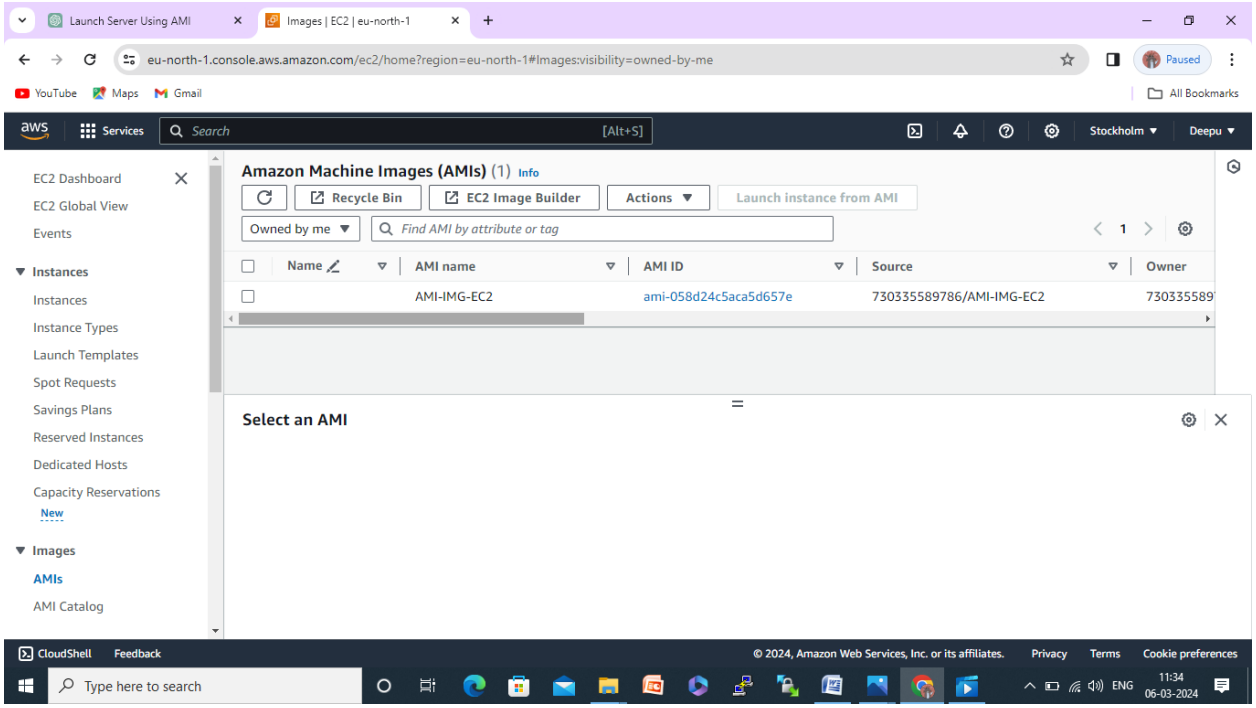
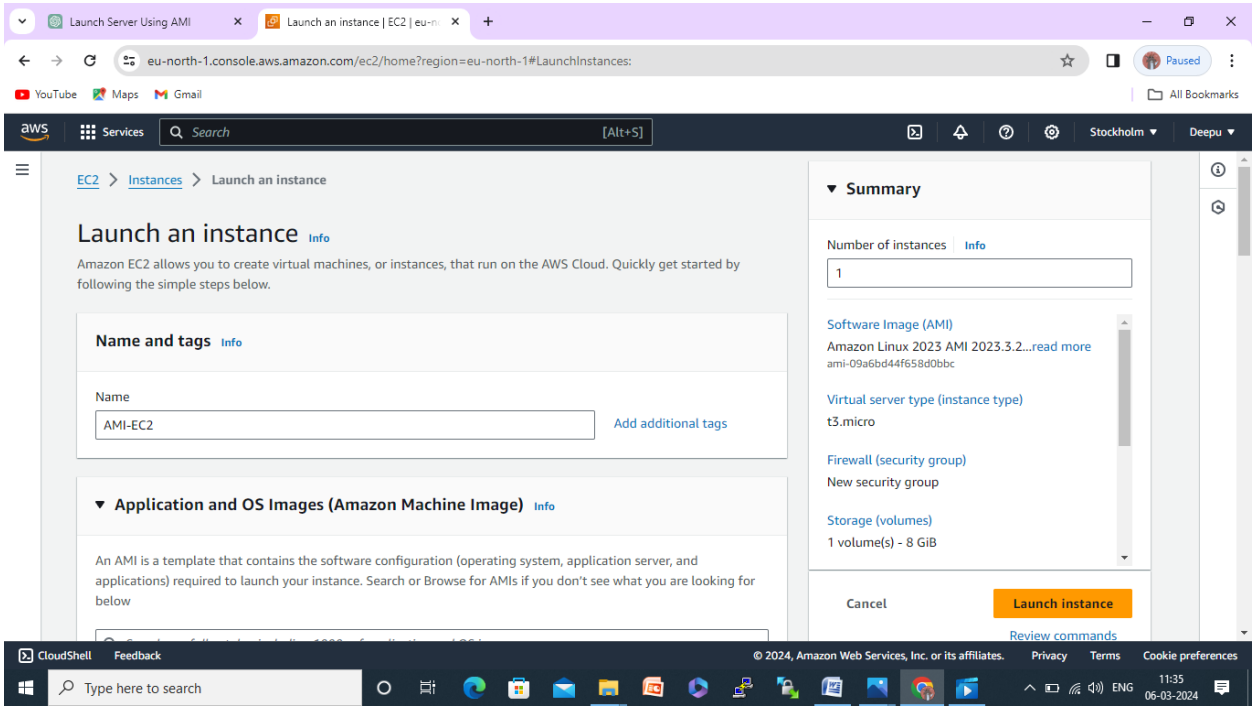
TASK

1. How to launch server using AMI?





Launch Server Using AMI | Launch an instance | EC2 | eu-n

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

Services | Search [Alt+S] | Stockholm | Deepu

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

Recents | My AMIs | Quick Start

Owned by me | Shared with me

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

AMI-IMG-EC2
ami-058d24c5aca5d657e
2024-03-06T06:01:09.000Z Virtualization: hvm ENA enabled: true Root device type: ebs

Summary

Number of instances Info: 1

Software Image (AMI)
AMI-IMG-EC2
ami-058d24c5aca5d657e

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Cancel | Launch instance

Review commands

CloudShell | Feedback | © 2024, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

Type here to search | ENG | 11:35 06-03-2024

Launch Server Using AMI | Instances | EC2 | eu-north-1

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false

Services | Search [Alt+S] | Stockholm | Deepu

EC2 Dashboard
EC2 Global View
Events

Instances
- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity Reservations New

Images
- AMIs
- AMI Catalog

Instances (2) Info

Connect | Instance state | Actions | Launch instances

Find Instance by attribute or tag (case-sensitive)

Any state

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Z
lin-ec2	i-001708b93cc8ae479	Running	t3.micro	2/2 checks passed	View alarms +	eu-north-1c
AMI-EC2	i-0754036baf49f27e9	Running	t3.micro	Initializing	View alarms +	eu-north-1c

