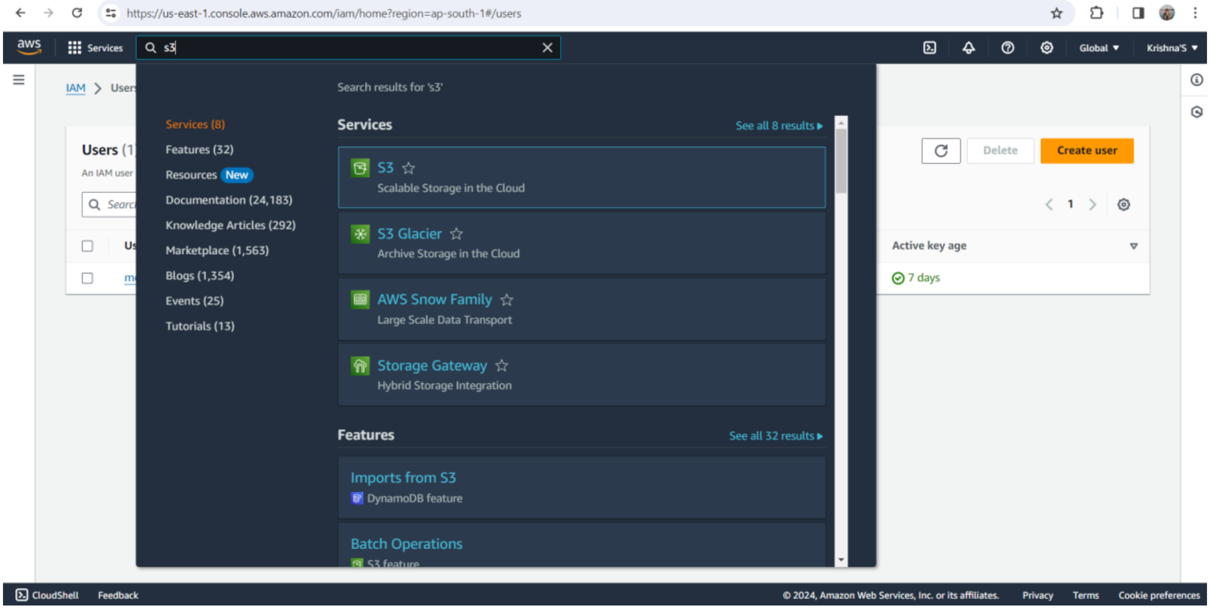
AWS ASSIGNMENT

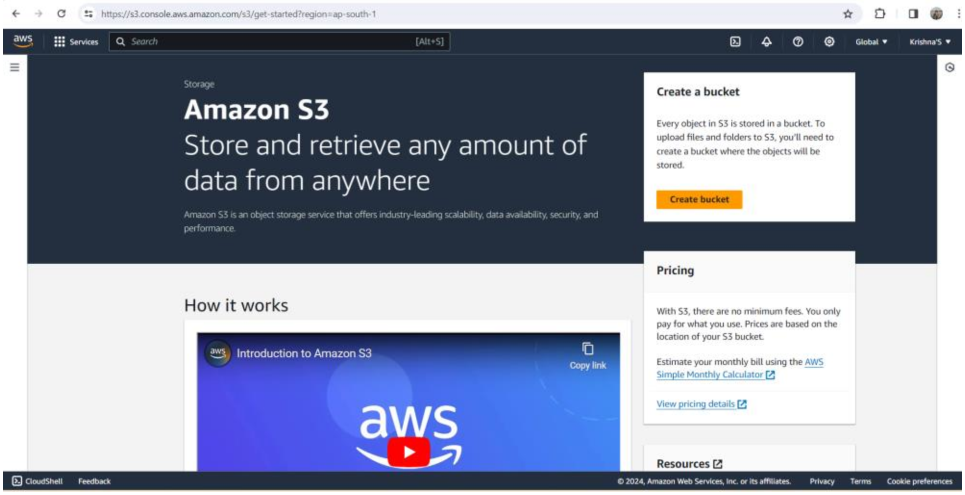
1. Create 5 AWS S3 buckets with a random prefix that should end in a bucket number. For example, *bucket-prefix-1, bucket-prefix-2 … bucket-prefix-5*
2. Create an EC2 instance with the following specifications:
   I. OS – Ubuntu 22 LTS
   II. There is at least one IAM Role attached with the permission to upload files to the 3rd bucket created in Problem 1.
   III. User Data – A script that should upload a text file with the instance's Private IP Address and Hostname to the S3 Bucket.

Steps to solve the Assignment:

1. Create 5 S3 Buckets with any name that is not used previously it should be unique because S3 Service is a Global Service.
2. Log into the AWS Console and Open S3 Bucket Service



3. Click on the Create Bucket Option


https://s3.console.aws.amazon.com/s3/get-started?region=ap-south-1
Services
Search
[Alt+S]
Global
Krishna'S
Storage
Amazon S3
Store and retrieve any amount of data from anywhere
Create a bucket
Create bucket
Pricing
How it works
Introduction to Amazon S3
Copy link
aws
View pricing details
Resources
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

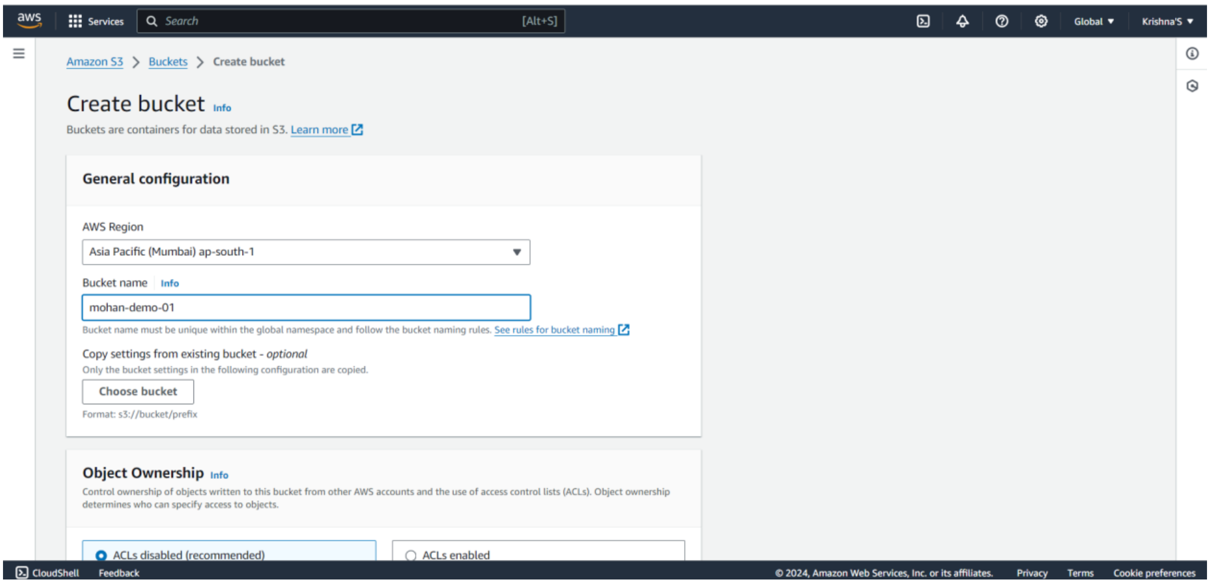
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

4. Enter the S3 Bucket Name select the region leave the remaining options as it is and click on Create bucket



Create bucket

Buckets are containers for data stored in S3. Learn more

General configuration

AWS Region: Asia Pacific (Mumbai) ap-south-1

Bucket name: mohan-demo-01

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

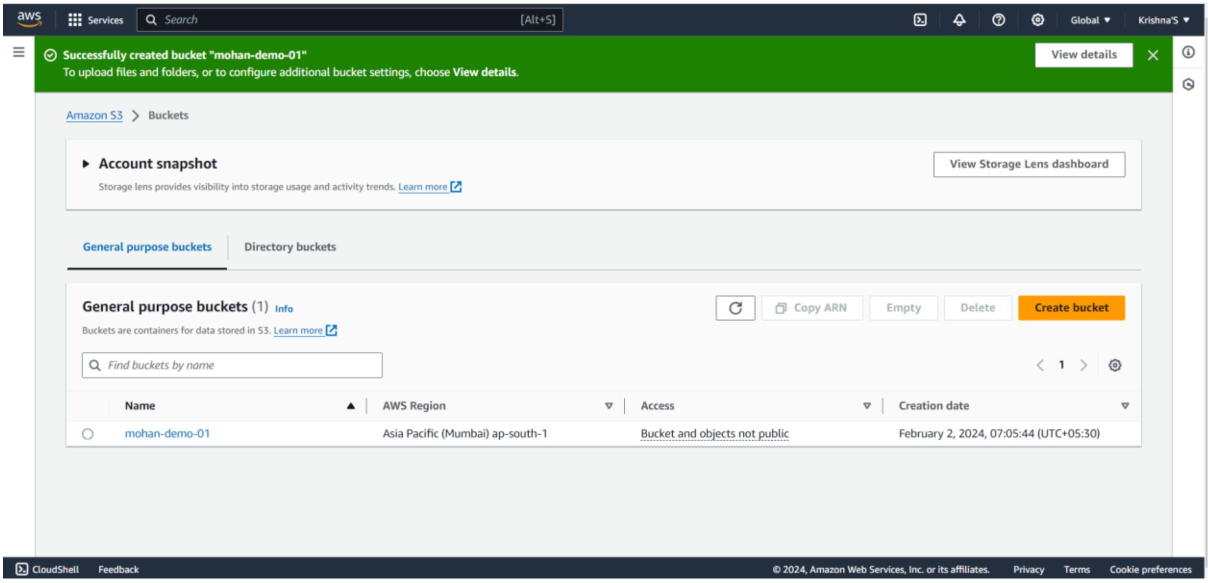
Format: s3://bucket/prefix

Object Ownership

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) ○ ACLs enabled

5. After clicking on the create bucket option s3 bucket is created successfully.



Successfully created bucket "mohan-demo-01"

To upload files and folders, or to configure additional bucket settings, choose **View details**.

▸ Account snapshot

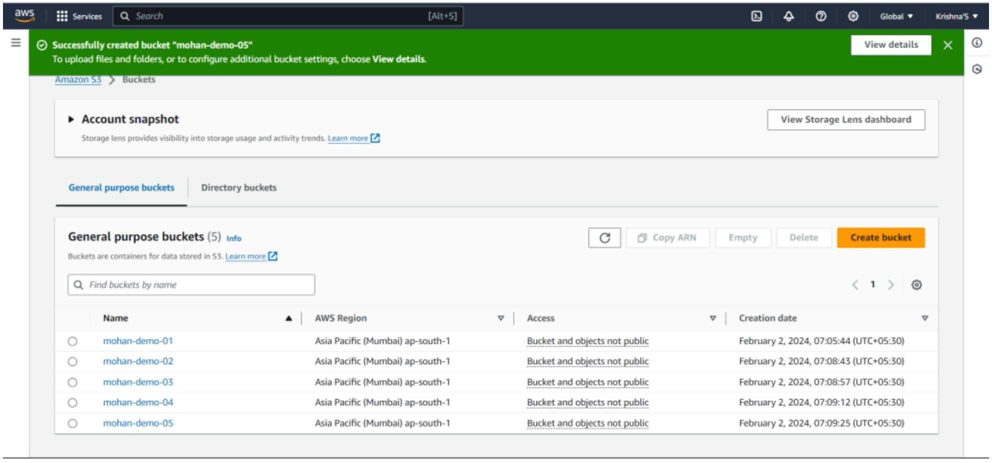
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1)

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	mohan-demo-01	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 2, 2024, 07:05:44 (UTC+05:30)

6. Repeat the Same Steps to create the remaining 4 S3 Buckets



Successfully created bucket "mohan-demo-05"

To upload files and folders, or to configure additional bucket settings, choose **View details**.

