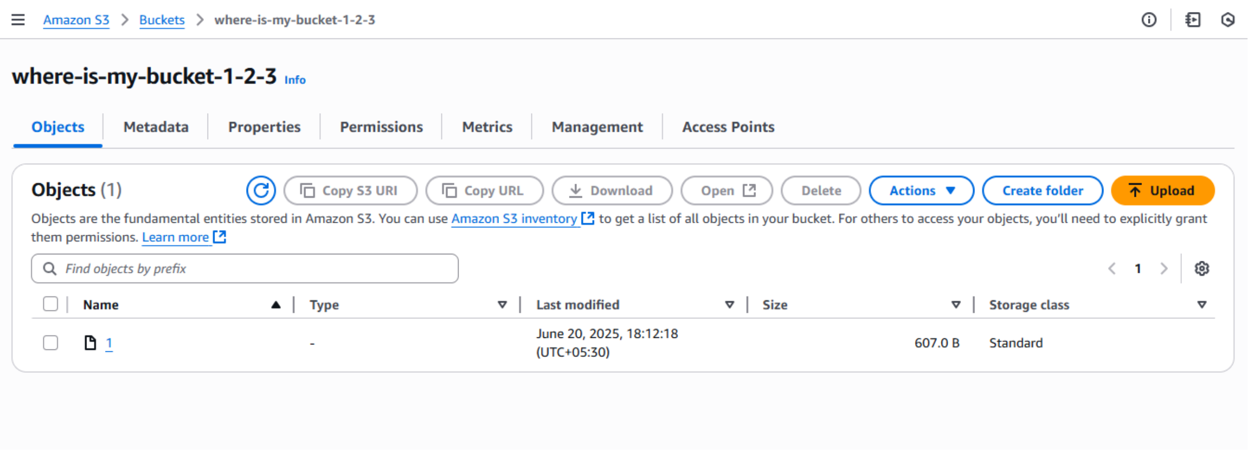
2 matches

	Policy name	Type	Used as	Description
○	EC2SpecificRegionsAc...	Customer managed	None	-
○	my-first-policy	Customer managed	Permissions policy (1)	added

6) We have two accounts Account A and Account B , Account A user should access s3 bucket in Account B. (Collaborate with team member and execute this. Mostly asked in every interview)



```
{
    "UserId": "AROAUHZ36BVI76QHKRFXK:i-096308314522bf644",
    "Account": "291646606673",
    "Arn": "arn:aws:sts::291646606673:assumed-role/crossacc/i-096308314522bf644"
}
[ec2-user@ip-172-31-32-247 ~]$ aws sts assume-role \
  --role-arn arn:aws:iam::866018956544:role/s3_cross_account_access_role \
  --role-session-name s3accesssession
{
    "Credentials": {
        "AccessKeyId": "ASIA4TIWASUAPA7U6F5O",
        "SecretAccessKey": "TGXuOAW3XGIuMmG+TZyye3l4FvAqLIxRhhWNqMpe",
        "SessionToken": "IQoJb3JpZ2luX2VjENX//////////wEaCXVzLXdlc3QtMiJIMEYCIQDjTGrxUELmE4bfk+mm5Lk1o8JDZe0+8VaBATM3/fKZ4QIhAOBxlQ7t
NnIOdYhWSpUp0gSjXfyzHEKw4qDMDP7LL27KKqUCCL7//////////wEQABoMODY2MDE4OTU2NTQ0Igx1E51pkn0CKuShHp0q+QHIWZs5bMv78uSj+KN6G/Y06oSFRTV7Md40j
jrInntZaoZQSP7wtpIhigq6hCe8Nt8rwehX/4VLEE/4Jdsuadd6ZbBVc+Qh0mVMPGrybZ5zkuSwpeDwGJ8DBejSXVfYdMmr4n3xMp2N091Ok4pZvTb8+2sWNfa88tMGnEU1Z8
86GZyc8lDswi9j5OKQTEIB//JocSeEMz4mpjcwzc2boNRI2Dqt+YsK6ygCgVTapMRVEk8VAB4DXkPRHS+uEvAd2uAamSOy1tT60AeWAz/fQsxpK6ogJCV8INZlu/W4nzRjdMc
TwTp0zYESQ0Jx5kzGpTLDGJBIWtGtEz0wtKzVwgY6nAFUuoPooXeFaK5VTN5gHQSQhimsYl8kmBByOE9SywlXAQz58RWlJgHz7c2V1GHFiwTbpsRZBloH3zO6gYp2y4/ewBa+
+zQcEPMZ40z9orlHVN/uHFfo54cUuosCqyu4ju16+rLW/5MS9p6OuNIjUI+GKNUFb+AlUayw2fKMxtB65gcWBKflJJ7/3SaPUxZrwZ52eipyKkOS19frUQk=",
        "Expiration": "2025-06-20T13:38:12+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROA4TIWASUABNJ3O6SRX:s3accesssession",
        "Arn": "arn:aws:sts::866018956544:assumed-role/s3_cross_account_access_role/s3accesssession"
    }
}
[ec2-user@ip-172-31-32-247 ~]$ export AWS_ACCESS_KEY_ID=ASIA4TIWASUAPA7U6F5O
export AWS_SECRET_ACCESS_KEY=TGXuOAW3XGIuMmG+TZyye3l4FvAqLIxRhhWNqMpe
export AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjENX//////////wEaCXVzLXdlc3QtMiJIMEYCIQDjTGrxUELmE4bfk+mm5Lk1o8JDZe0+8VaBATM3/fKZ4QIhAOBxlQ7t
NnIOdYhWSpUp0gSjXfyzHEKw4qDMDP7LL27KKqUCCL7//////////wEQABoMODY2MDE4OTU2NTQ0Igx1E51pkn0CKuShHp0q+QHIWZs5bMv78uSj+KN6G/Y06oSFRTV7Md40j
jrInntZaoZQSP7wtpIhigq6hCe8Nt8rwehX/4VLEE/4Jdsuadd6ZbBVc+Qh0mVMPGrybZ5zkuSwpeDwGJ8DBejSXVfYdMmr4n3xMp2N091Ok4pZvTb8+2sWNfa88tMGnEU1Z8
86GZyc8lDswi9j5OKQTEIB//JocSeEMz4mpjcwzc2boNRI2Dqt+YsK6ygCgVTapMRVEk8VAB4DXkPRHS+uEvAd2uAamSOy1tT60AeWAz/fQsxpK6ogJCV8INZlu/W4nzRjdMc
TwTp0zYESQ0Jx5kzGpTLDGJBIWtGtEz0wtKzVwgY6nAFUuoPooXeFaK5VTN5gHQSQhimsYl8kmBByOE9SywlXAQz58RWlJgHz7c2V1GHFiwTbpsRZBloH3zO6gYp2y4/ewBa+
+zQcEPMZ40z9orlHVN/uHFfo54cUuosCqyu4ju16+rLW/5MS9p6OuNIjUI+GKNUFb+AlUayw2fKMxtB65gcWBKflJJ7/3SaPUxZrwZ52eipyKkOS19frUQk=
[ec2-user@ip-172-31-32-247 ~]$ aws s3 ls s3://where-is-my-bucket-1-2-3
[ec2-user@ip-172-31-32-247 ~]$ aws s3 ls s3://where-is-my-bucket-1-2-3
2025-06-20 12:42:18        607 1
[ec2-user@ip-172-31-32-247 ~]$ 
```



where-is-my-bucket-1-2-3 Info

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

□	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class ▽
□	1	-	June 20, 2025, 18:12:18 (UTC+05:30)	607.0 B	Standard