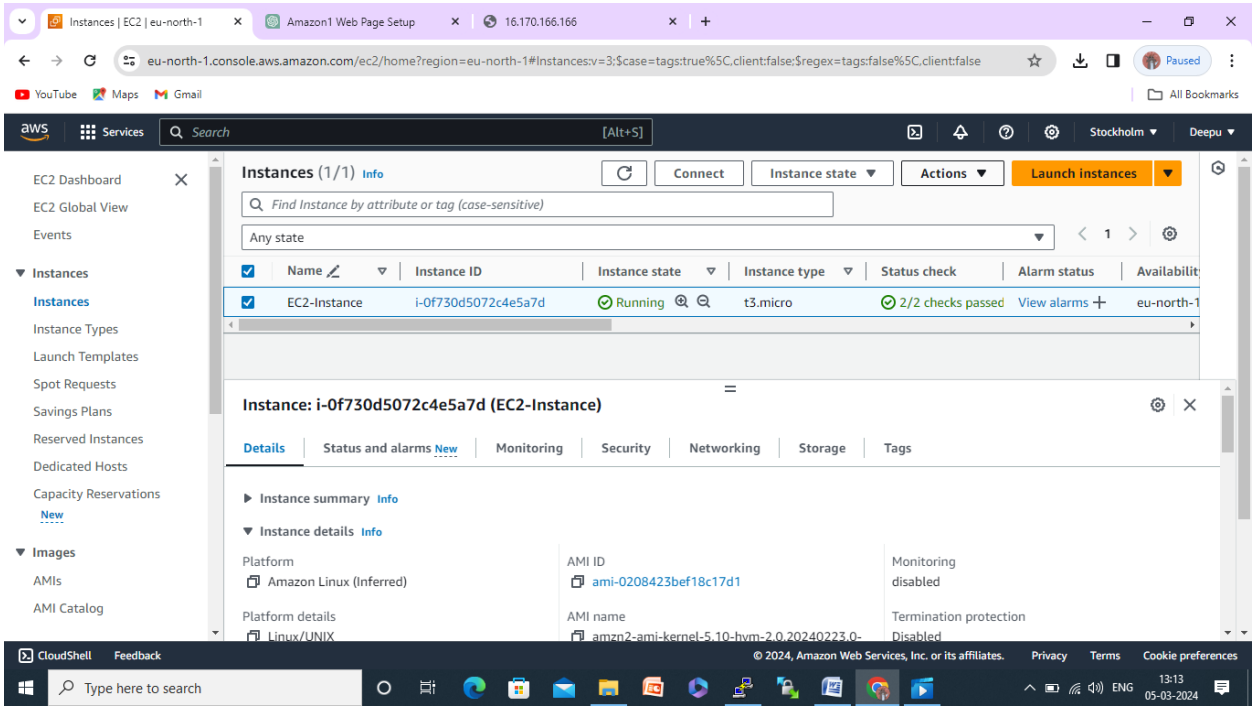
Select an instance

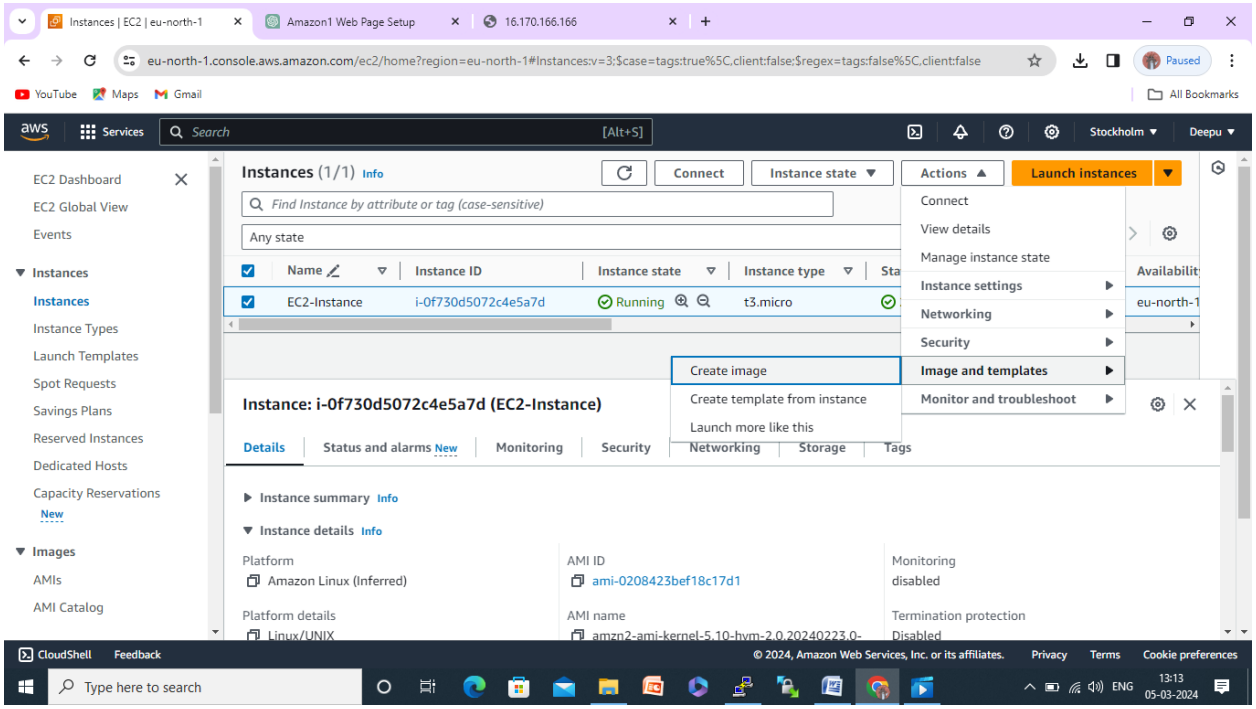
CloudShell | Feedback | © 2024, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

Type here to search | ENG | 11:36 06-03-2024

2. How to login to server if u lost your key-pair?

To login again to the server, create an AMI of the server and login with a new key-pair or with the existing one.





Create Image | EC2 | eu-north-1 | Amazon1 Web Page Setup | 16.170.166.166

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateImage:instanceId=i-0f730d5072c4e5a7d

EC2 > Instances > i-0f730d5072c4e5a7d > Create image

Create image Info

An image (also referred to as an AMI) defines the programs and settings that are applied when you launch an EC2 instance. You can create an image from the configuration of an existing instance

Instance ID
i-0f730d5072c4e5a7d (EC2-Instance)

Image name
AMI-EC2
Maximum 127 characters. Can't be modified after creation.

Image description - *optional*
FOR BACKUP
Maximum 255 characters

No reboot
Enable

Instance volumes

Images | EC2 | eu-north-1 | Amazon1 Web Page Setup | 16.170.166.166

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Images:visibility=owned-by-me

AMIs
AMI Catalog
Elastic Block Store
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Load Balancing
Load Balancers
Target Groups
Trust Stores New
Auto Scaling
Auto Scaling Groups

Amazon Machine Images (AMIs) (1/1) Info

Recycle Bin | EC2 Image Builder | Actions | Launch instance from AMI

Owned by me | Find AMI by attribute or tag

Name	AMI name	AMI ID	Source	Owner
AMI-EC2	AMI-EC2	ami-05d06222ecfe33e7c	730335589786/AMI-EC2	730335589

AMI ID: ami-05d06222ecfe33e7c (AMI-EC2)

Details | Permissions | Storage | Tags

AMI ID ami-05d06222ecfe33e7c (AMI-EC2)	Image type machine	Platform details Linux/UNIX	Root device type EBS
AMI name AMI-EC2	Owner account ID 730335589786	Architecture x86_64	Usage operation RunInstances
Root device name	Status	Source	Virtualization type

Launch an instance | EC2 | eu-n | Amazon1 Web Page Setup | 16.170.166.166

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

YouTube Maps Gmail All Bookmarks

aws Services Search [Alt+S] Stockholm Deepu

Launch an instance Info

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

Name and tags Info

Name

AMI-Instance

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

Recents | My AMIs | Quick Start

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

ami-02d0a1cbe2c3e5ae4

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel | Launch instance

Review commands

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 13:17 05-03-2024

Launch an instance | EC2 | eu-n | Amazon1 Web Page Setup | 16.170.166.166

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:

YouTube Maps Gmail All Bookmarks

aws Services Search [Alt+S] Stockholm Deepu

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

Recents | My AMIs | Quick Start

Owned by me | Shared with me

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

AMI-EC2

ami-05d06222ecfe33e7c

2024-03-05T07:43:56.000Z Virtualization: hvm ENA enabled: true Root device type: ebs

Summary

Number of instances Info

1

Software Image (AMI)

FOR BACKUP

ami-05d06222ecfe33e7c

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

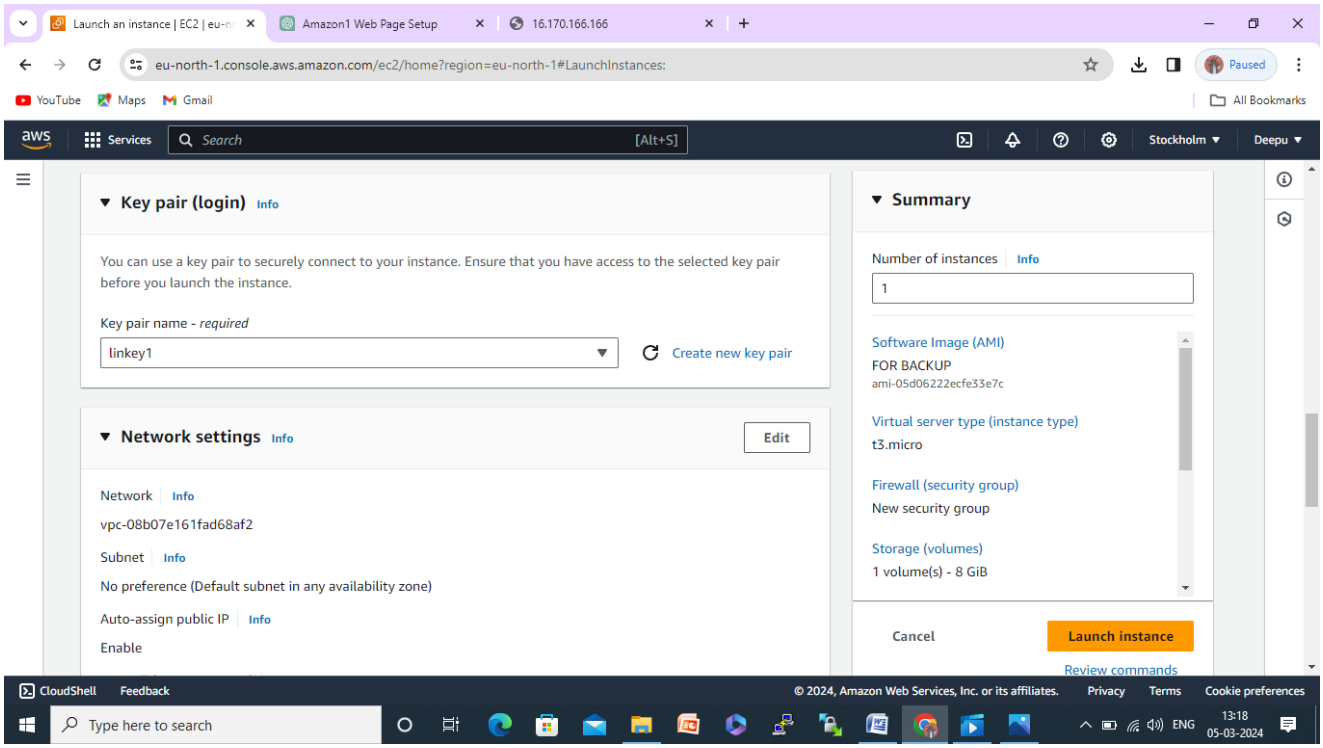
Cancel | Launch instance

Review commands

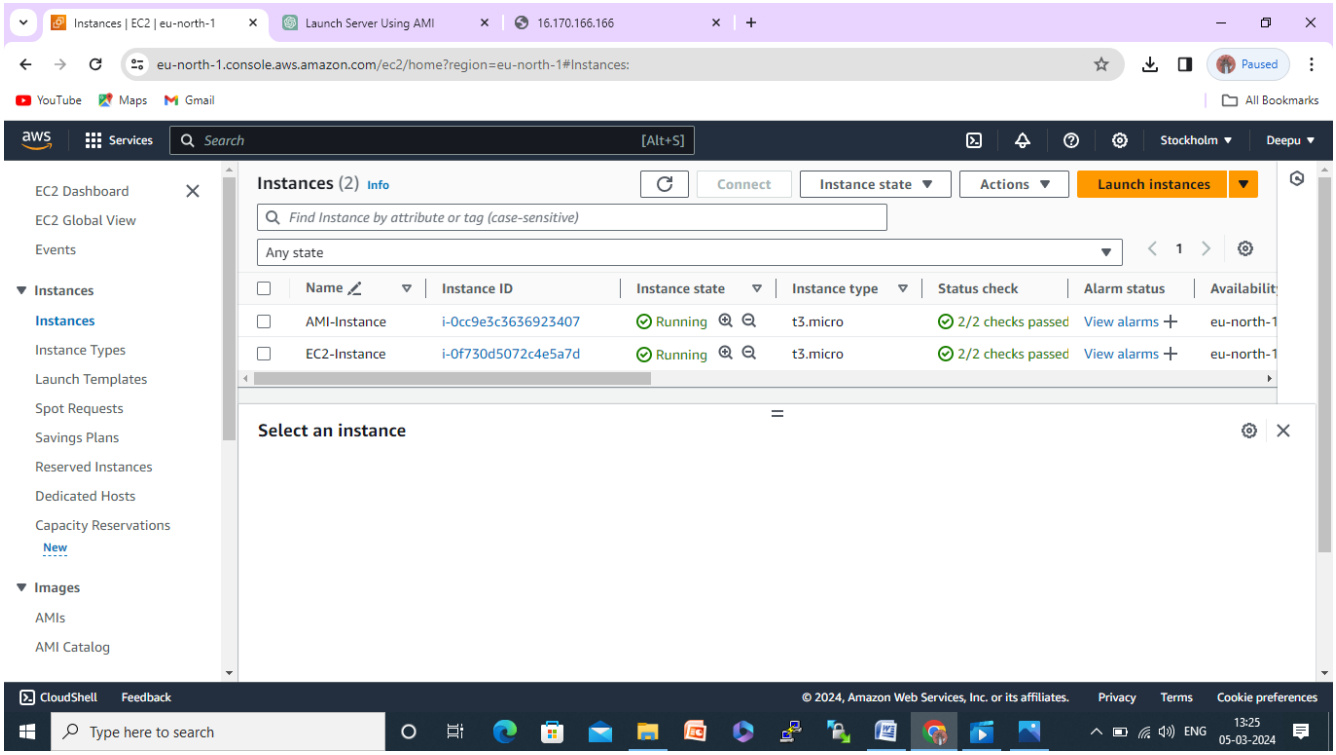
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 13:17 05-03-2024

Now Create a new key-pair which you losed or use the existing key-pair.