▸ Account snapshot

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

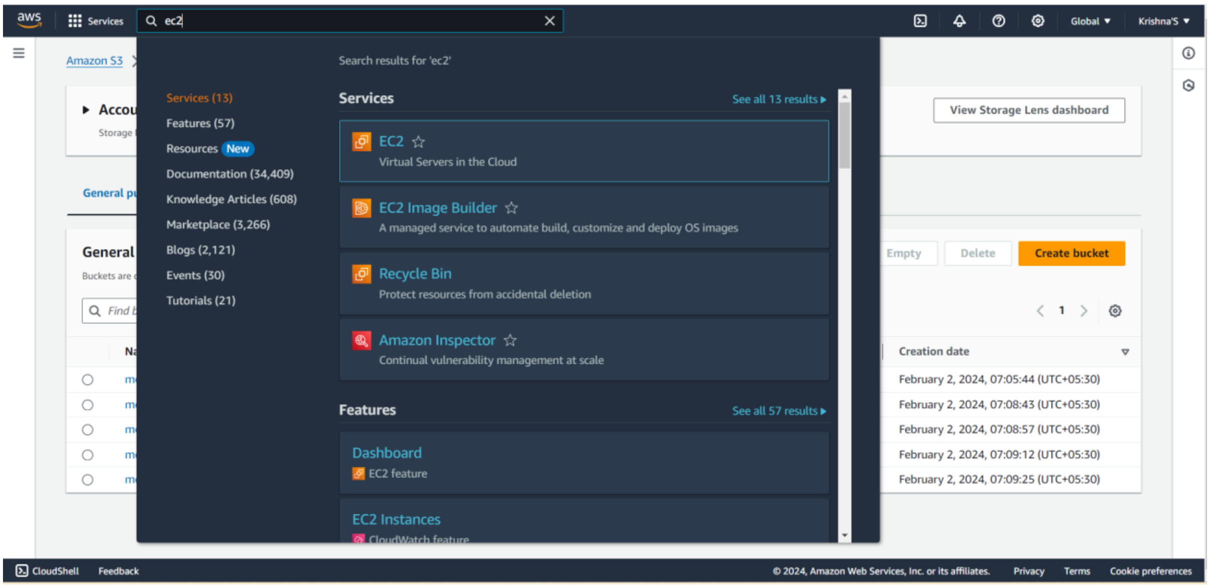
General purpose buckets (5)

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	mohan-demo-01	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 2, 2024, 07:05:44 (UTC+05:30)
○	mohan-demo-02	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 2, 2024, 07:08:43 (UTC+05:30)
○	mohan-demo-03	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 2, 2024, 07:08:57 (UTC+05:30)
○	mohan-demo-04	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 2, 2024, 07:09:12 (UTC+05:30)
○	mohan-demo-05	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 2, 2024, 07:09:25 (UTC+05:30)

2. Create a EC2 Instance with Ubuntu 22 LTS Image

1. Search EC2 Instance in the Search Bar and Launch the EC2 Instance Service



Search results for 'ec2'

- Services (13)
- Features (57)
- Resources New
- Documentation (34,409)
- Knowledge Articles (608)
- Marketplace (3,266)
- Blogs (2,121)
- Events (30)
- Tutorials (21)

Services — See all 13 results ▸

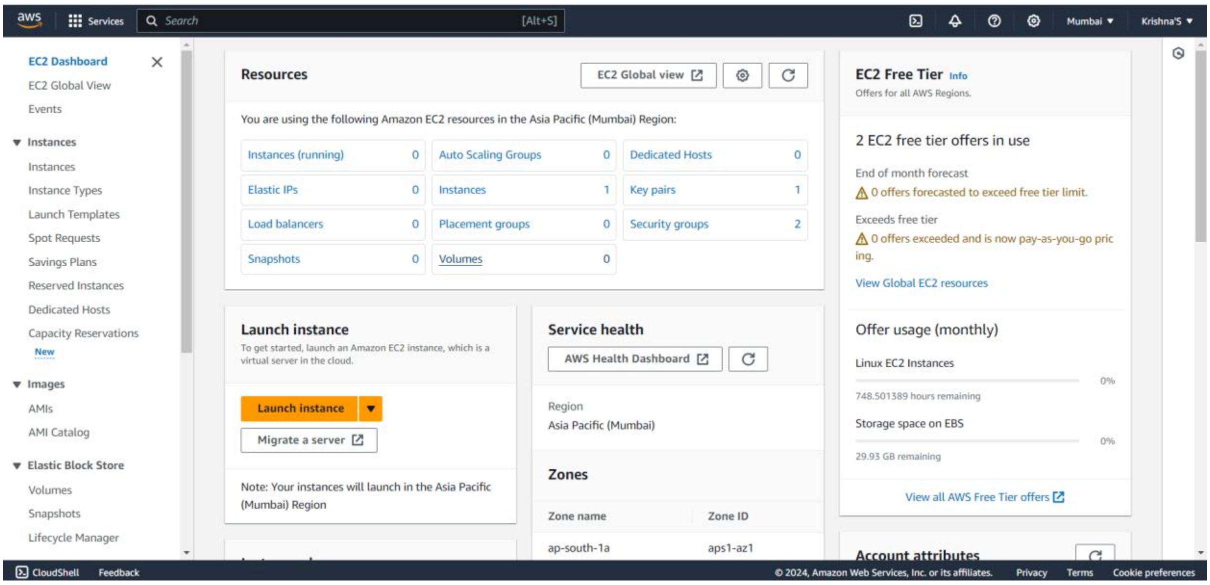
- EC2 — Virtual Servers in the Cloud
- EC2 Image Builder — A managed service to automate build, customize and deploy OS images
- Recycle Bin — Protect resources from accidental deletion
- Amazon Inspector — Continual vulnerability management at scale

Features — See all 57 results ▸

- Dashboard — EC2 feature
- EC2 Instances — CloudWatch feature

Creation date
February 2, 2024, 07:05:44 (UTC+05:30)
February 2, 2024, 07:08:43 (UTC+05:30)
February 2, 2024, 07:08:57 (UTC+05:30)
February 2, 2024, 07:09:12 (UTC+05:30)
February 2, 2024, 07:09:25 (UTC+05:30)

2. Click on Launch Instance to create the EC2 instance



Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	1	Key pairs	1
Load balancers	0	Placement groups	0	Security groups	2
Snapshots	0	Volumes	0		

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the Asia Pacific (Mumbai) Region

Service health

Region
Asia Pacific (Mumbai)

Zones

Zone name	Zone ID
ap-south-1a	aps1-az1

EC2 Free Tier Info

Offers for all AWS Regions.

2 EC2 free tier offers in use

End of month forecast

⚠ 0 offers forecasted to exceed free tier limit.

Exceeds free tier

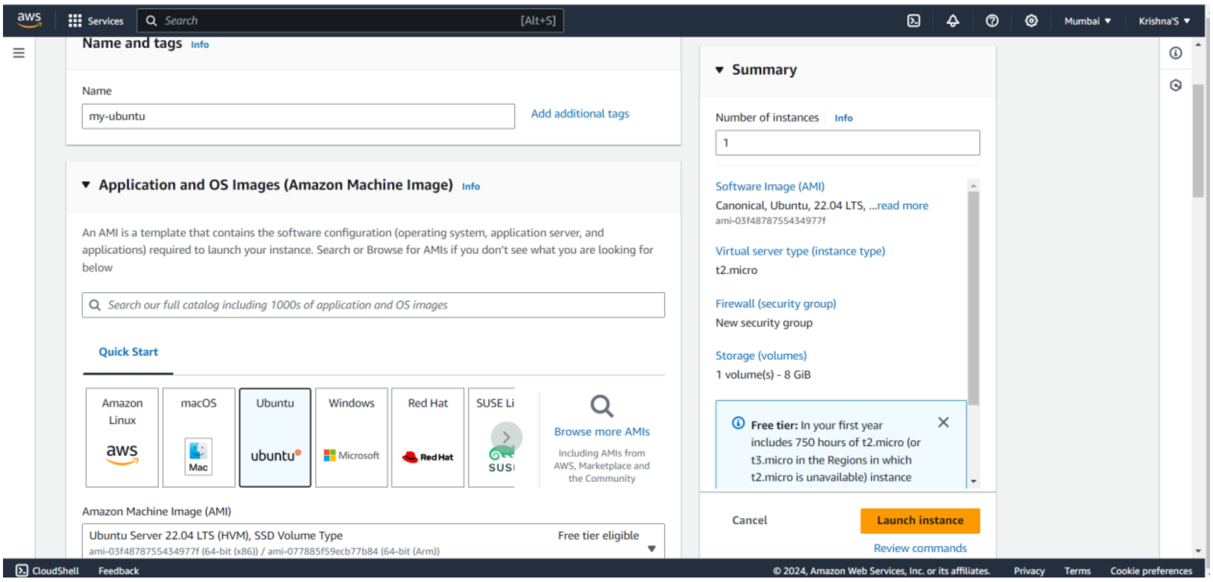
⚠ 0 offers exceeded and is now pay-as-you-go pricing.

Offer usage (monthly)

Linux EC2 Instances 0%
748.501389 hours remaining

Storage space on EBS 0%
29.93 GB remaining

3. Enter the Name and Select the Image as Ubuntu 22.04 LTS



Name and tags Info

Name

my-ubuntu

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to 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

Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Li

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type — Free tier eligible

ami-03f4878755434977f (64-bit (x86)) / ami-077885f59ecb77b84 (64-bit (Arm))

▼ Summary

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more

ami-03f4878755434977f

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

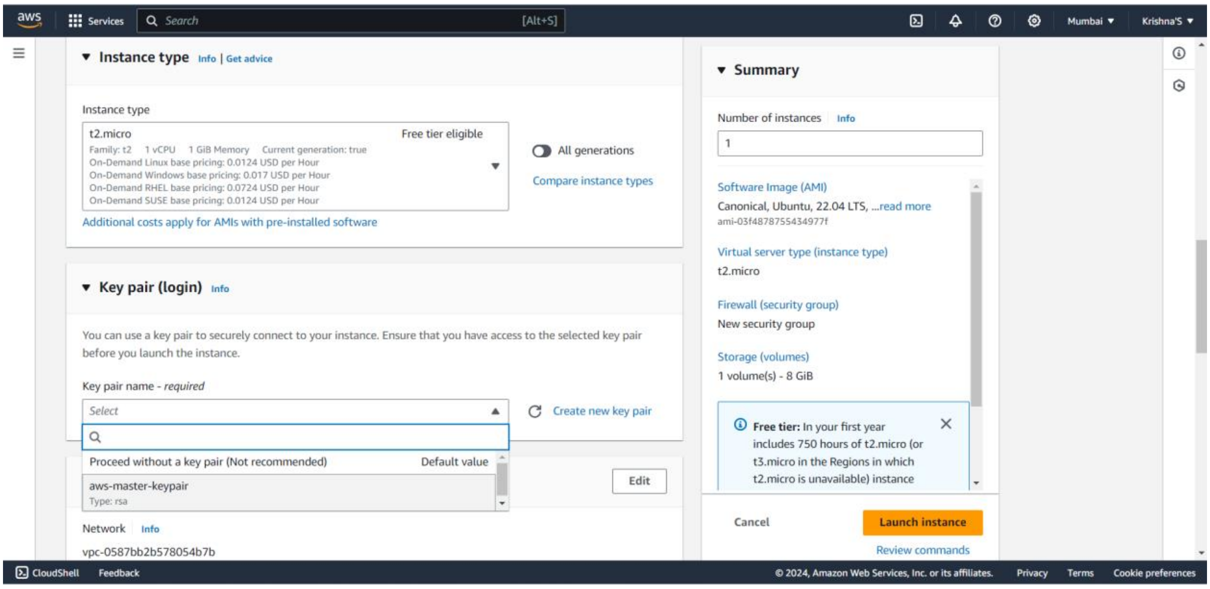
1 volume(s) - 8 GiB

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

Cancel | Launch instance

Review commands

4. Select the Instance type as t2.micro and select the key pair. In my case, I already have the key pair I'm using that. If Key Pair is not available you can create it



▼ Instance type Info | Get advice

Instance type

t2.micro — Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Linux base pricing: 0.0124 USD per Hour

On-Demand Windows base pricing: 0.017 USD per Hour

On-Demand RHEL base pricing: 0.0724 USD per Hour

On-Demand SUSE base pricing: 0.0124 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select

Create new key pair

Proceed without a key pair (Not recommended) — Default value

aws-master-keypair

Type: rsa

Edit

Network Info

vpc-0587bb2b578054b7b

▼ Summary

Number of instances Info

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more

ami-03f4878755434977f

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

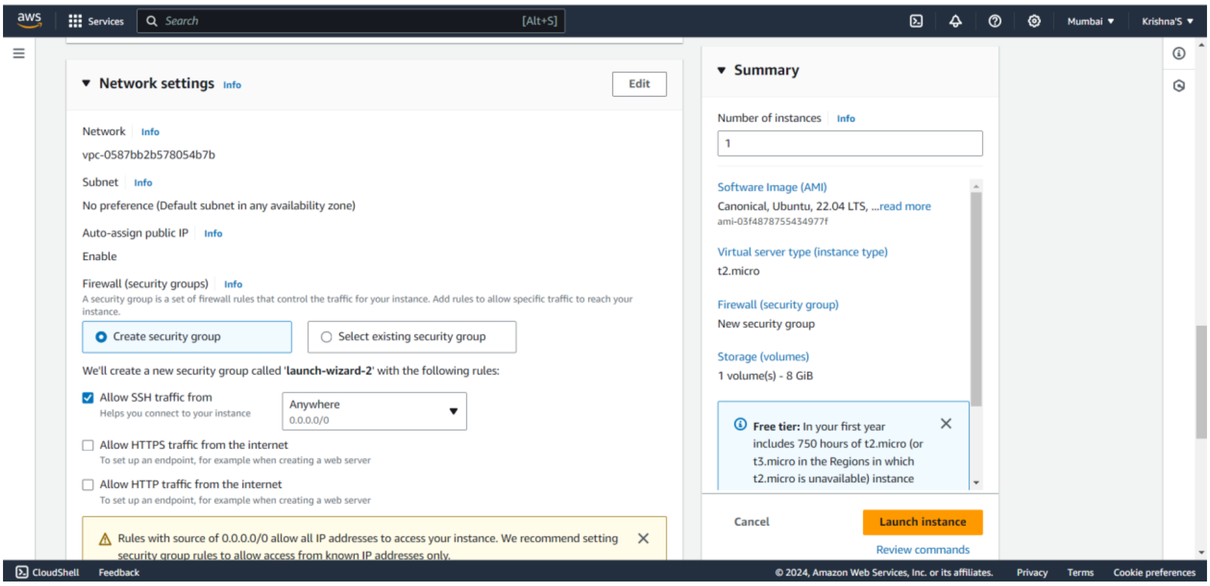
1 volume(s) - 8 GiB

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

Cancel | Launch instance

Review commands

5. I’m using the Default VPC Settings



▼ Network settings Info

Edit

Network Info
vpc-0587bb2b578054b7b

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-2**' with the following rules:

☑ Allow SSH traffic from
Helps you connect to your instance
Anywhere ▼
0.0.0.0/0

□ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ Summary

Number of instances Info
1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-03f4878755434977f