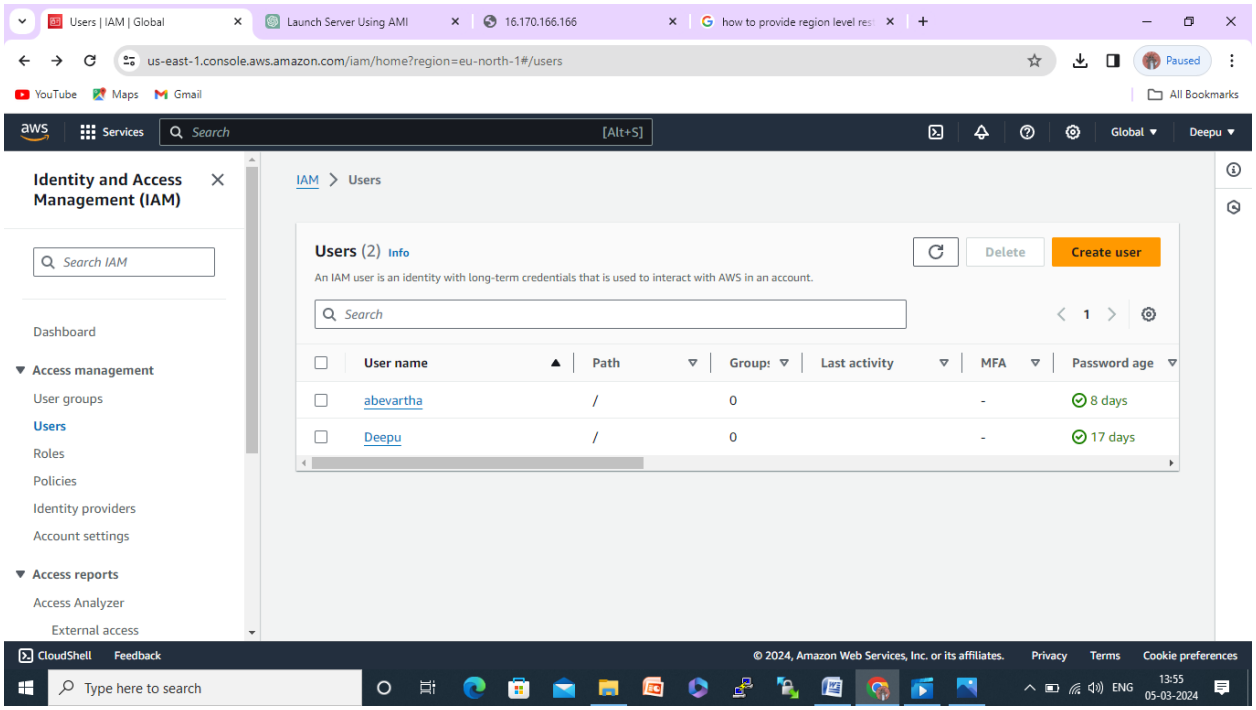


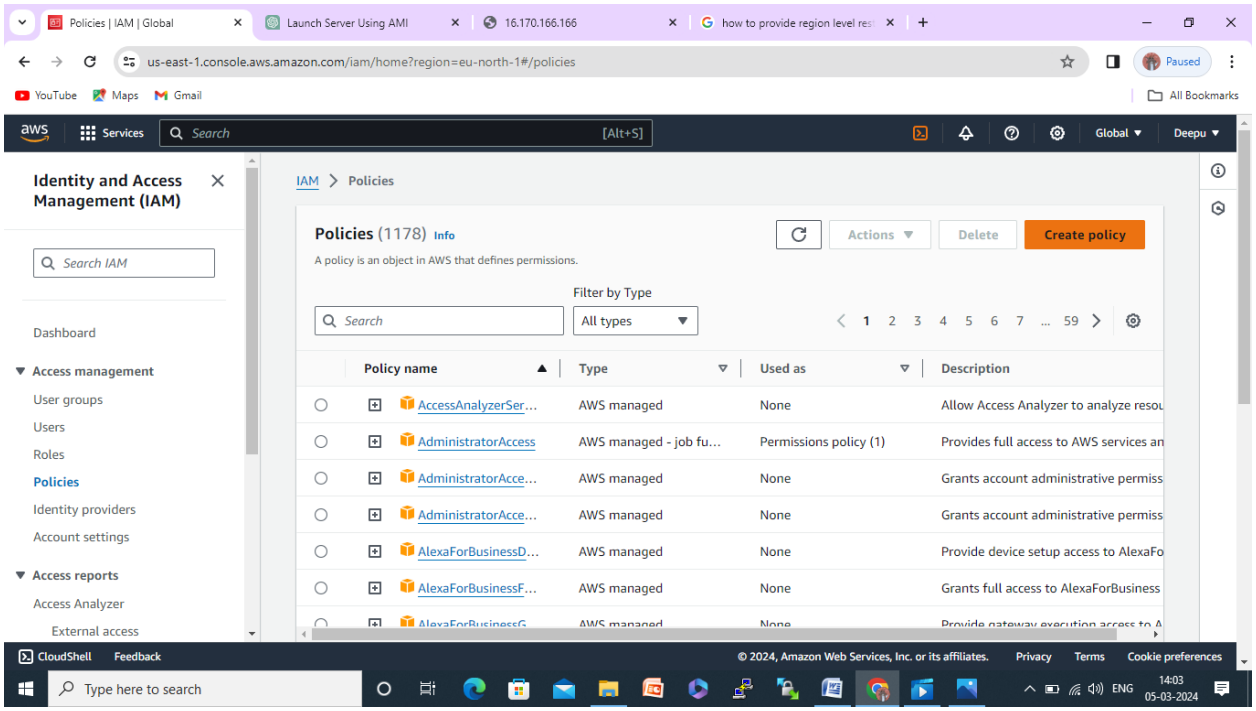
•



3. How to provide region level restriction for IAM users?

To provide region-level restrictions for IAM users in AWS, you can use IAM policies with conditions that specify the regions where the IAM users are allowed to perform actions.





Within the IAM policy, use the Condition element to define the region-based restriction. You can use the aws:RequestedRegion condition key to specify the allowed regions.

Create policy | IAM | Global | Launch Server Using AMI | 16.170.166.166 | how to provide region level res

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

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

Policy editor Visual | JSON | Actions

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": "ec2:*",
7              "Resource": "*",
8              "Condition": {
9                  "StringEquals": {
10                     "aws:RequestedRegion": "us-west-2"
11                 }
12             }
13         }
14     ]
15 }
16
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 14:10 05-03-2024

Create policy | IAM | Global | Launch Server Using AMI | 16.170.166.166 | how to provide region level res

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

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

Policy editor Visual | JSON | Actions

Select a service

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

Service

Choose a service

+ Add more permissions

Cancel Next

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 14:04 05-03-2024

Create policy | IAM | Global | Launch Server Using AMI | 16.170.166.166 | how to provide region level res

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

YouTube Maps Gmail All Bookmarks

aws Services Search [Alt+S] Global Deepu

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Restriction-policy-IAM-ur

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

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

Restriction-policy

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

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 14:12 05-03-2024

Create policy | IAM | Global | Launch Server Using AMI | 16.170.166.166 | how to provide region level res

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

YouTube Maps Gmail All Bookmarks

aws Services Search [Alt+S] Global Deepu

Search

Allow (1 of 404 services) Show remaining 403 services

Service	Access level	Resource	Request condition
EC2	Full access	All resources	aws:RequestedRegion 2

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.

Add new tag

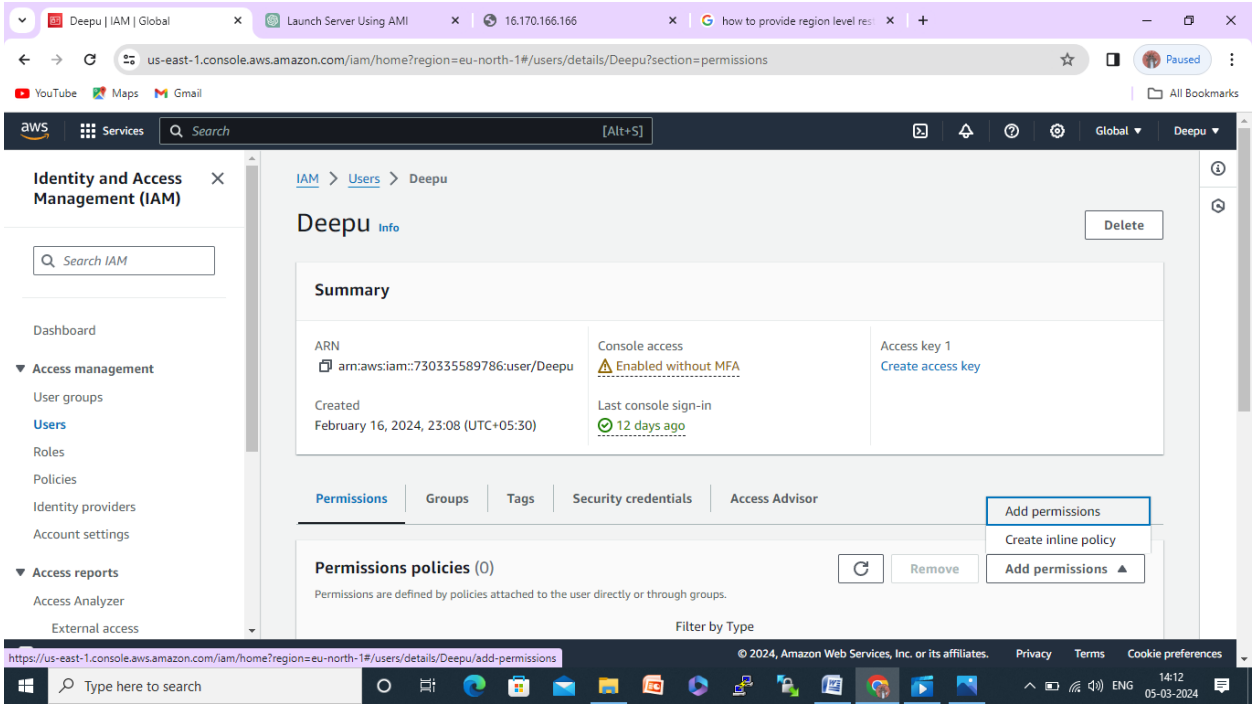
You can add up to 50 more tags.