Virtual server type (instance type)
t2.micro

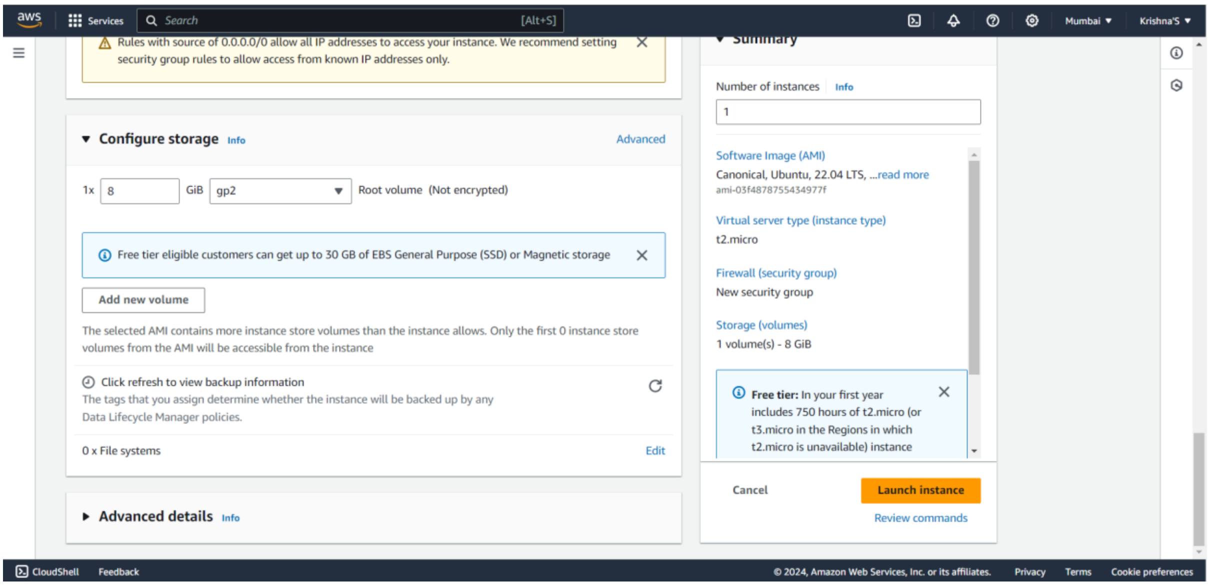
Firewall (security group)
New security group

Storage (volumes)
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

Cancel
Launch instance
Review commands

6. Configure Storage as 8 GB and then click on Launch Instance



⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ Configure storage Info

Advanced

1x 8 GiB gp2 ▼ Root volume (Not encrypted)

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems
Edit

▶ Advanced details Info

▼ Summary

Number of instances Info
1

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-03f4878755434977f

Virtual server type (instance type)
t2.micro

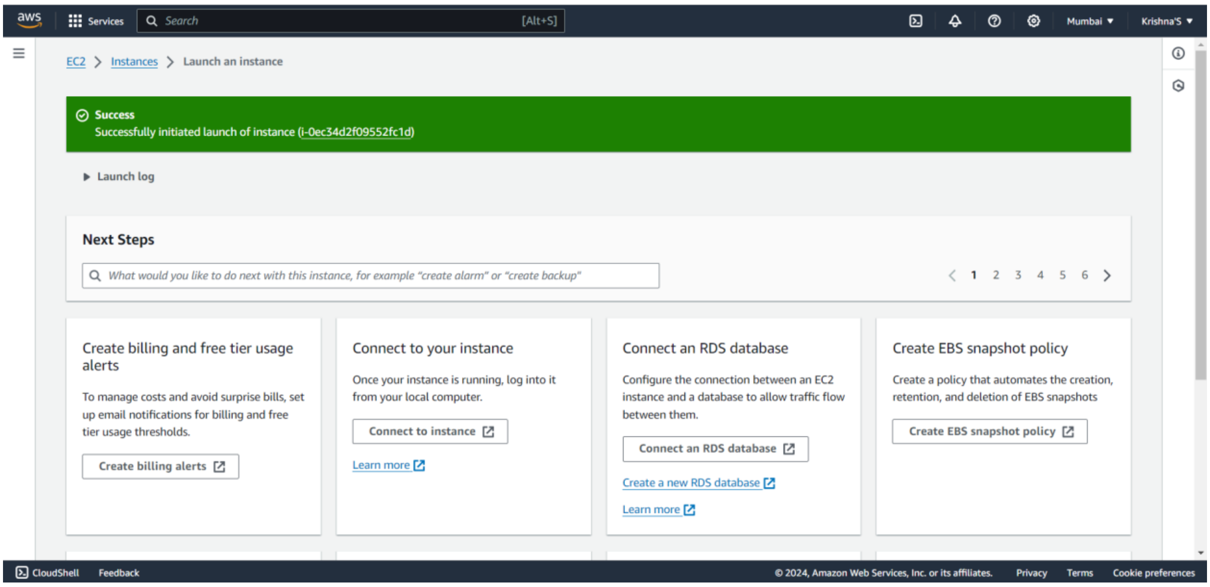
Firewall (security group)
New security group

Storage (volumes)
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

Cancel
Launch instance
Review commands

7. Instance launch is successfully initiated and click on the instance ID to check whether the instance is running or not.



Success
Successfully initiated launch of instance (i-0ec34d2f09552fc1d)

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

< 1 2 3 4 5 6 >

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Create billing alerts

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect to instance

Learn more

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Connect an RDS database

Create a new RDS database

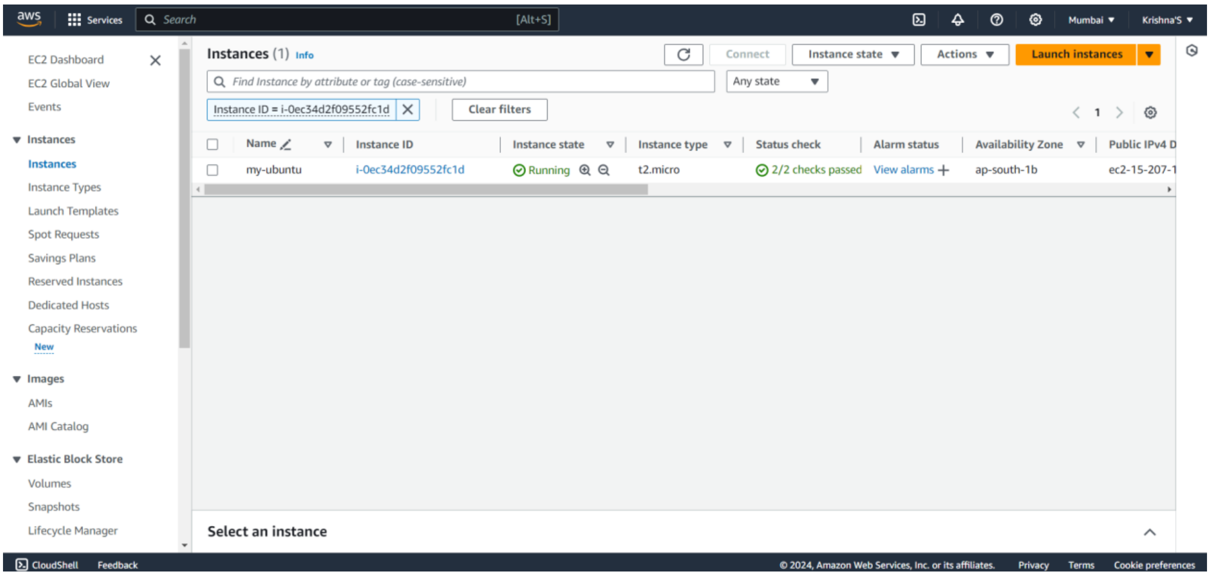
Learn more

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots

Create EBS snapshot policy

8. Check whether the instance status is up and running or not



Instances (1) Info

Find Instance by attribute or tag (case-sensitive)

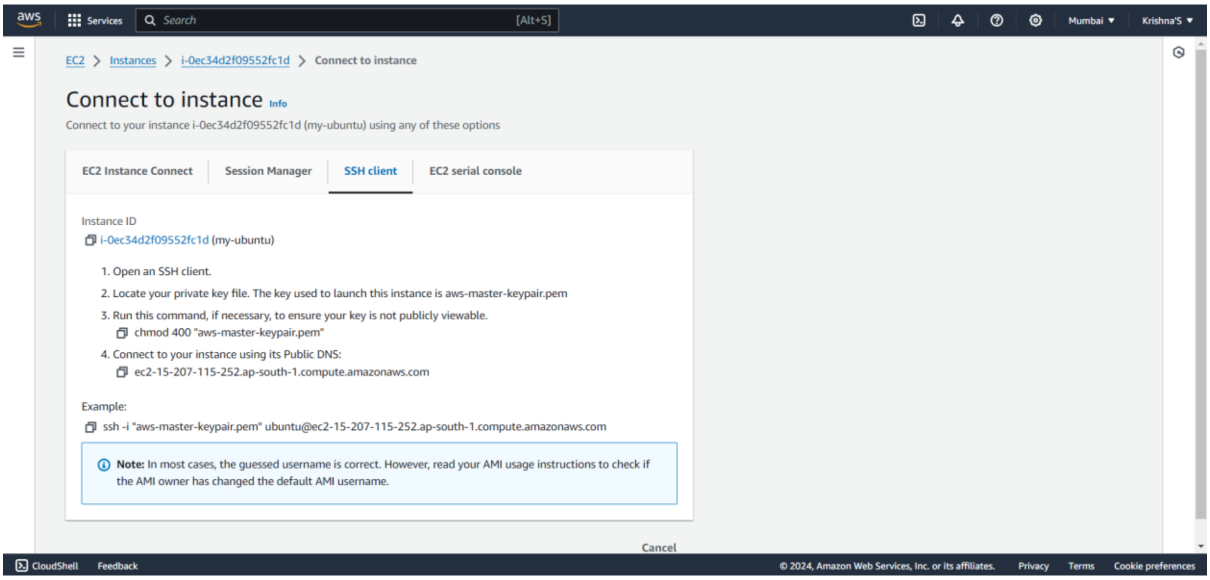
Any state ▼

Instance ID = i-0ec34d2f09552fc1d ✕

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
□	my-ubuntu	i-0ec34d2f09552fc1d	✓ Running	t2.micro	✓ 2/2 checks passed	View alarms +	ap-south-1b	ec2-15-207-1

Select an instance

9. Connect to the Instance by selecting the instance by clicking on Connect I’m using SSH Client to Connect it



EC2 > Instances > i-0ec34d2f09552fc1d > Connect to instance

Connect to instance Info

Connect to your instance i-0ec34d2f09552fc1d (my-ubuntu) using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID

i-0ec34d2f09552fc1d (my-ubuntu)

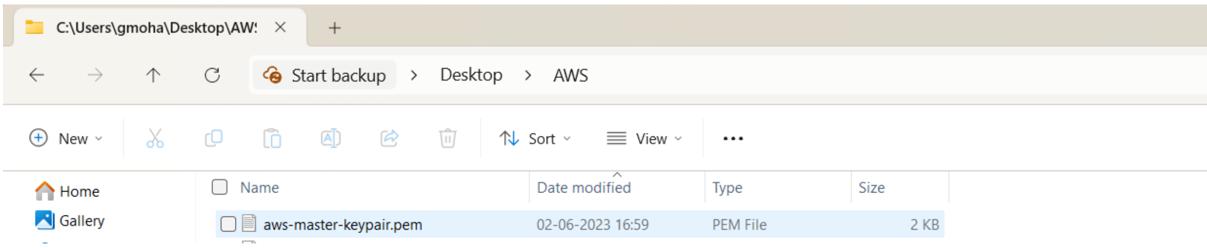
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is aws-master-keypair.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
   chmod 400 "aws-master-keypair.pem"
4. Connect to your instance using its Public DNS:
   ec2-15-207-115-252.ap-south-1.compute.amazonaws.com

Example:

```
ssh -i "aws-master-keypair.pem" ubuntu@ec2-15-207-115-252.ap-south-1.compute.amazonaws.com
```

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

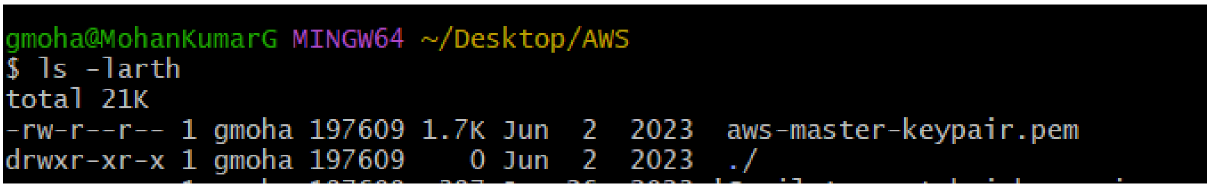
10. Open CMD or GitBash Where your Pem file is located and then enter this command ssh -i "aws-master-keypair.pem" ubuntu@ec2-15-207-115-252.ap-south-1.compute.amazonaws.com