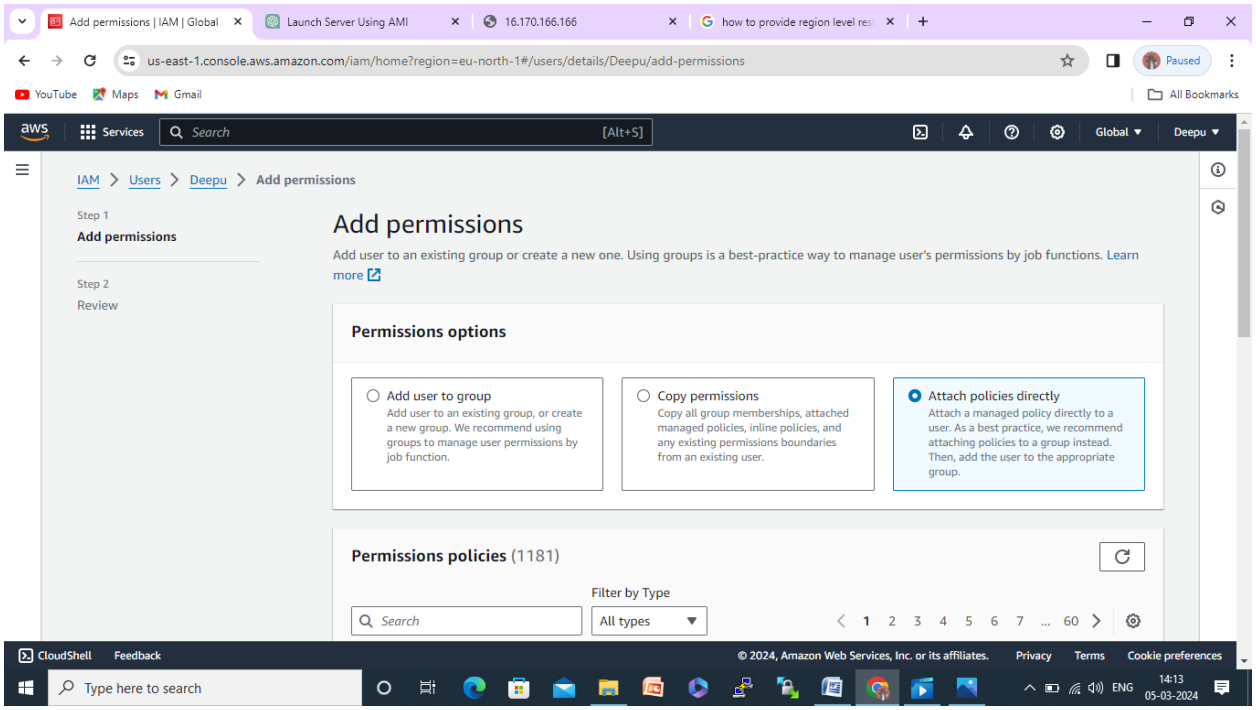
Cancel Previous Create policy

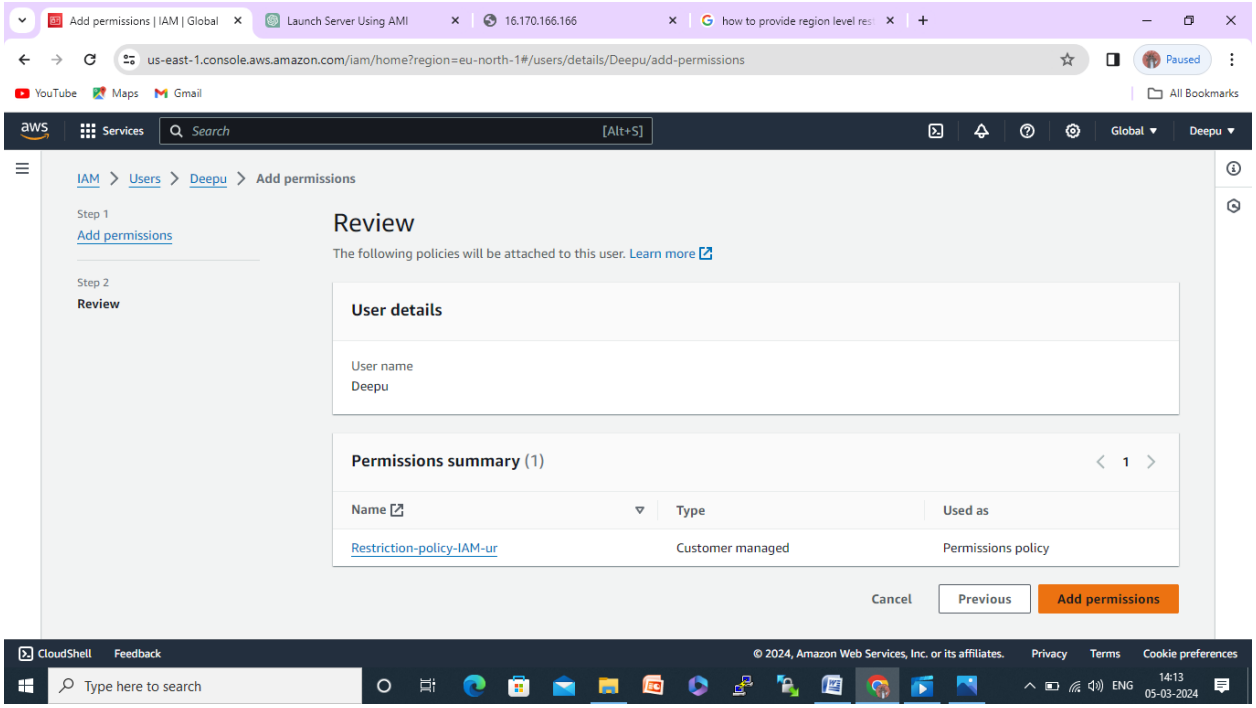
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 14:12 05-03-2024

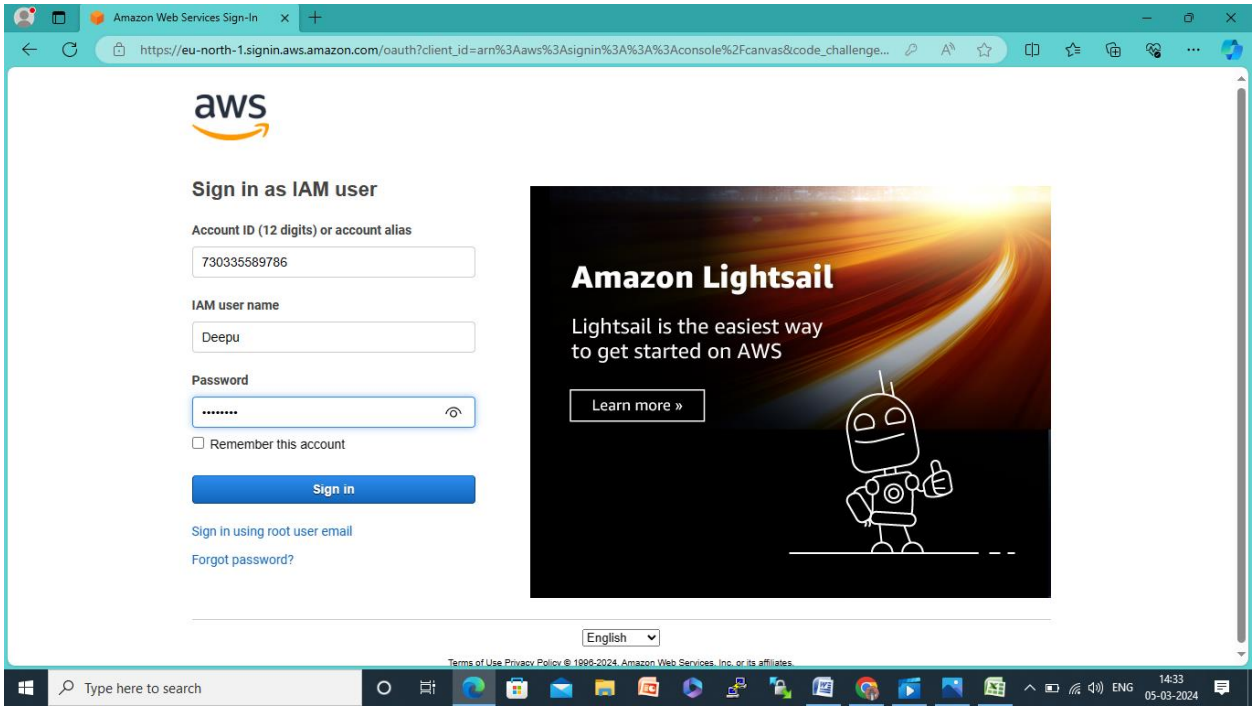
Asigning user deepu with a created custom policy.