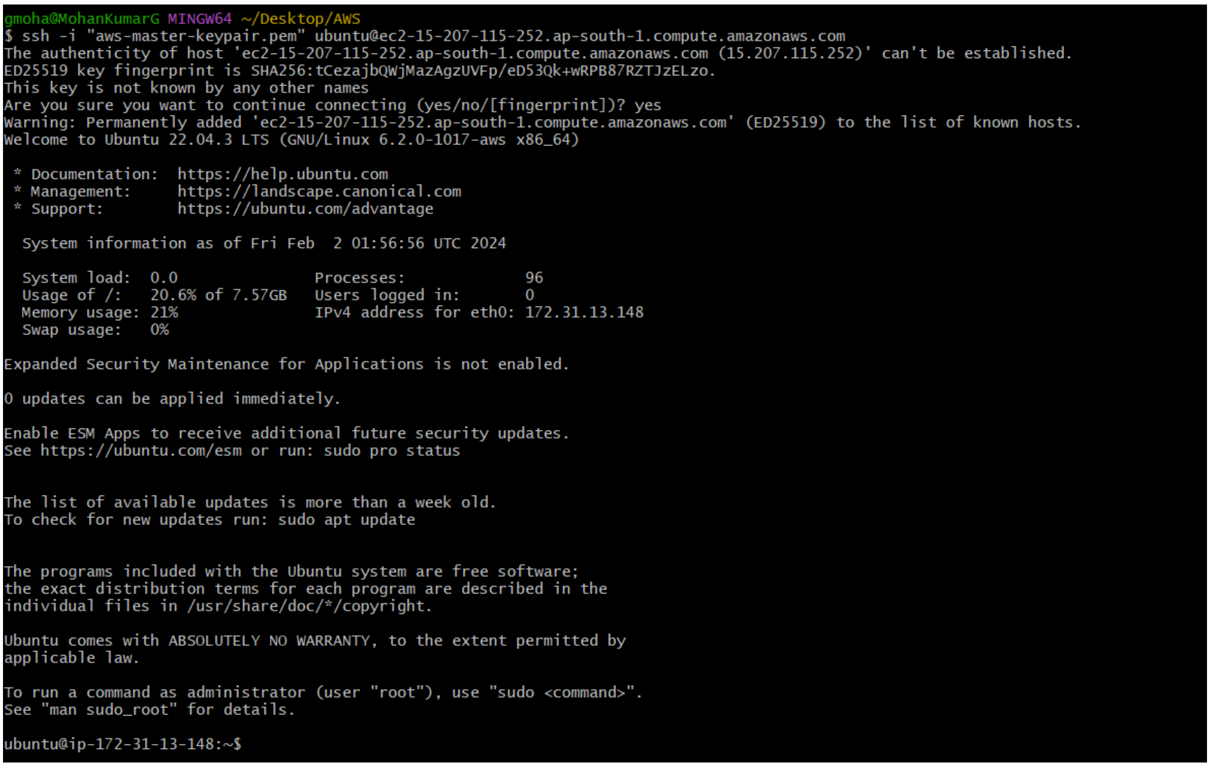
C:\Users\gmoha\Desktop\AW!

Start backup > Desktop > AWS

Name	Date modified	Type	Size
aws-master-keypair.pem	02-06-2023 16:59	PEM File	2 KB



```
gmoha@MohanKumarG MINGW64 ~/Desktop/AWS
$ ls -larth
total 21K
-rw-r--r-- 1 gmoha 197609 1.7K Jun  2  2023  aws-master-keypair.pem
drwxr-xr-x 1 gmoha 197609    0 Jun  2  2023  ./
```

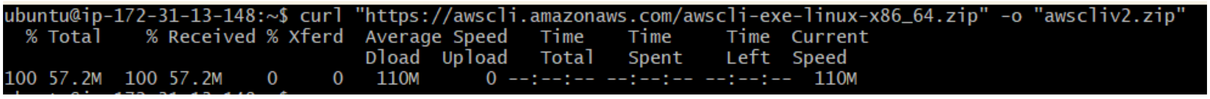


```
gmoha@MohanKumarG MINGW64 ~/Desktop/AWS
$ ssh -i "aws-master-keypair.pem" ubuntu@ec2-15-207-115-252.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-15-207-115-252.ap-south-1.compute.amazonaws.com (15.207.115.252)' can't be established.
ED25519 key fingerprint is SHA256:tCezajbQWjMazAgzUVFp/eD53Qk+wRPB87RZTJzELzo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-15-207-115-252.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1017-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Feb  2 01:56:56 UTC 2024

  System load:  0.0               Processes:             96
  Usage of /:   20.6% of 7.57GB   Users logged in:       0
  Memory usage: 21%               IPv4 address for eth0: 172.31.13.148
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-13-148:~$
```

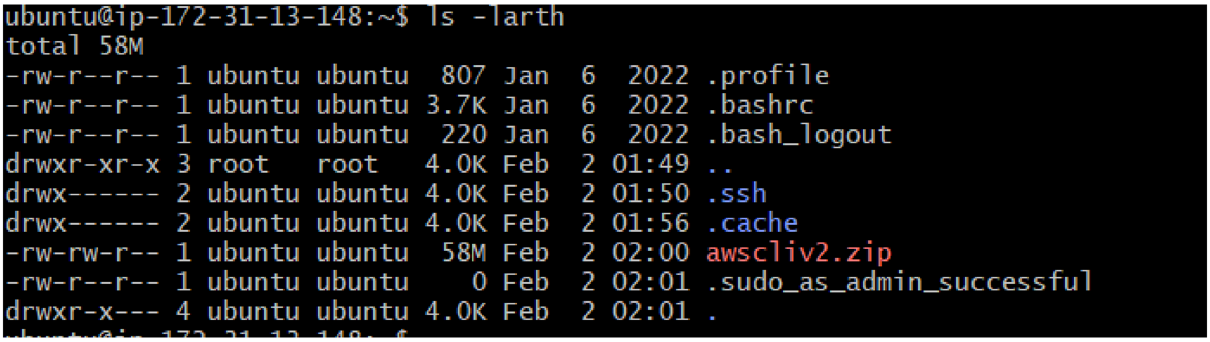
11. Install the AWS CLI in the EC2 Instances
    Follow the link to get the AWS CLI installation instructions:
    https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html

    To install the AWS CLI, run the following commands.

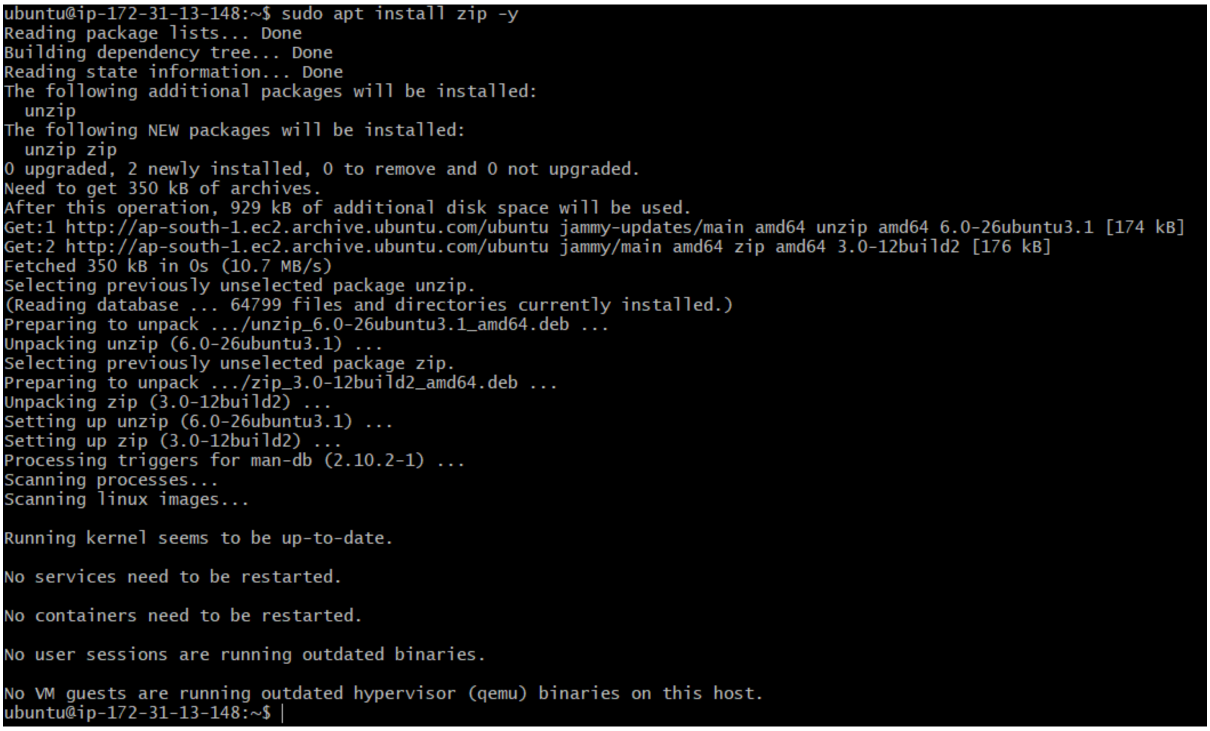
    curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
    sudo apt install zip -y
    unzip awscliv2.zip
    sudo ./aws/install



```
ubuntu@ip-172-31-13-148:~$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 57.2M  100 57.2M    0     0   110M      0 --:--:-- --:--:-- --:--:--  110M
```

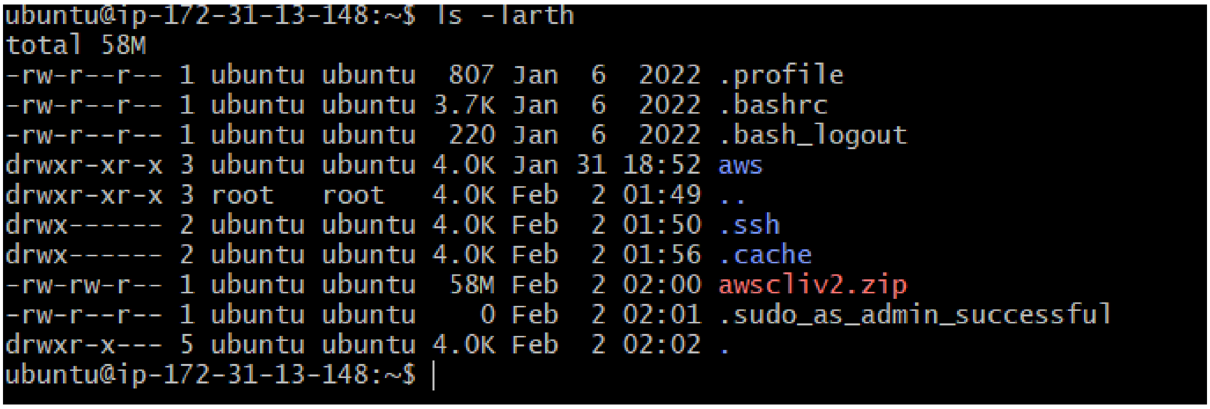


```
ubuntu@ip-172-31-13-148:~$ ls -larth
total 58M
-rw-r--r-- 1 ubuntu ubuntu  807 Jan  6  2022 .profile
-rw-r--r-- 1 ubuntu ubuntu 3.7K Jan  6  2022 .bashrc
-rw-r--r-- 1 ubuntu ubuntu  220 Jan  6  2022 .bash_logout
drwxr-xr-x 3 root   root   4.0K Feb  2 01:49 ..
drwx------ 2 ubuntu ubuntu 4.0K Feb  2 01:50 .ssh
drwx------ 2 ubuntu ubuntu 4.0K Feb  2 01:56 .cache
-rw-rw-r-- 1 ubuntu ubuntu  58M Feb  2 02:00 awscliv2.zip
-rw-r--r-- 1 ubuntu ubuntu    0 Feb  2 02:01 .sudo_as_admin_successful
drwxr-x--- 4 ubuntu ubuntu 4.0K Feb  2 02:01 .
```



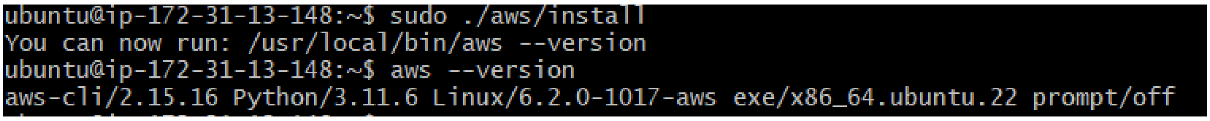
```
ubuntu@ip-172-31-13-148:~$ sudo apt install zip -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  unzip
The following NEW packages will be installed:
  unzip zip
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 350 kB of archives.
After this operation, 929 kB of additional disk space will be used.
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 unzip amd64 6.0-26ubuntu3.1 [174 kB]
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 zip amd64 3.0-12build2 [176 kB]
Fetched 350 kB in 0s (10.7 MB/s)
Selecting previously unselected package unzip.
(Reading database ... 64799 files and directories currently installed.)
Preparing to unpack .../unzip_6.0-26ubuntu3.1_amd64.deb ...
Unpacking unzip (6.0-26ubuntu3.1) ...
Selecting previously unselected package zip.
Preparing to unpack .../zip_3.0-12build2_amd64.deb ...
Unpacking zip (3.0-12build2) ...
Setting up unzip (6.0-26ubuntu3.1) ...
Setting up zip (3.0-12build2) ...
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-13-148:~$ |
```

Unzip the awscliv2.zip file with this command unzip awscliv2.zip.
After unzipping the awscliv2.zip file you will get the aws folder.



```
ubuntu@ip-172-31-13-148:~$ ls -larth
total 58M
-rw-r--r-- 1 ubuntu ubuntu  807 Jan  6  2022 .profile
-rw-r--r-- 1 ubuntu ubuntu 3.7K Jan  6  2022 .bashrc
-rw-r--r-- 1 ubuntu ubuntu  220 Jan  6  2022 .bash_logout
drwxr-xr-x 3 ubuntu ubuntu 4.0K Jan 31 18:52 aws
drwxr-xr-x 3 root   root   4.0K Feb  2 01:49 ..
drwx------ 2 ubuntu ubuntu 4.0K Feb  2 01:50 .ssh
drwx------ 2 ubuntu ubuntu 4.0K Feb  2 01:56 .cache
-rw-rw-r-- 1 ubuntu ubuntu  58M Feb  2 02:00 awscliv2.zip
-rw-r--r-- 1 ubuntu ubuntu    0 Feb  2 02:01 .sudo_as_admin_successful
drwxr-x--- 5 ubuntu ubuntu 4.0K Feb  2 02:02 .
ubuntu@ip-172-31-13-148:~$ |
```

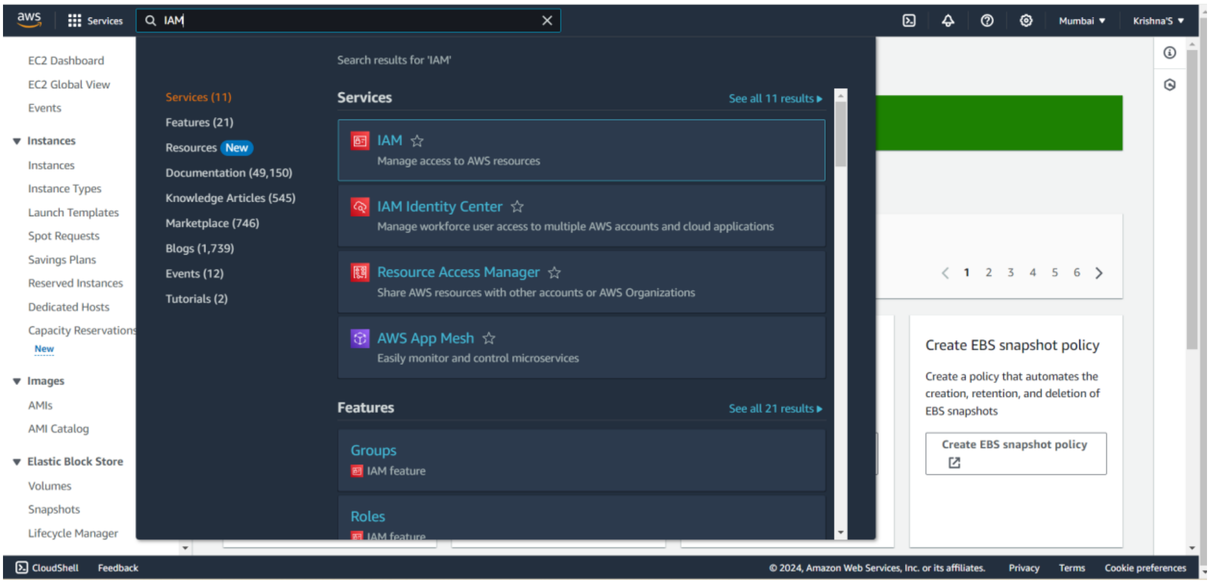
Install the AWS CLI by running the below command sudo ./aws/install



```
ubuntu@ip-172-31-13-148:~$ sudo ./aws/install
You can now run: /usr/local/bin/aws --version
ubuntu@ip-172-31-13-148:~$ aws --version
aws-cli/2.15.16 Python/3.11.6 Linux/6.2.0-1017-aws exe/x86_64.ubuntu.22 prompt/off
```

3. Create an IAM Policy for a Role to put the objects on the S3 bucket

1. Search IAM Service on the Search Bar



Search results for 'IAM'

IAM ☆
Manage access to AWS resources

IAM Identity Center ☆
Manage workforce user access to multiple AWS accounts and cloud applications

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

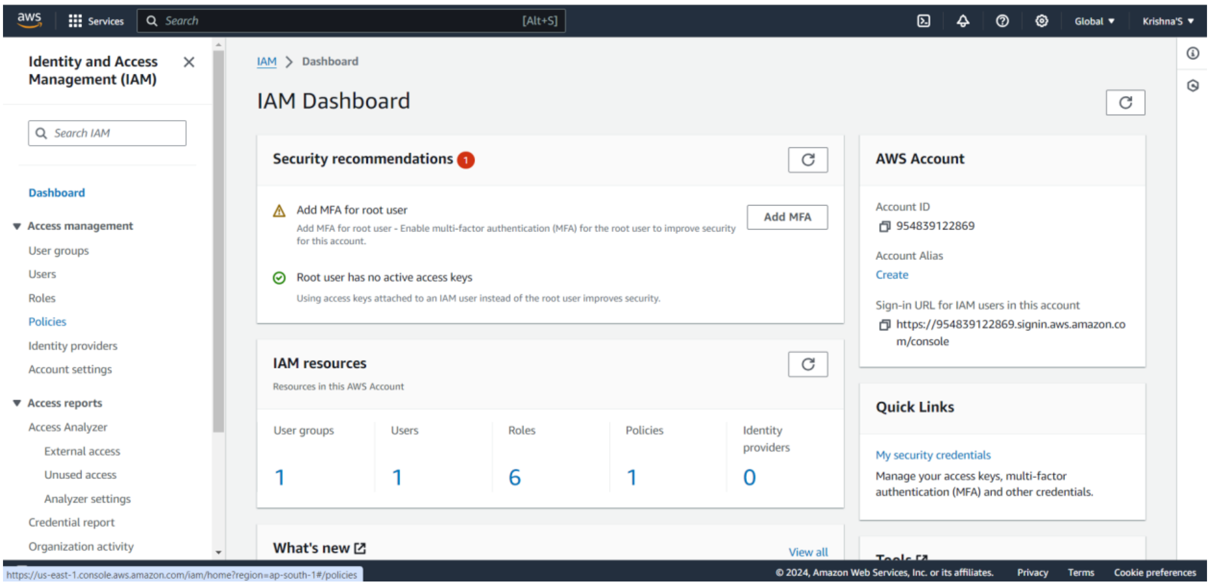
AWS App Mesh ☆
Easily monitor and control microservices

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots

© 2024, Amazon Web Services, Inc. or its affiliates.

2. Click on Policies



IAM Dashboard

Security recommendations 1

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.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

IAM resources
Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
1	1	6	1	0

AWS Account

Account ID
954839122869

Account Alias
Create

Sign-in URL for IAM users in this account
https://954839122869.signin.aws.amazon.com/console

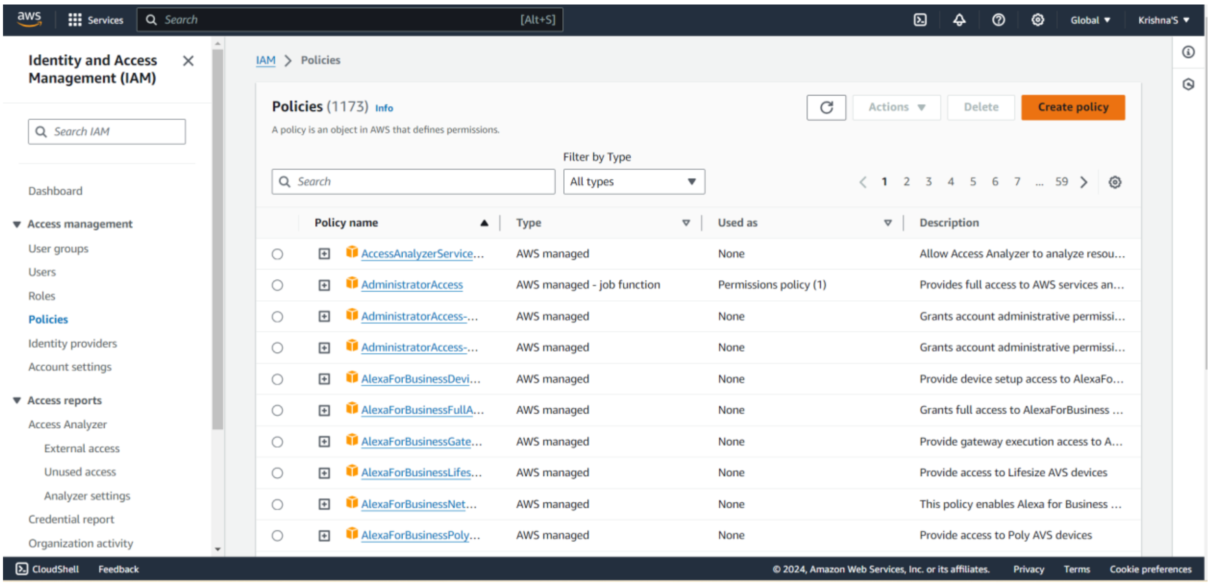
Quick Links

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

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies

© 2024, Amazon Web Services, Inc. or its affiliates.

3. Click on Create Policy

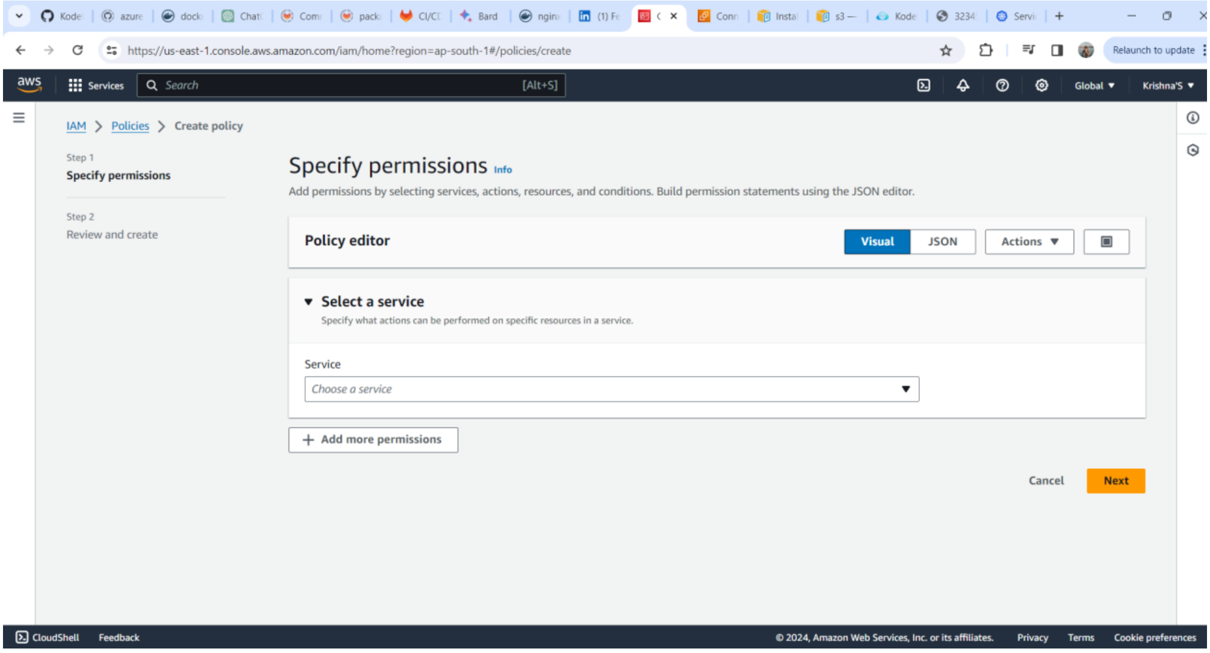


Policies (1173) Info

A policy is an object in AWS that defines permissions.

	Policy name	Type	Used as	Description
○	AccessAnalyzerService...	AWS managed	None	Allow Access Analyzer to analyze resou...
○	AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services an...
○	AdministratorAccess-...	AWS managed	None	Grants account administrative permissi...
○	AdministratorAccess-...	AWS managed	None	Grants account administrative permissi...
○	AlexaForBusinessDevi...	AWS managed	None	Provide device setup access to AlexaFo...
○	AlexaForBusinessFullA...	AWS managed	None	Grants full access to AlexaForBusiness ...
○	AlexaForBusinessGate...	AWS managed	None	Provide gateway execution access to A...
○	AlexaForBusinessLifes...	AWS managed	None	Provide access to Lifesize AVS devices
○	AlexaForBusinessNet...	AWS managed	None	This policy enables Alexa for Business ...
○	AlexaForBusinessPoly...	AWS managed	None	Provide access to Poly AVS devices

4. Select the S3 service



Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

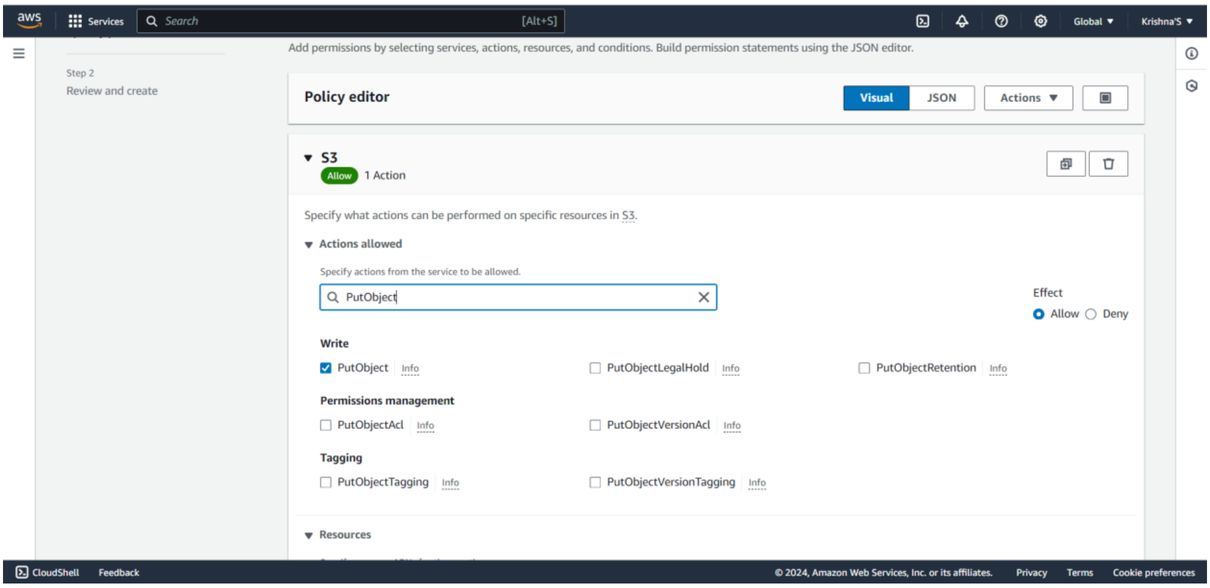
Policy editor

Select a service

Specify what actions can be performed on specific resources in a service.