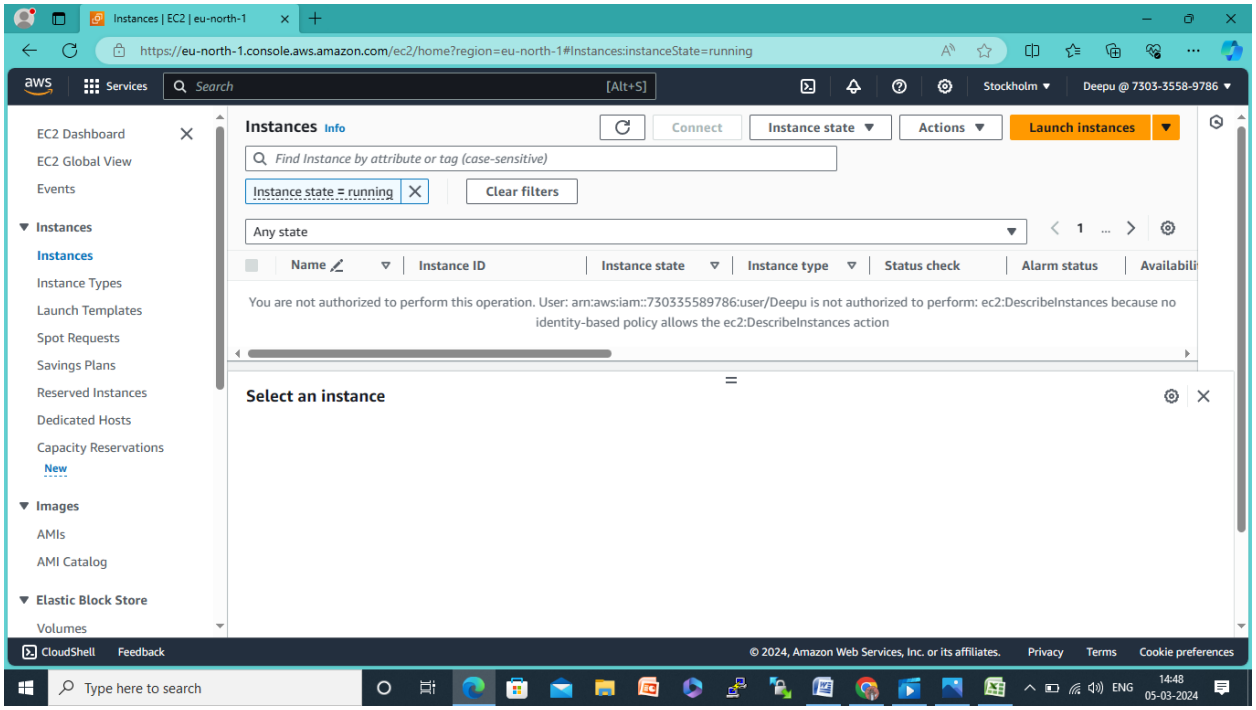




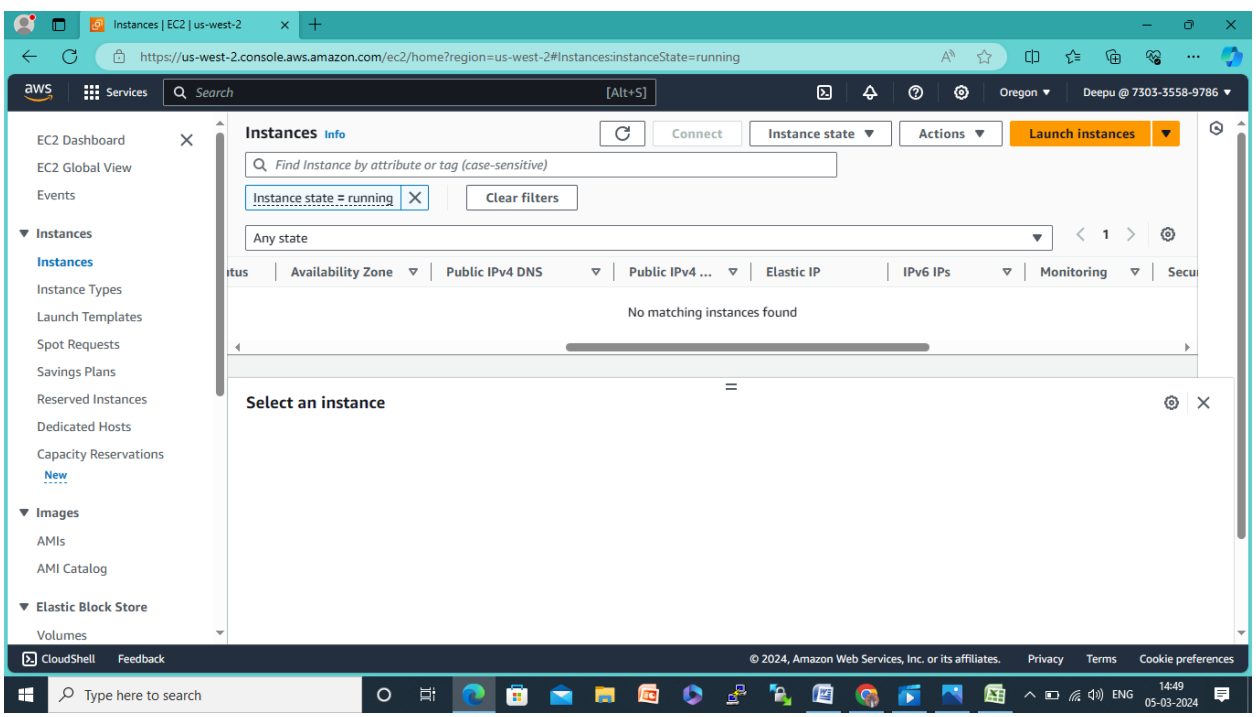
Login to checking the region level restriction for the IAM user deepu.



Restricted for other region for that IAM user

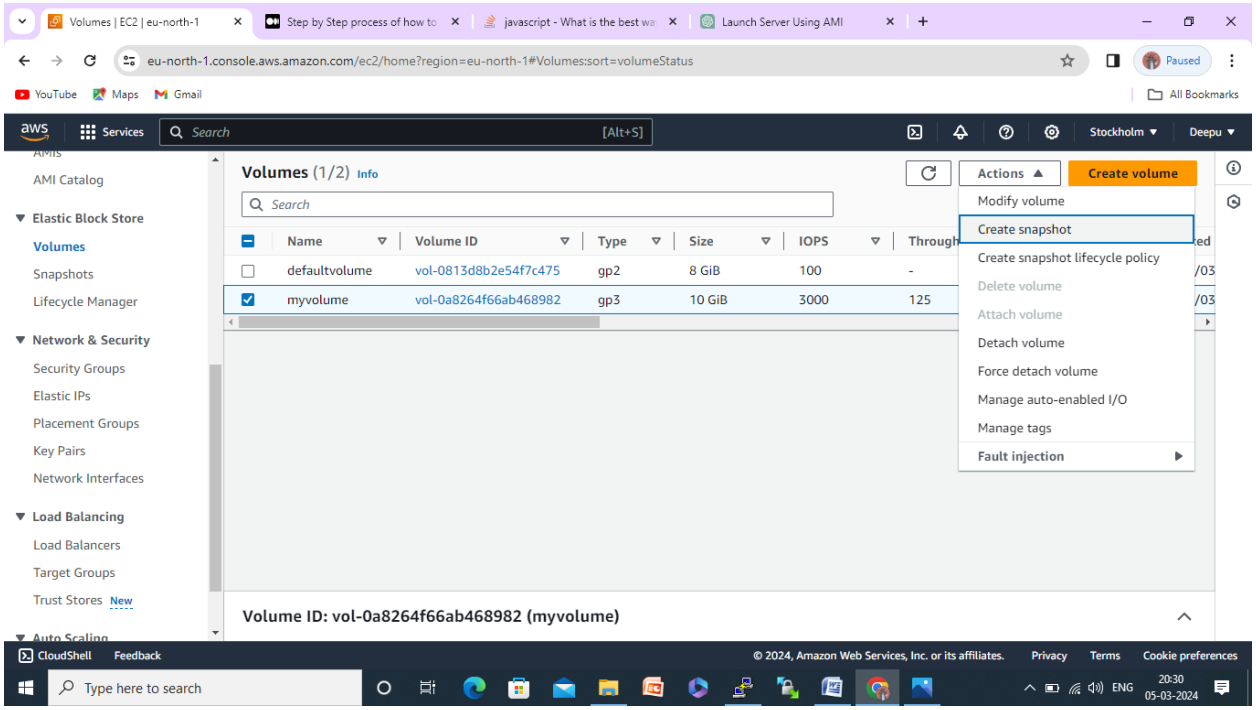


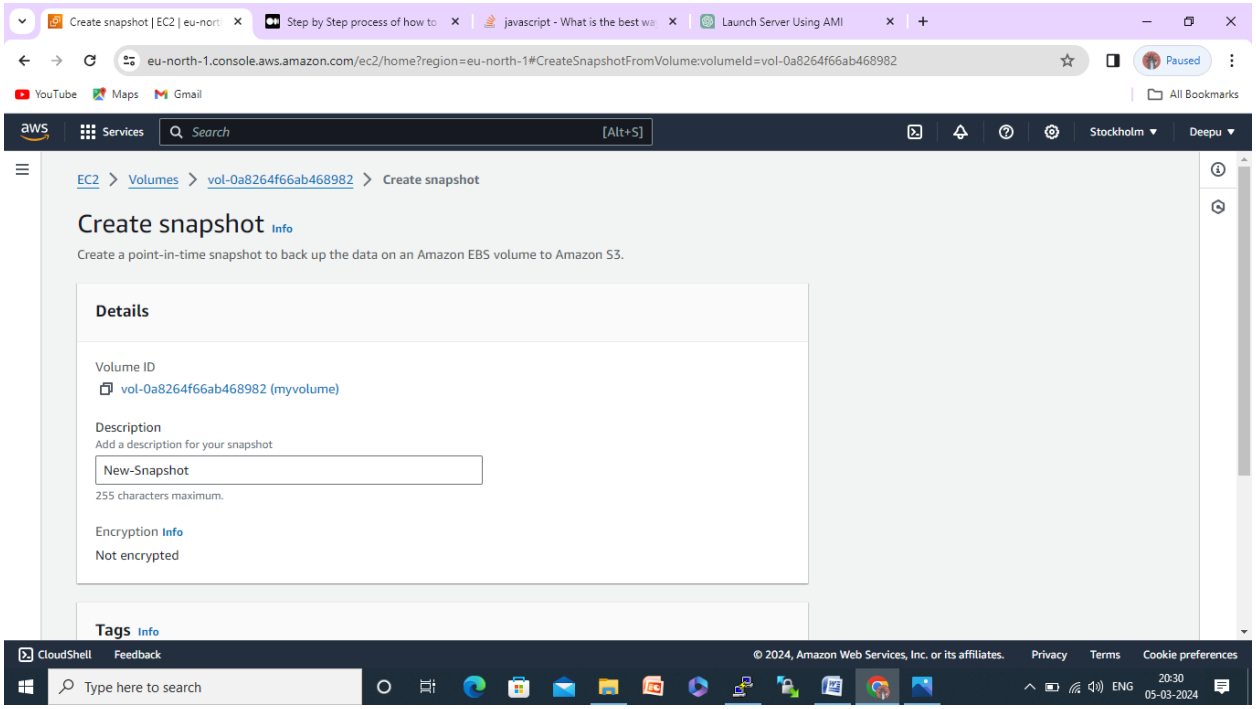
Alloowed only for this region us-west-2

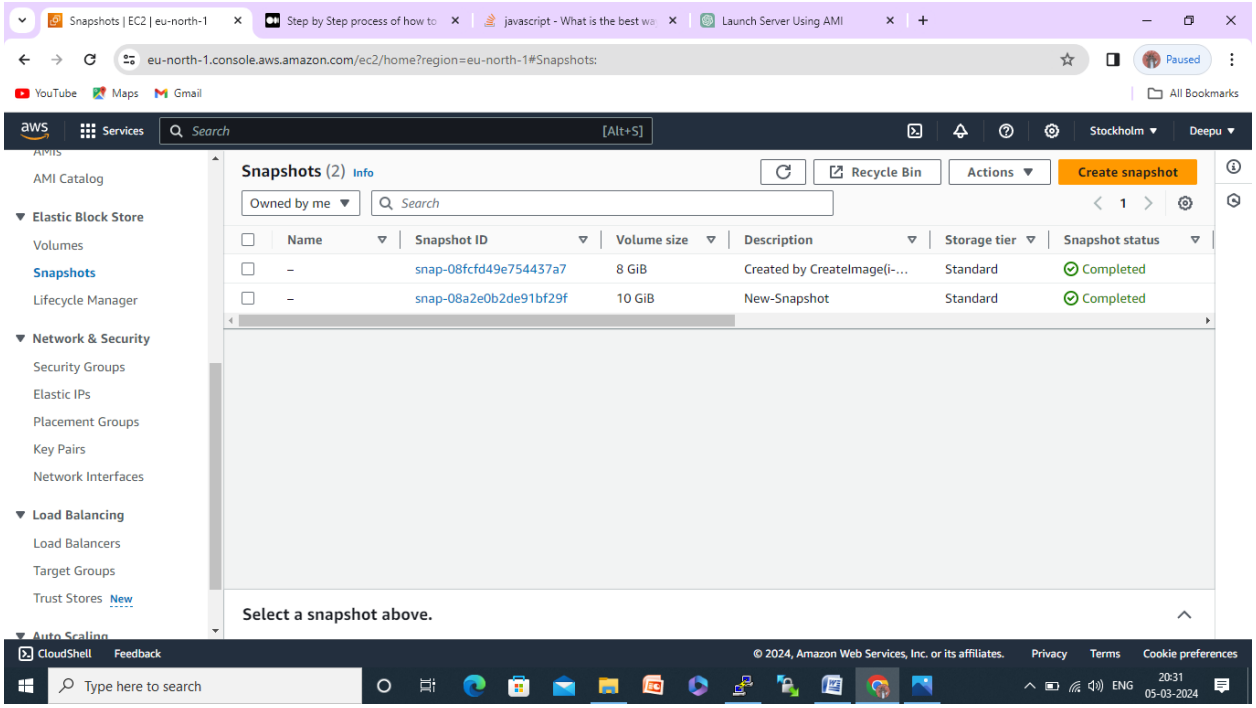


4. How backup your server?

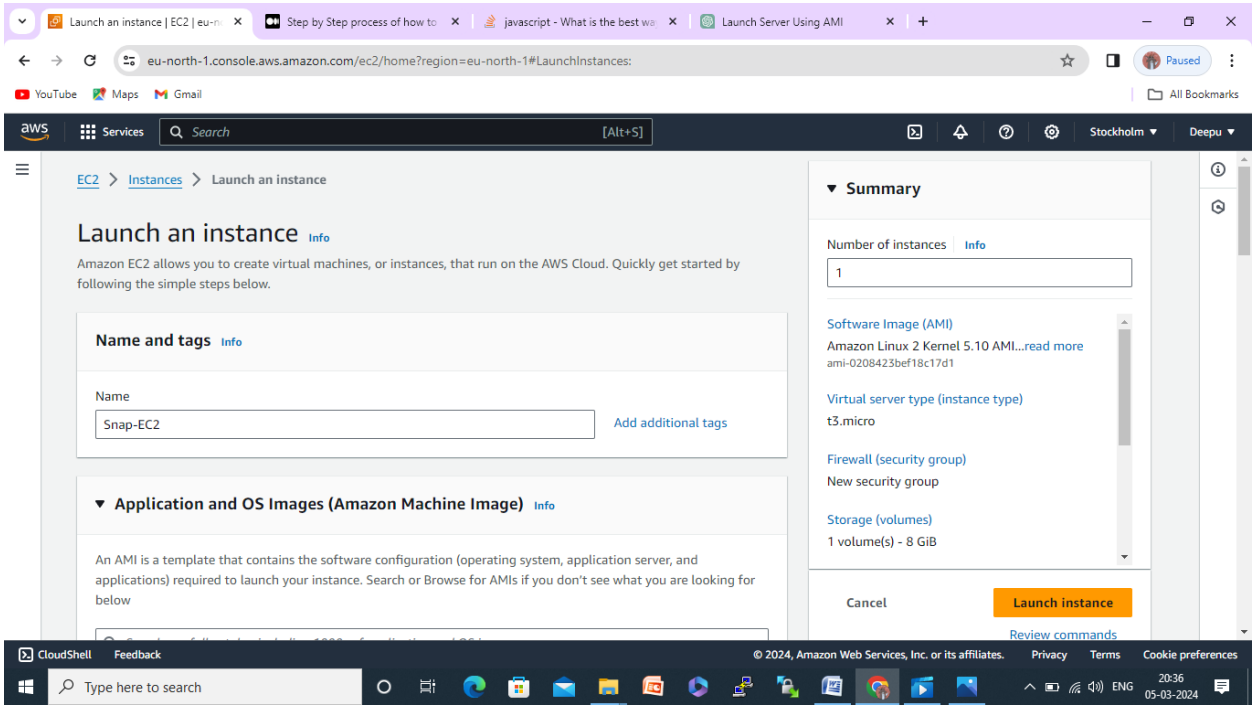
Backing up your server in AWS involves creating and managing snapshots of your server's volumes

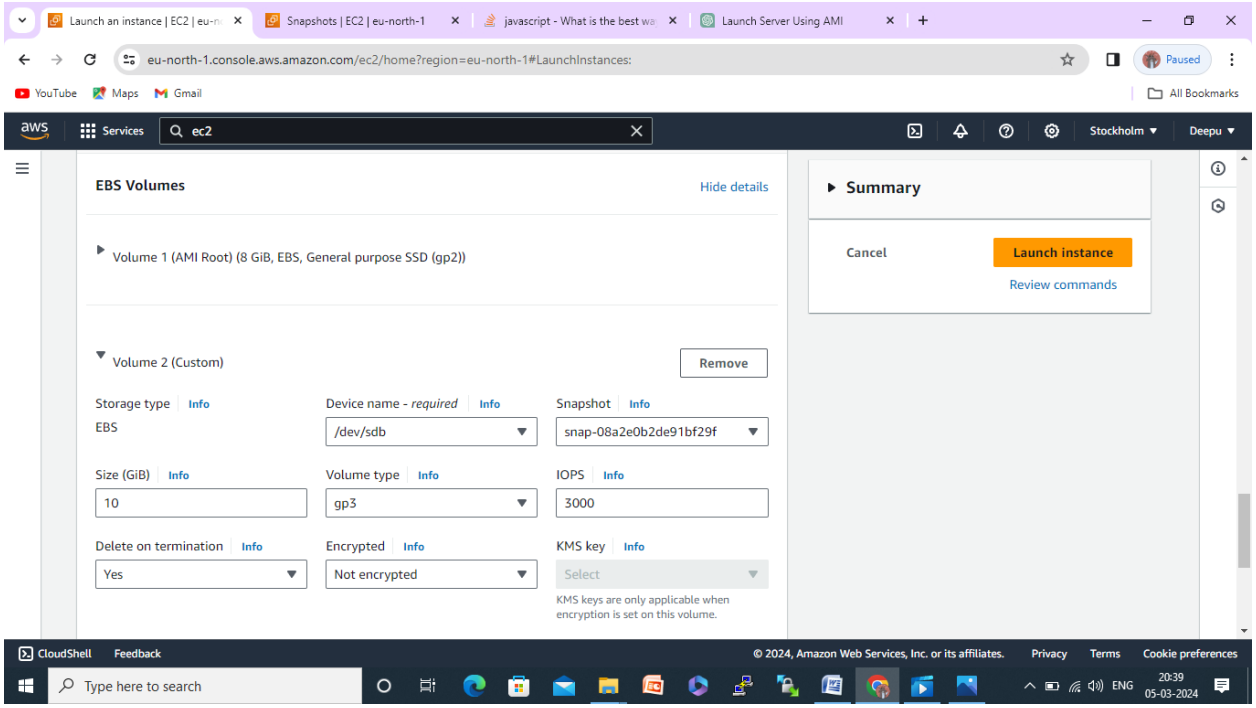


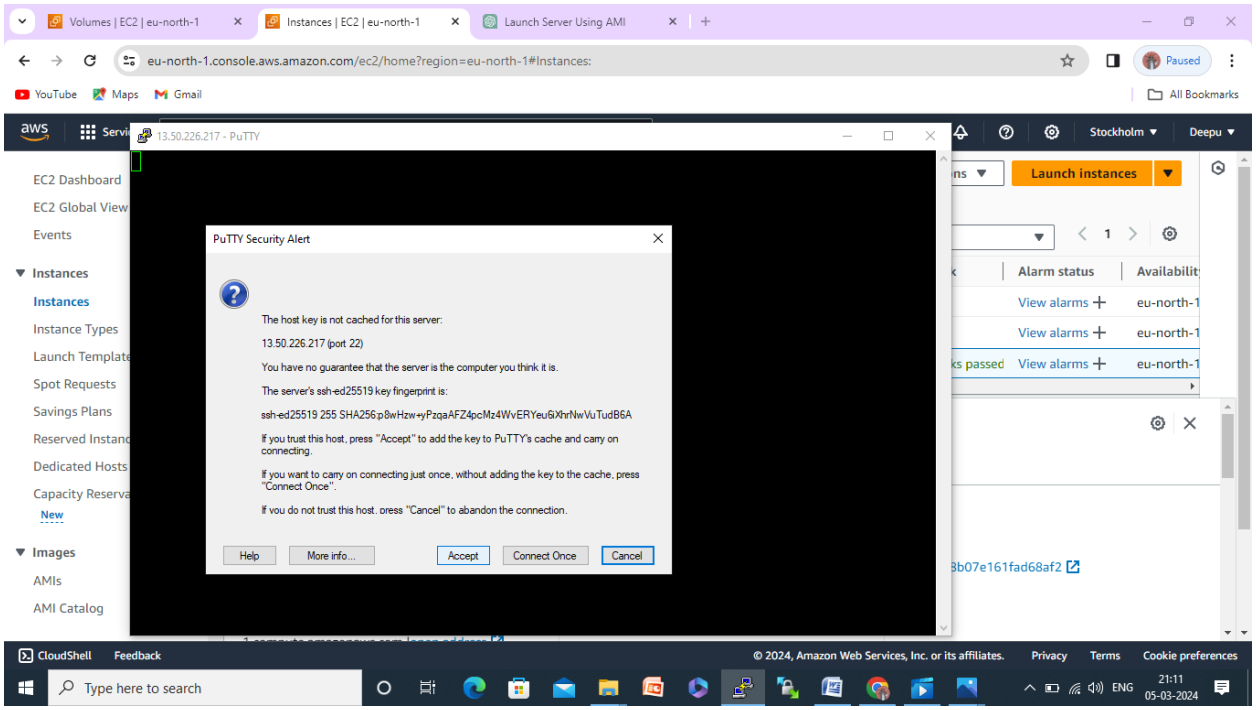




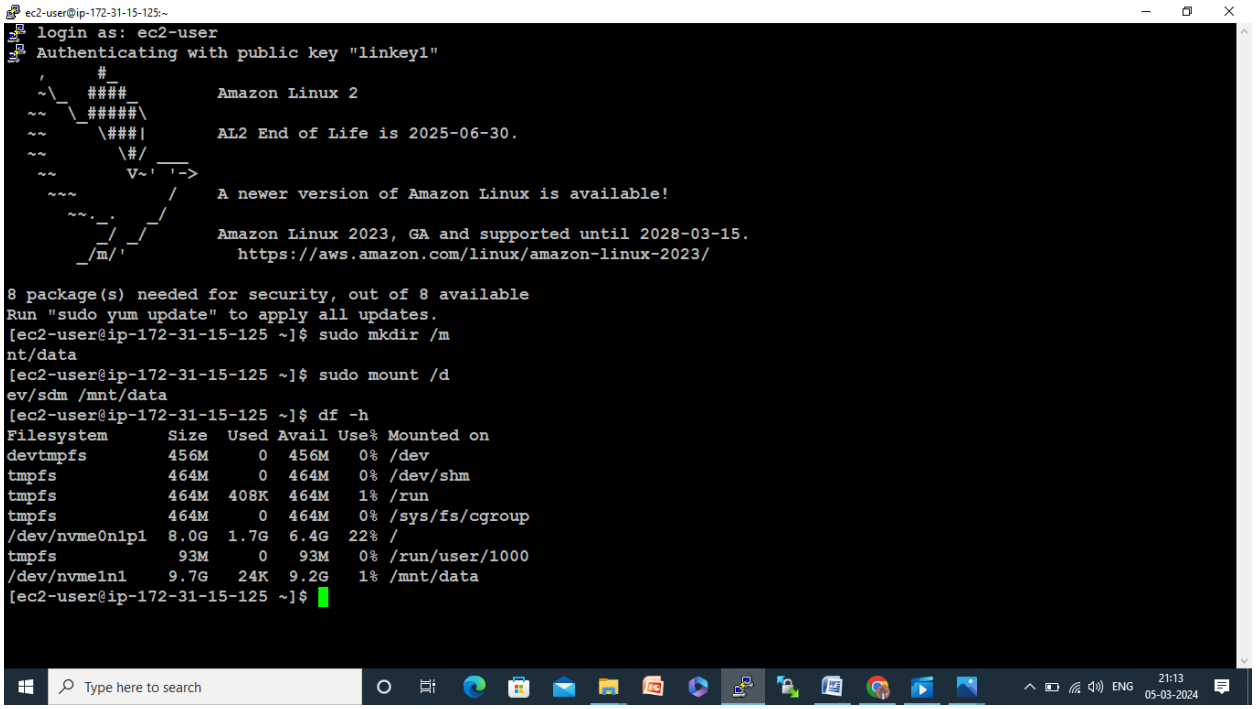
While creating a new instances, we can use that server which is backuped as a snapshot.