Service: Choose a service

5. Select Action Allowed as PutObject



Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

▼ S3

Allow 1 Action

Specify what actions can be performed on specific resources in S3.

▼ Actions allowed

Specify actions from the service to be allowed.

PutObject

Effect

● Allow ○ Deny

Write

☑ PutObject Info □ PutObjectLegalHold Info □ PutObjectRetention Info

Permissions management

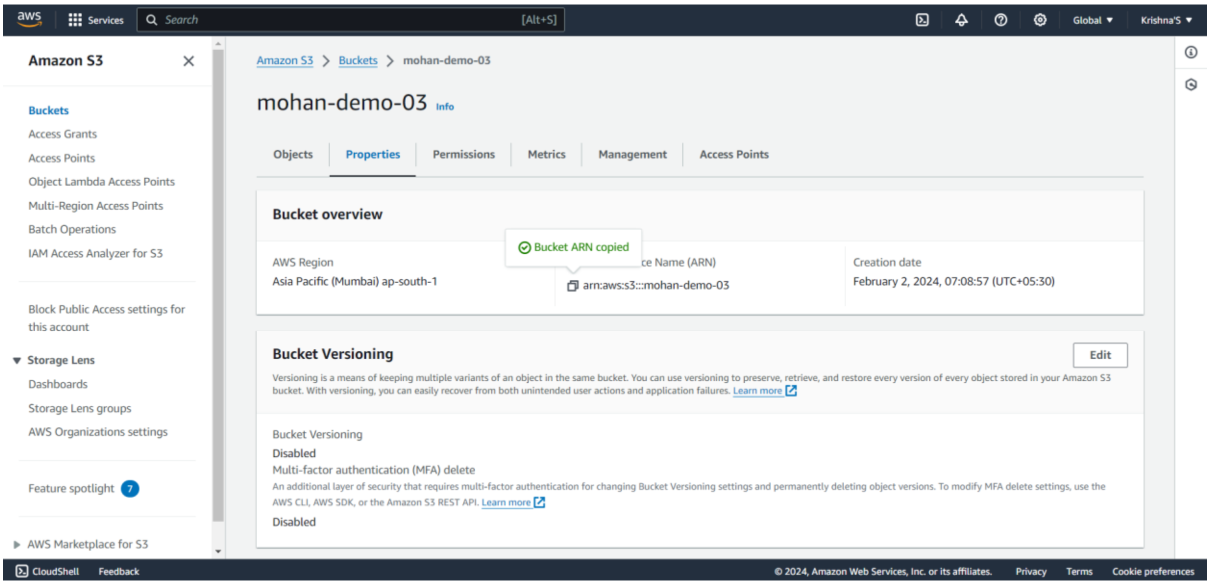
□ PutObjectAcl Info □ PutObjectVersionAcl Info

Tagging

□ PutObjectTagging Info □ PutObjectVersionTagging Info

▼ Resources

6. Selected the 3rd S3 Bucket arn



mohan-demo-03 Info

Bucket overview

Bucket ARN copied

AWS Region
Asia Pacific (Mumbai) ap-south-1

ce Name (ARN)
arn:aws:s3:::mohan-demo-03

Creation date
February 2, 2024, 07:08:57 (UTC+05:30)

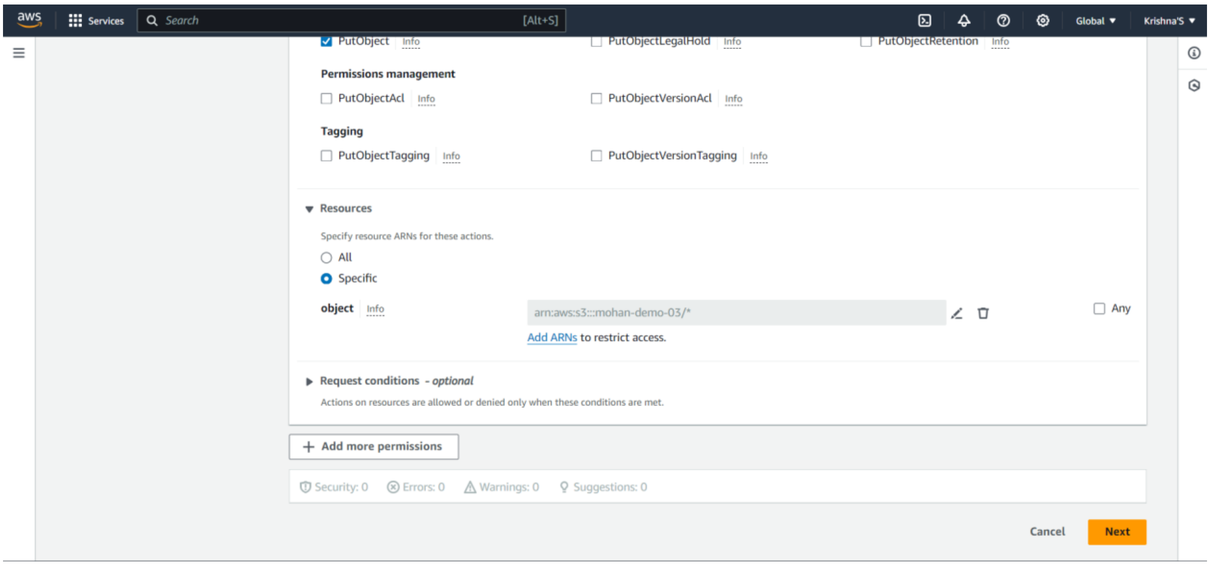
Bucket Versioning

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
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

7. Click on the ADD ARN add S3 Bucket ARN and click on Next



☑ PutObject Info □ PutObjectLegalHold Info □ PutObjectRetention Info

Permissions management

□ PutObjectAcl Info □ PutObjectVersionAcl Info

Tagging

□ PutObjectTagging Info □ PutObjectVersionTagging Info

▼ Resources

Specify resource ARNs for these actions.

○ All
● Specific

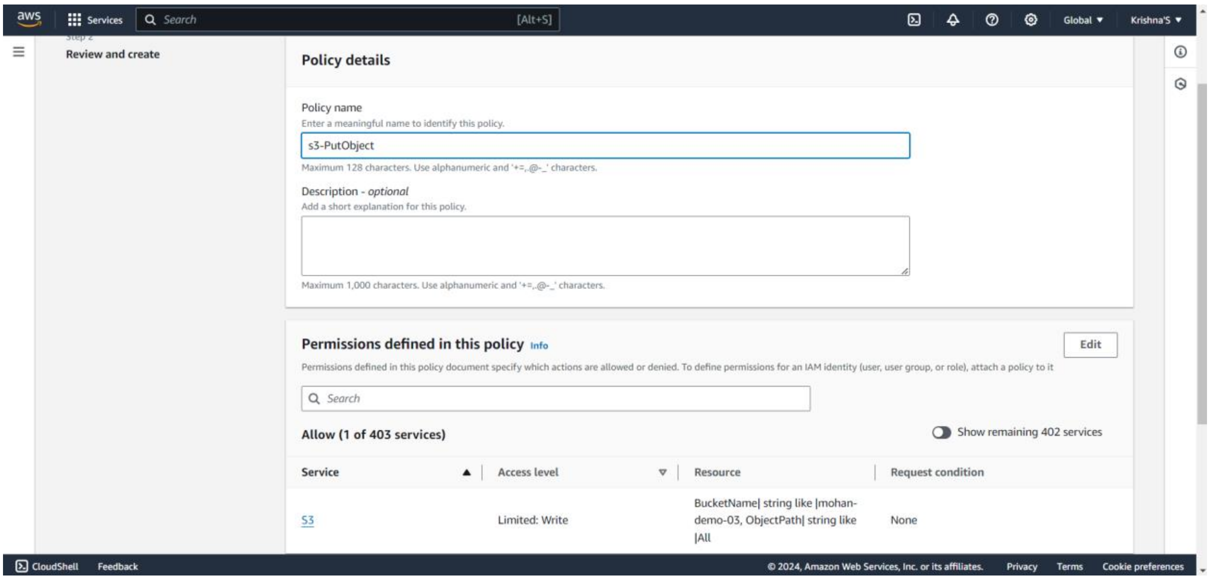
object Info arn:aws:s3:::mohan-demo-03/* □ Any

Add ARNs to restrict access.

▶ Request conditions - *optional*

Actions on resources are allowed or denied only when these conditions are met.

8. Enter the Policy Name and then click on Create Policy



Policy details

Policy name
Enter a meaningful name to identify this policy.
s3-PutObject
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.

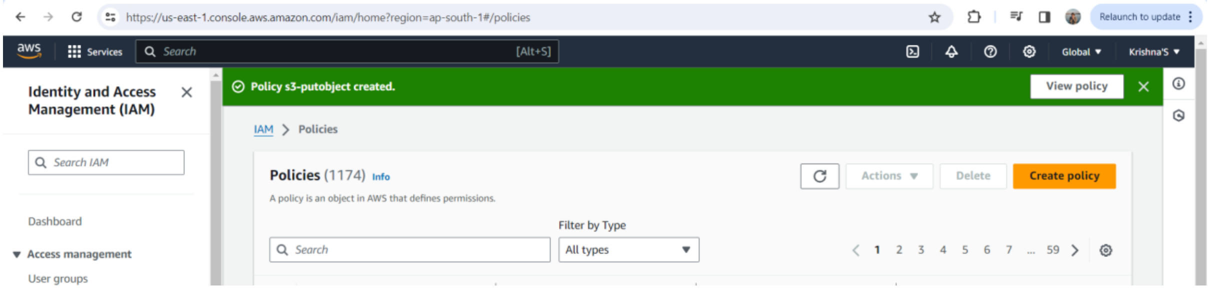
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

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

Allow (1 of 403 services)

Service	Access level	Resource	Request condition
S3	Limited: Write	BucketName| string like |mohan-demo-03, ObjectPath| string like |All	None

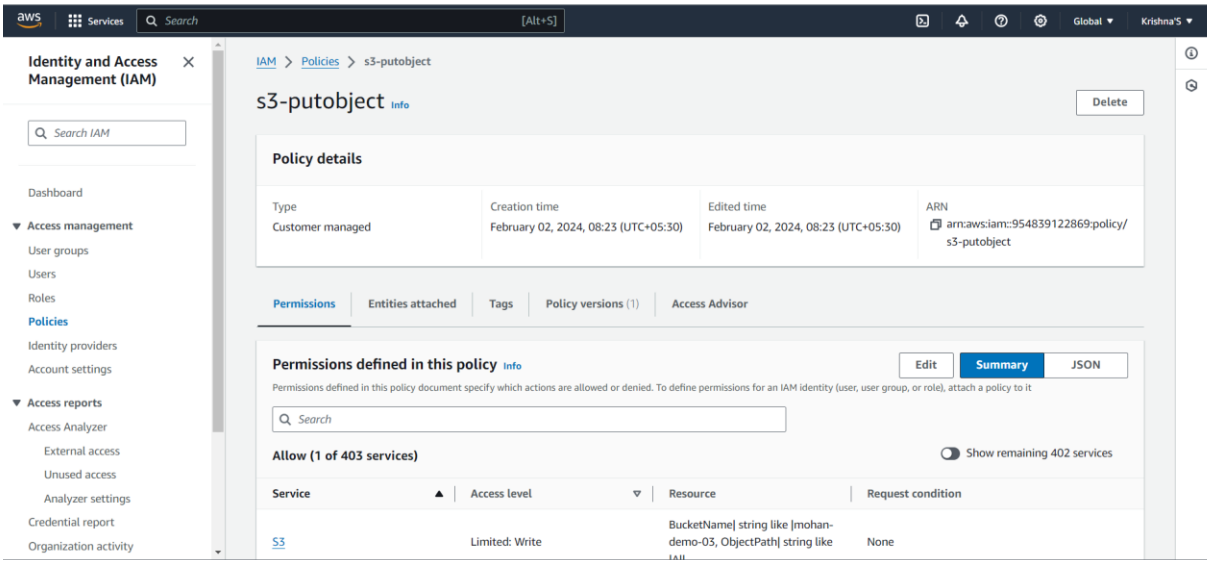


https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies
Relaunch to update
aws
Services
Search
[Alt+S]
Global ▾
Krishna'S ▾
Identity and Access Management (IAM)
Search IAM
Dashboard
▼ Access management
User groups

Policy s3-putobject created.