Launch an instance | EC2 | eu-n
Snapshots | EC2 | eu-north-1
javascript - What is the best wa
Launch Server Using AMI
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:
Paused
YouTube
Maps
Gmail
All Bookmarks
aws
Services
ec2
Stockholm
Deepu
EBS Volumes
Hide details
Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp2))
Volume 2 (Custom)
Remove
Storage type Info
EBS
Device name - required Info
/dev/sdb
Snapshot Info
snap-08a2e0b2de91bf29f
Size (GiB) Info
10
Volume type Info
gp3
IOPS Info
3000
Delete on termination Info
Yes
Encrypted Info
Not encrypted
KMS key Info
Select
KMS keys are only applicable when encryption is set on this volume.
Summary
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
20:39
05-03-2024

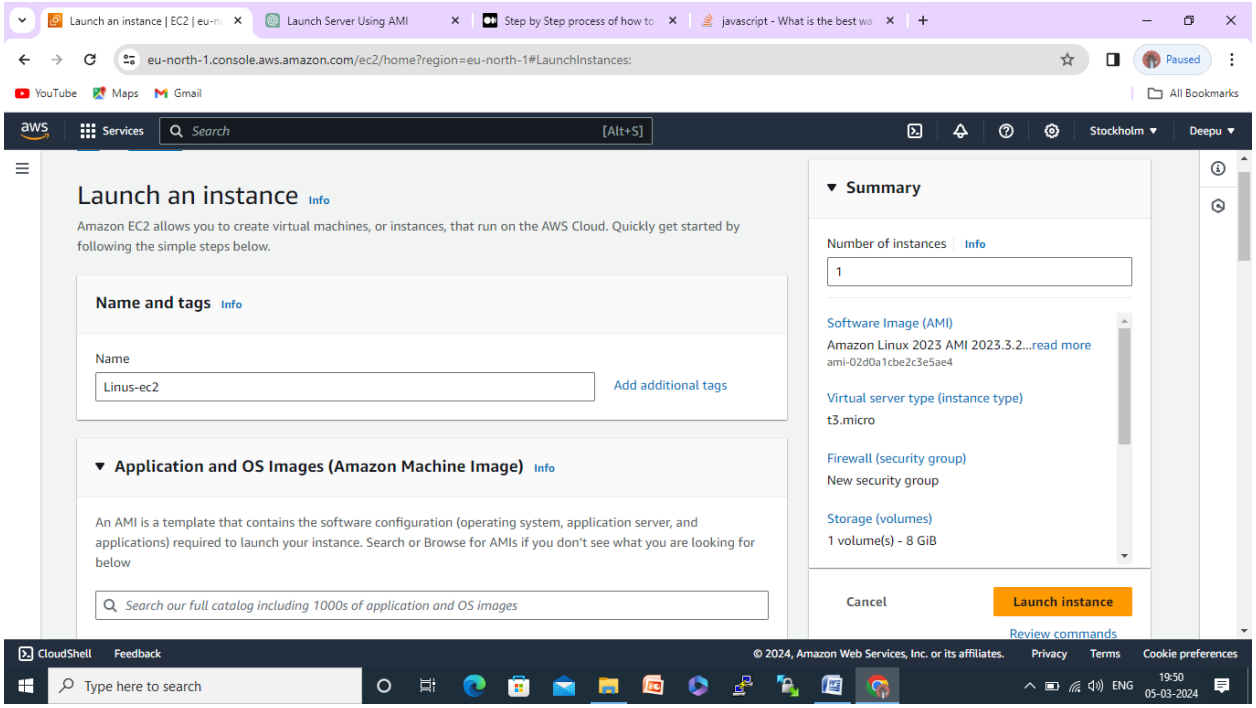

Volumes | EC2 | eu-north-1
Instances | EC2 | eu-north-1
Launch Server Using AMI
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Instances:
Paused
YouTube
Maps
Gmail
All Bookmarks
aws
13.50.226.217 - PuTTY
Stockholm
Deepu
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Template
Spot Requests
Savings Plans
Reserved Instanc
Dedicated Hosts
Capacity Reserva
New
Images
AMIs
AMI Catalog
Launch instances
Alarm status
View alarms
eu-north-1
PuTTY Security Alert
The host key is not cached for this server:
13.50.226.217 (port 22)
You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:p8wHzw+yPzqaAFZ4pcMz4WvERYeu6iXhrNwVuTudB6A
If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".
If you do not trust this host, press "Cancel" to abandon the connection.
Help
More info...
Accept
Connect Once
Cancel
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
21:11
05-03-2024

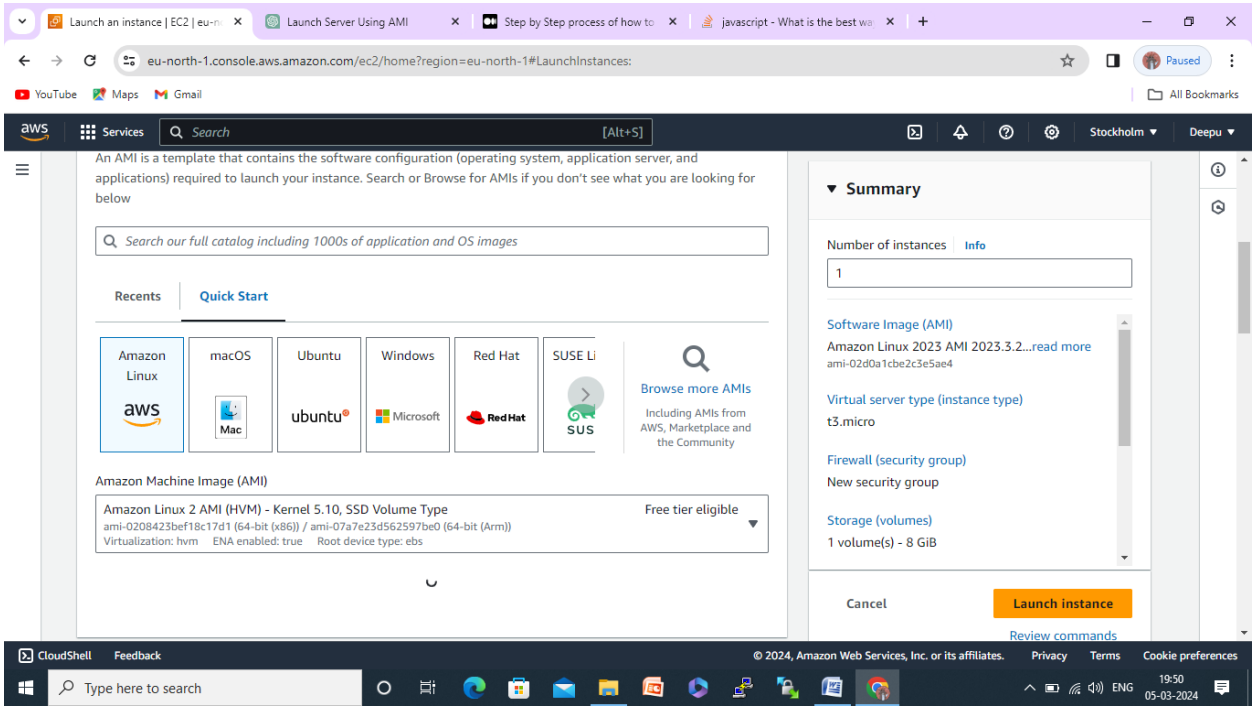
- **Once attached, identify the device name of the volume on the new EC2 instance, which is created using the snapshot.**
- **“lsblk” command to list all block devices and their mount points.**
- **The new volume will likely be listed as something like /dev/xvdf or /dev/sdf.**
- **Create a directory where you want to mount the volume on your Linux file system- ----“sudo mkdir /mnt/data”**
- **Use the mount command to mount the volume to the desired mount point----“sudo mount /dev/xvdf /mnt/data”**
- **After mounting the volume, you can verify that it's mounted by “df –h”**