Policies (1174) Info

A policy is an object in AWS that defines permissions.



s3-putobject

Policy details

Type	Creation time	Edited time	ARN
Customer managed	February 02, 2024, 08:23 (UTC+05:30)	February 02, 2024, 08:23 (UTC+05:30)	arn:aws:iam::954839122869:policy/s3-putobject

Permissions defined in this policy

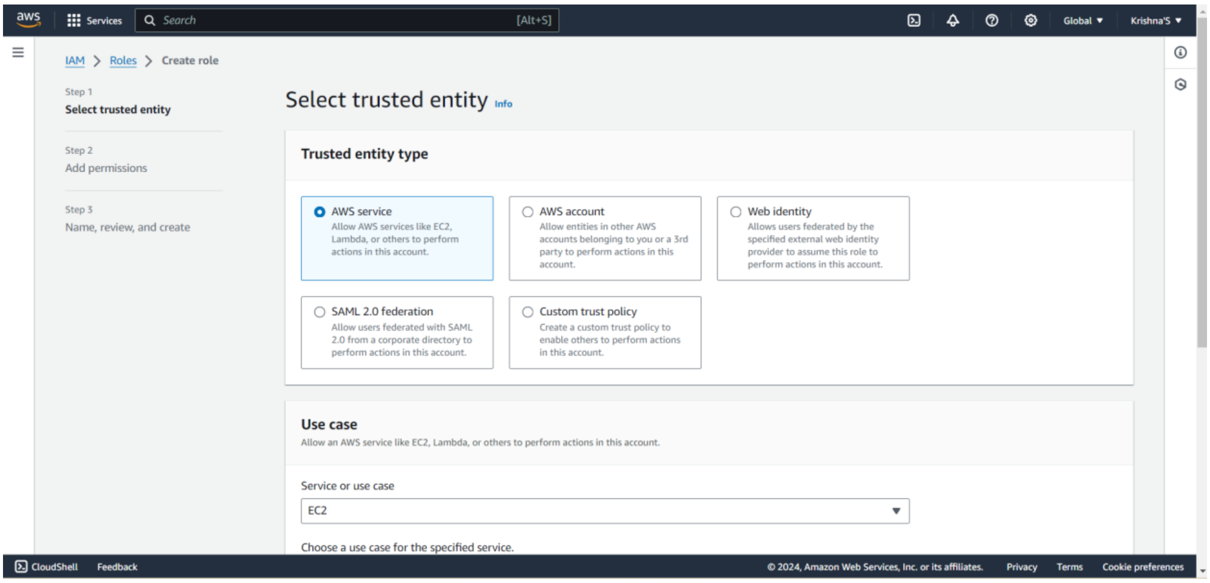
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 403 services)

Service	Access level	Resource	Request condition
S3	Limited: Write	BucketName| string like |mohan-demo-03, ObjectPath| string like |All	None

4. Create a Role to Attach the previously created Policy.

1. Click on Roles and Click on Create Role. Select the Trust entity type as **AWS Service** and Use Case as **EC2** and Click on Next



Select trusted entity

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.

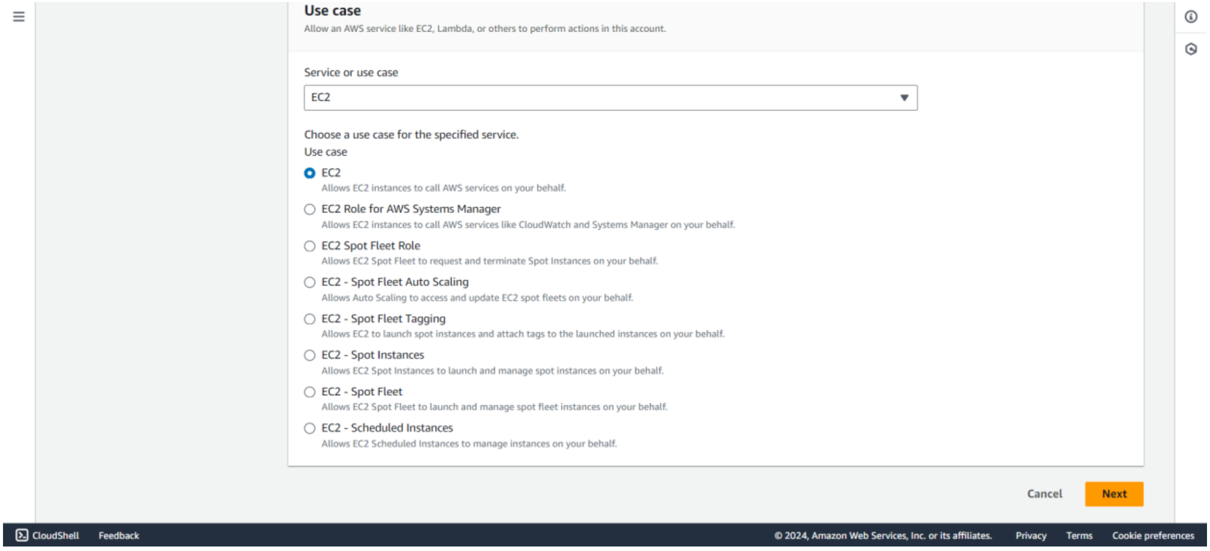
Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2 ▾

Choose a use case for the specified service.



Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

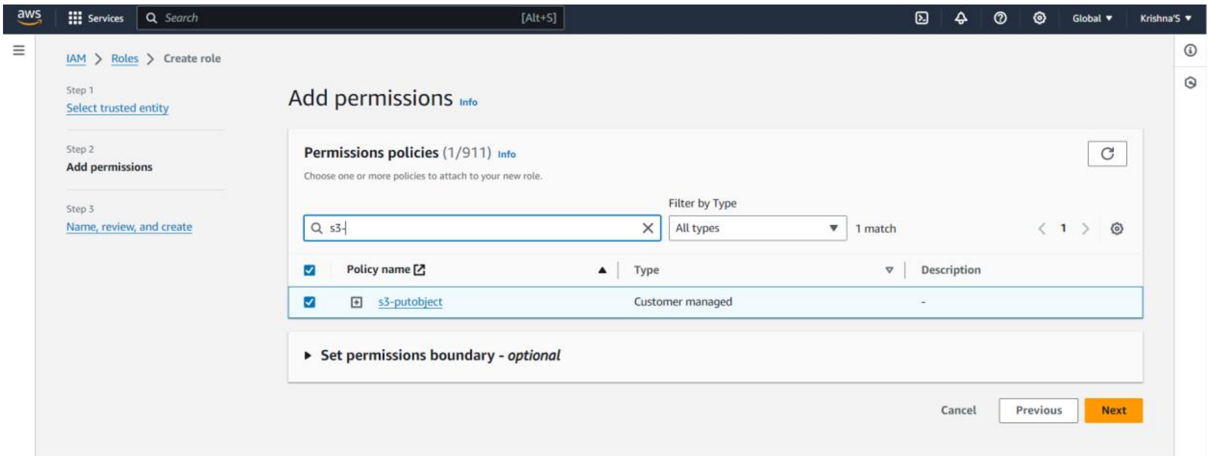
EC2

Choose a use case for the specified service.

Use case

- ● EC2
  Allows EC2 instances to call AWS services on your behalf.
- ○ EC2 Role for AWS Systems Manager
  Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- ○ EC2 Spot Fleet Role
  Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- ○ EC2 - Spot Fleet Auto Scaling
  Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- ○ EC2 - Spot Fleet Tagging
  Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- ○ EC2 - Spot Instances
  Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
- ○ EC2 - Spot Fleet
  Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- ○ EC2 - Scheduled Instances
  Allows EC2 Scheduled Instances to manage instances on your behalf.

2. Add the Permissions. Search the Previously created s3-putobject and click on the next



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

Permissions policies (1/911) Info

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

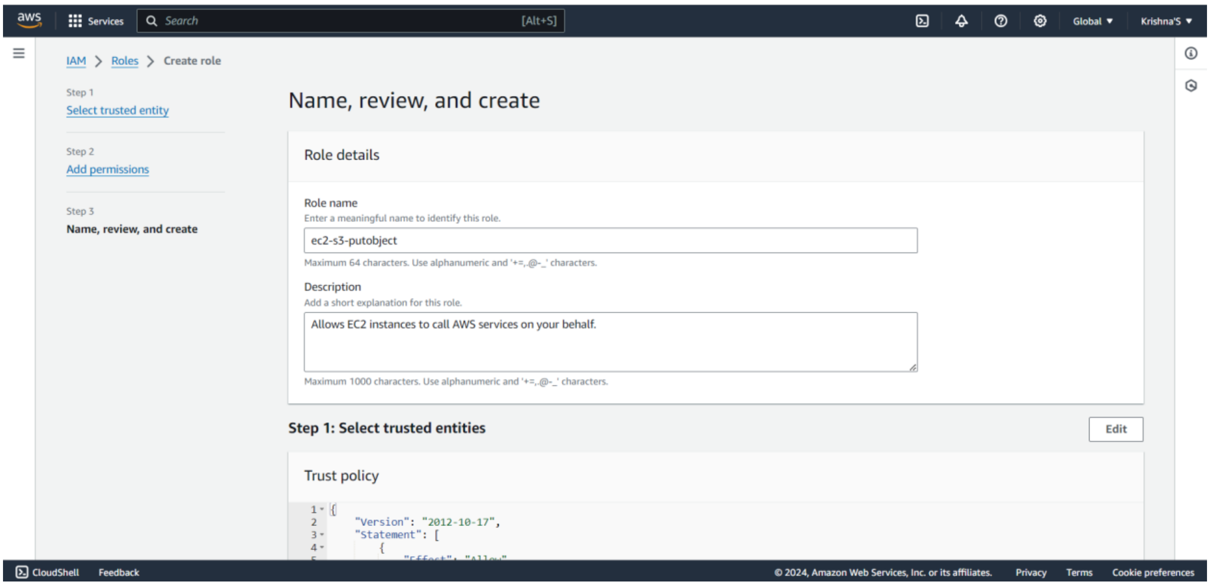
Filter by Type

s3- | All types | 1 match

☑	Policy name	Type	Description
☑	s3-putobject	Customer managed	-

▸ **Set permissions boundary - *optional***

3. Enter the Role Name and then Click on Create Role.



IAM > Roles > Create role

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.

ec2-s3-putobject

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

Description
Add a short explanation for this role.

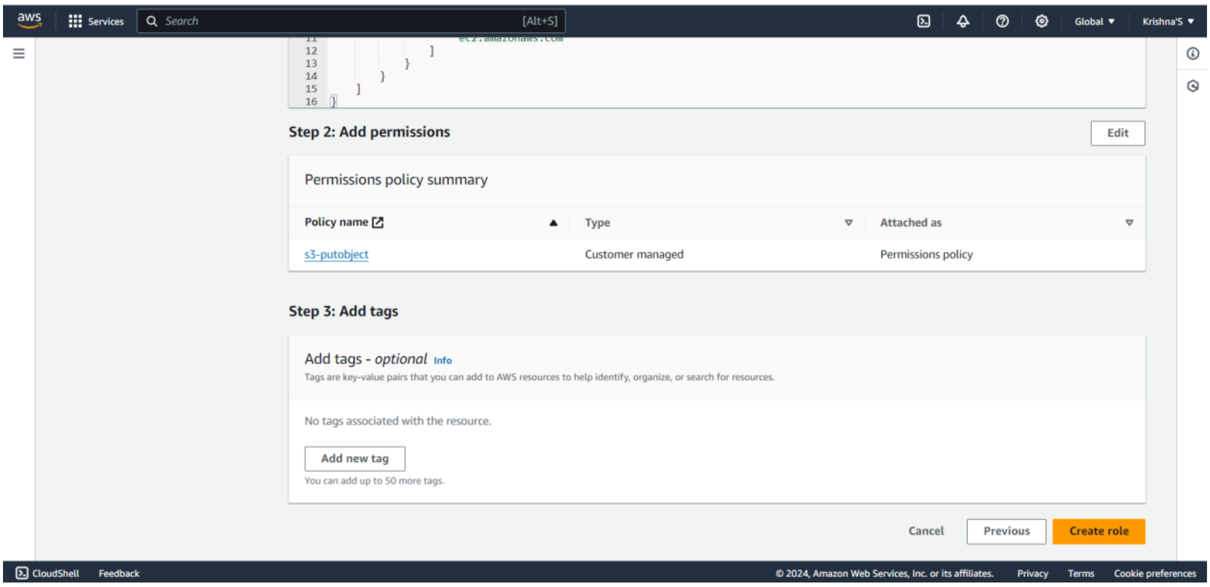
Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```



```
                ]
            }
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
s3-putobject	Customer managed	Permissions policy

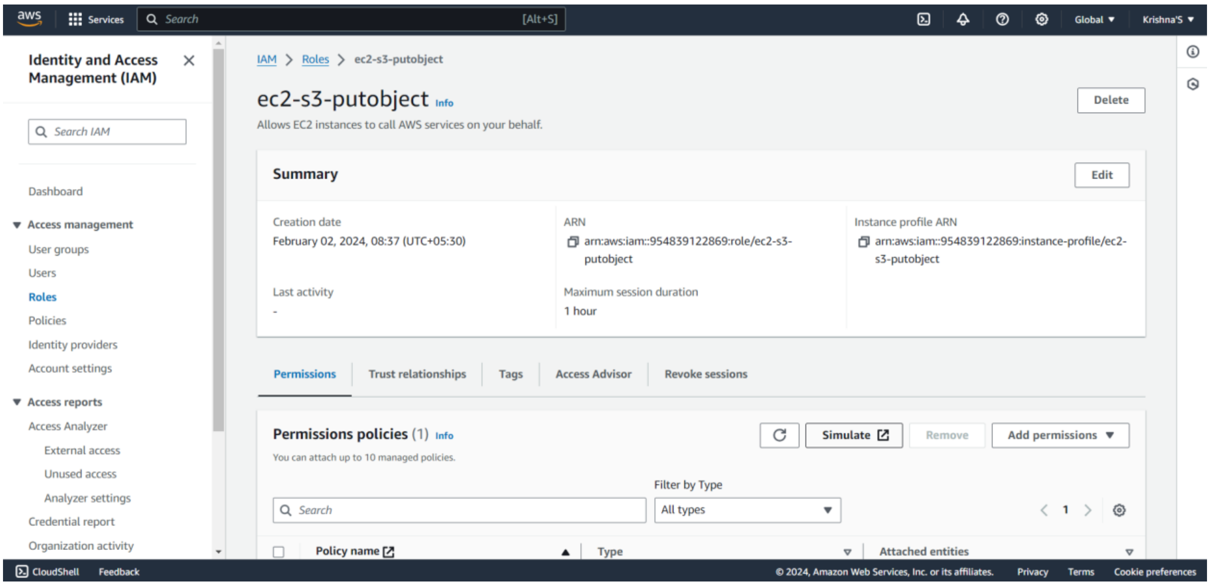
Step 3: Add tags

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.

You can add up to 50 more tags.



IAM > Roles > ec2-s3-putobject

ec2-s3-putobject Info

Allows EC2 instances to call AWS services on your behalf.

Summary

Creation date: February 02, 2024, 08:37 (UTC+05:30)

ARN: arn:aws:iam::954839122869:role/ec2-s3-putobject

Instance profile ARN: arn:aws:iam::954839122869:instance-profile/ec2-s3-putobject

Last activity: -

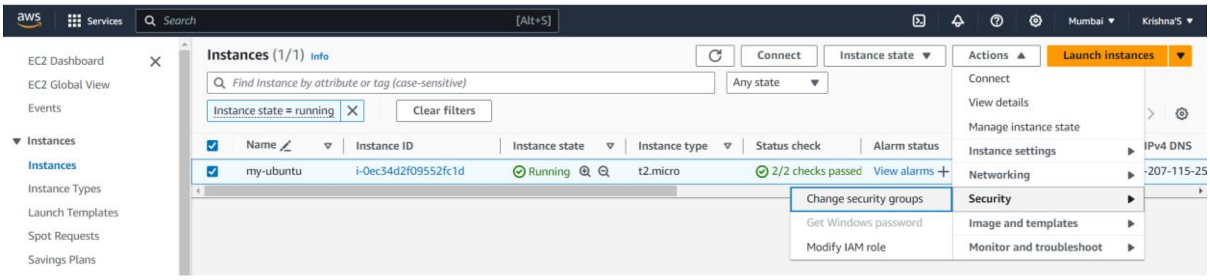
Maximum session duration: 1 hour

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type: All types

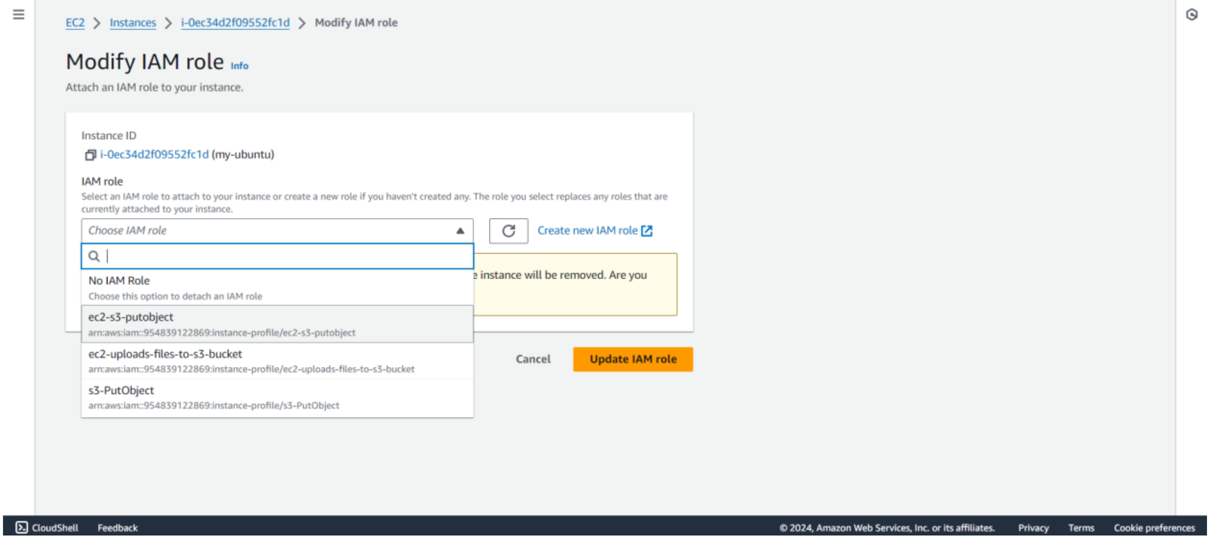
4. Go to the EC2 Instance and Attach ec2-s3-putoject role. Click on EC2 Instance Click on Actions and Click on Security and Modify IAM Role



Instances (1/1) Info

Instance state = running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	IPv4 DNS
my-ubuntu	i-0ec34d2f09552fc1d	Running	t2.micro	2/2 checks passed	View alarms +	-207-115-25


EC2 > Instances > i-0ec34d2f09552fc1d > Modify IAM role
Info
Create new IAM role
Cancel
Update IAM role
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Modify IAM role

Attach an IAM role to your instance.

Instance ID
i-0ec34d2f09552fc1d (my-ubuntu)

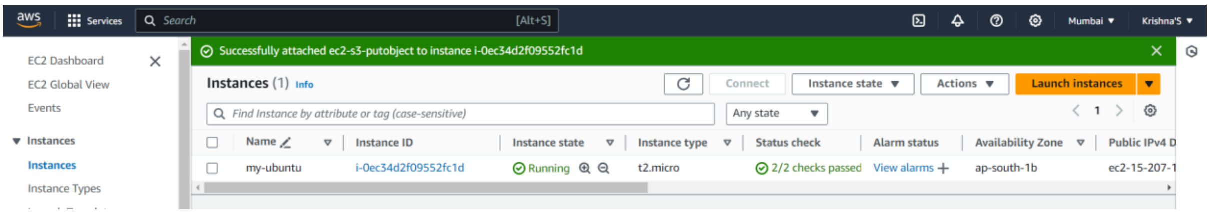
IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

Choose IAM role

- No IAM Role
  Choose this option to detach an IAM role
- ec2-s3-putobject
  arn:aws:iam::954839122869:instance-profile/ec2-s3-putobject
- ec2-uploads-files-to-s3-bucket
  arn:aws:iam::954839122869:instance-profile/ec2-uploads-files-to-s3-bucket
- s3-PutObject
  arn:aws:iam::954839122869:instance-profile/s3-PutObject

…e instance will be removed. Are you

Select the ec2-s3-putobject role and click on Update IAM role



Successfully attached ec2-s3-putobject to instance i-0ec34d2f09552fc1d

Instances (1) Info

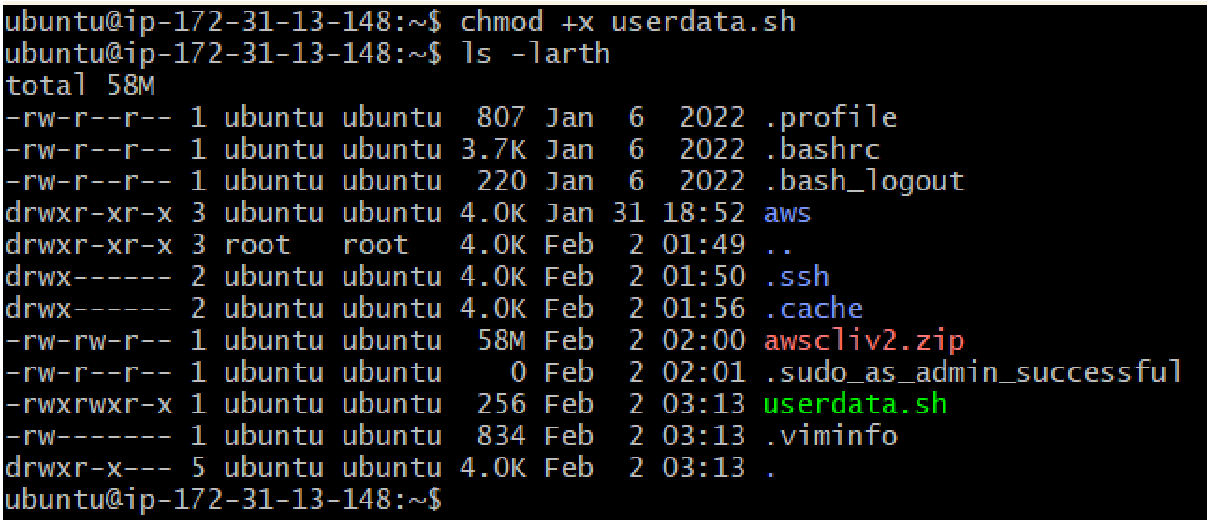
Find Instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
□	my-ubuntu	i-0ec34d2f09552fc1d	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-15-207-1

Go to the terminal and Create a script that should upload a text file with the instance's Private IP Address and Hostname to the S3 Bucket

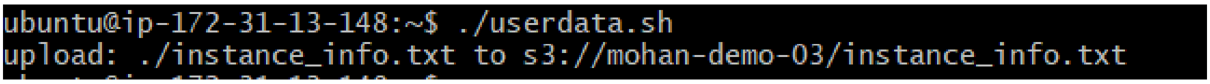
```
vi userdata.sh

#!/bin/bash

# Create a text file with Private IP Address and Hostname
echo "Private IP: $(hostname -I)" > instance_info.txt
echo "Hostname: $(hostname)" >> instance_info.txt

# Upload the file to S3 bucket
aws s3 cp instance_info.txt s3://mohan-demo-03/
```

Provide the Execute Permission to the Script

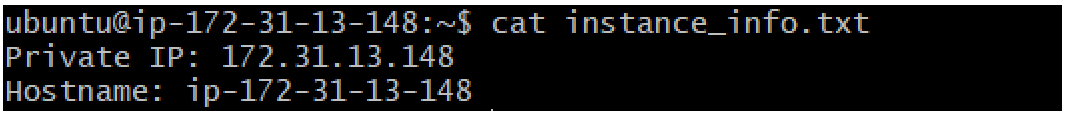


```
ubuntu@ip-172-31-13-148:~$ chmod +x userdata.sh
ubuntu@ip-172-31-13-148:~$ ls -larth
total 58M
-rw-r--r-- 1 ubuntu ubuntu  807 Jan  6  2022 .profile
-rw-r--r-- 1 ubuntu ubuntu 3.7K Jan  6  2022 .bashrc
-rw-r--r-- 1 ubuntu ubuntu  220 Jan  6  2022 .bash_logout
drwxr-xr-x 3 ubuntu ubuntu 4.0K Jan 31 18:52 aws
drwxr-xr-x 3 root   root   4.0K Feb  2 01:49 ..
drwx------ 2 ubuntu ubuntu 4.0K Feb  2 01:50 .ssh
drwx------ 2 ubuntu ubuntu 4.0K Feb  2 01:56 .cache
-rw-rw-r-- 1 ubuntu ubuntu  58M Feb  2 02:00 awscliv2.zip
-rw-r--r-- 1 ubuntu ubuntu    0 Feb  2 02:01 .sudo_as_admin_successful
-rwxrwxr-x 1 ubuntu ubuntu  256 Feb  2 03:13 userdata.sh
-rw------- 1 ubuntu ubuntu  834 Feb  2 03:13 .viminfo
drwxr-x--- 5 ubuntu ubuntu 4.0K Feb  2 03:13 .
ubuntu@ip-172-31-13-148:~$
```

Run the Script to upload the file to the AWS s3 bucket

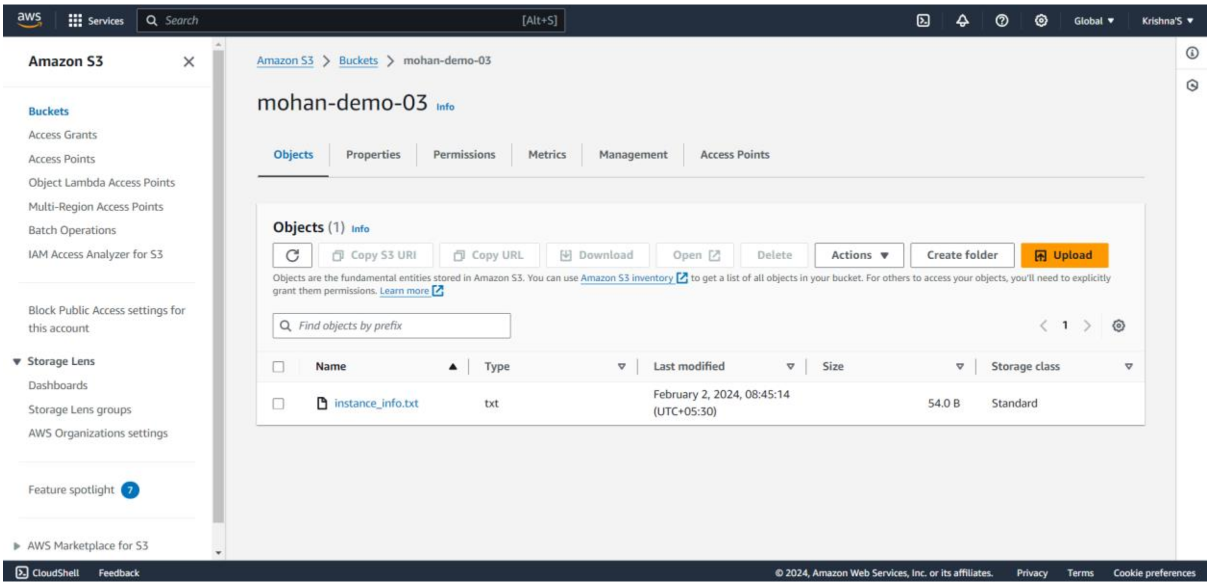


```
ubuntu@ip-172-31-13-148:~$ ./userdata.sh
upload: ./instance_info.txt to s3://mohan-demo-03/instance_info.txt
```



```
ubuntu@ip-172-31-13-148:~$ cat instance_info.txt
Private IP: 172.31.13.148
Hostname: ip-172-31-13-148
```

The script is Executed Successfully and the file is uploaded to the S3. Check the S3 Bucket to confirm whether the file is uploaded or not



mohan-demo-03

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
□	instance_info.txt	txt	February 2, 2024, 08:45:14 (UTC+05:30)	54.0 B	Standard