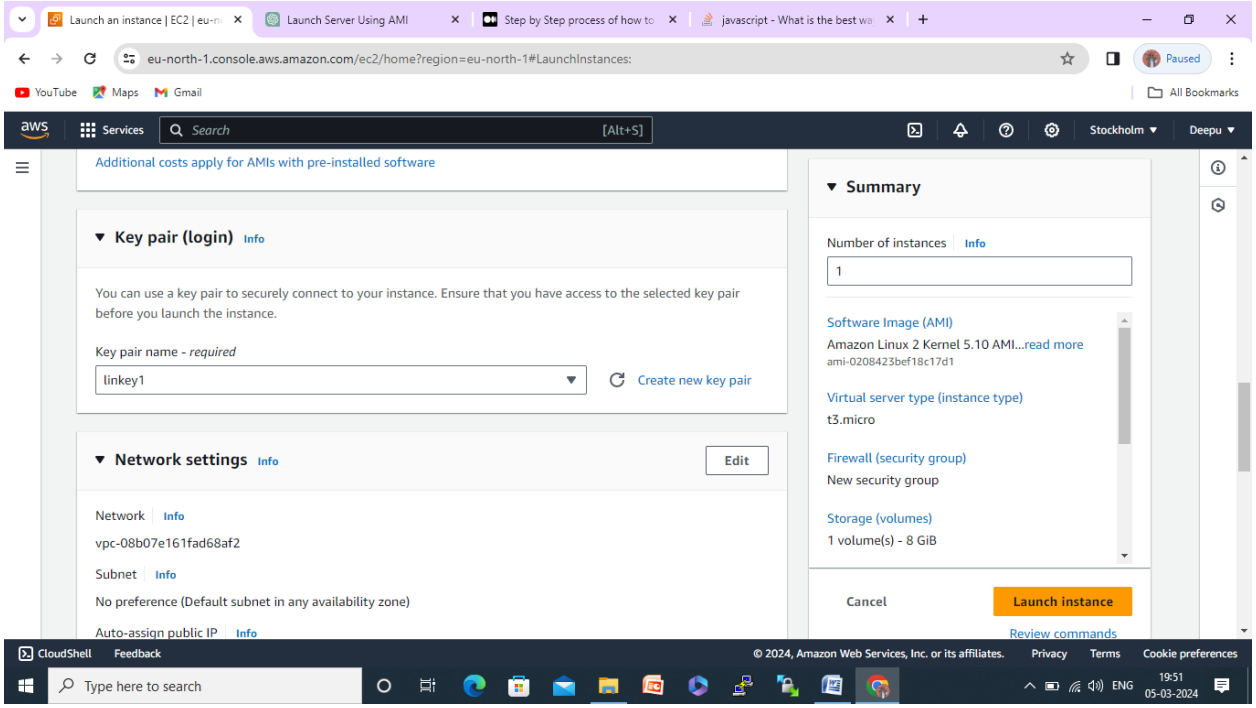


5. How to mount volume in linux instance?

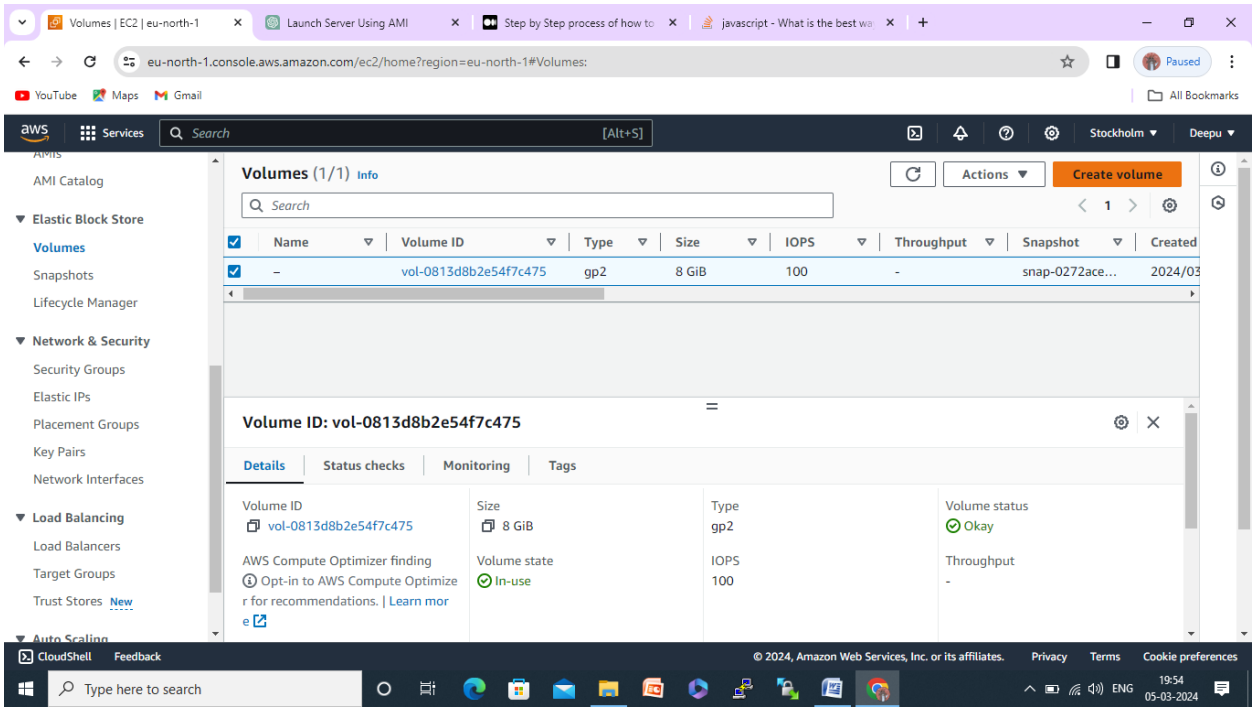
Creating a EC2 instance to mount the volume







Creating the new volume to the instance



Create volume | EC2 | eu-north- | Launch Server Using AMI | Step by Step process of how to | javascript - What is the best wa

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateVolume:

YouTube Maps Gmail All Bookmarks

aws Services Search [Alt+S] Stockholm Deepu

Volume settings

Volume type Info

General Purpose SSD (gp2)

Size (GiB) Info

10

Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS Info

100 / 3000

Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) Info

Not applicable

Availability Zone Info

eu-north-1a

Snapshot ID - *optional* Info

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 19:54 05-03-2024

Create volume | EC2 | eu-north- | Launch Server Using AMI | Step by Step process of how to | javascript - What is the best wa

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#CreateVolume:

YouTube Maps Gmail All Bookmarks

aws Services Search [Alt+S] Stockholm Deepu

Size (GiB) Info

10

Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS Info

100 / 3000

Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) Info

Not applicable

Availability Zone Info

eu-north-1c

Snapshot ID - *optional* Info

Don't create volume from a snapshot

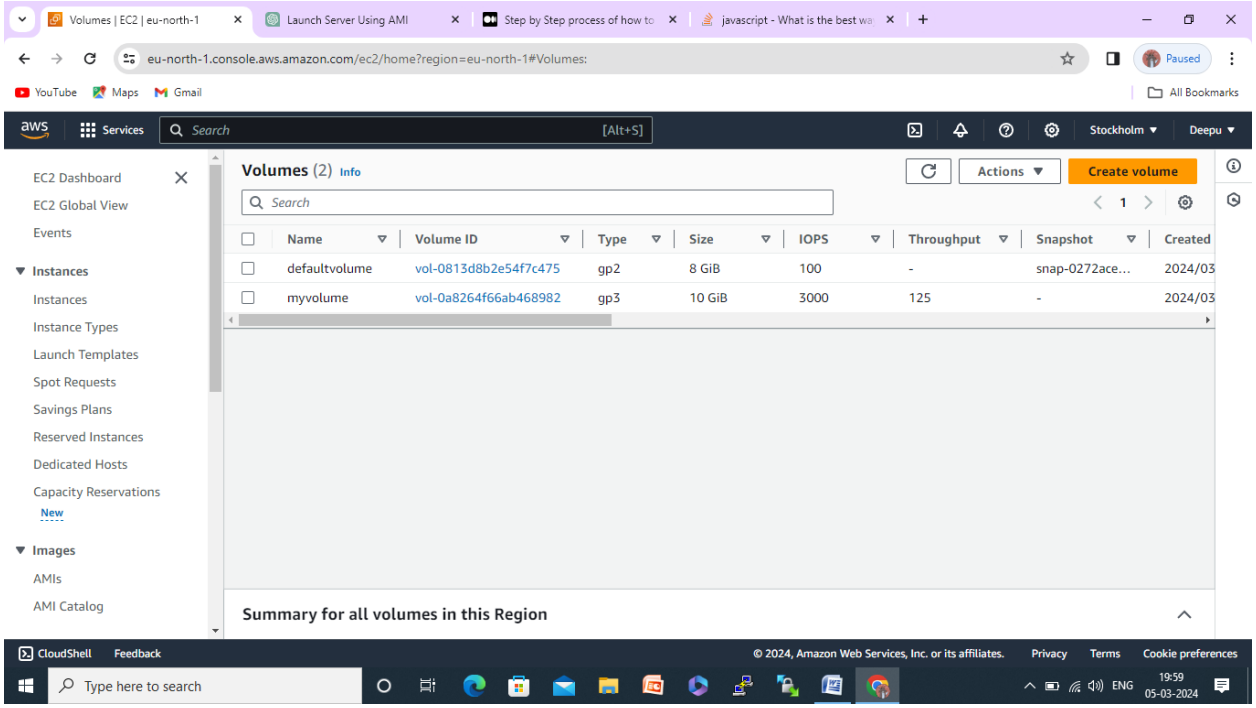
Encryption Info

Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.

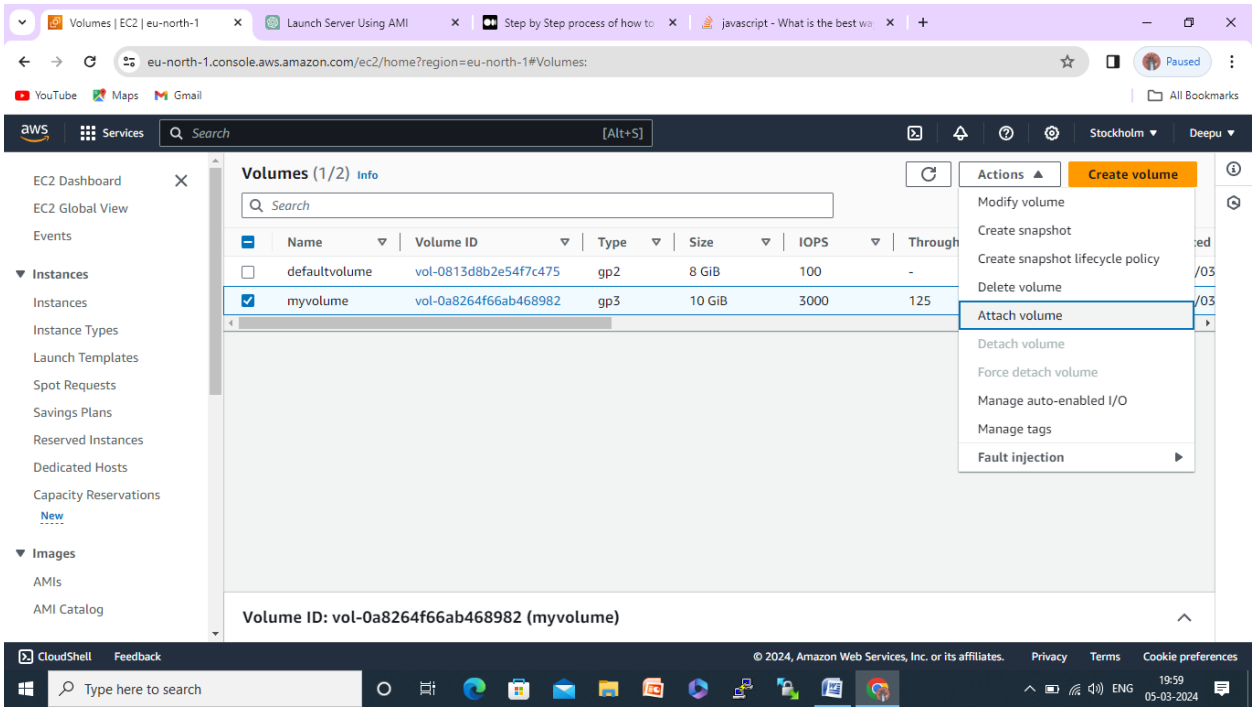
☐ Encrypt this volume

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 19:56 05-03-2024



Attaching the volume the created instance in the same region



Attach volume | EC2 | eu-north- | Launch Server Using AMI | Step by Step process of how to | javascript - What is the best wa

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#AttachVolume:volumeId=vol-0a8264f66ab468982

Attach a volume to an instance to use it as you would a regular physical hard disk drive.

Basic details

Volume ID

vol-0a8264f66ab468982 (myvolume)

Availability Zone

eu-north-1c

Instance Info

i-04b2056224cc366e8

i-04b2056224cc366e8
(linux-EC2) (running)

Recommended device names for Linux: /dev/sda1 for root volume. /dev/sd[f-p] for data volumes.

Newer Linux kernels may rename your devices to **/dev/xvdf** through **/dev/xvdp** internally, even when the device name entered here (and shown in

Attach volume | EC2 | eu-north- | Launch Server Using AMI | Step by Step process of how to | javascript - What is the best wa

eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#AttachVolume:volumeId=vol-0a8264f66ab468982

Volume ID

vol-0a8264f66ab468982 (myvolume)

Availability Zone

eu-north-1c

Instance Info

i-04b2056224cc366e8

Only instances in the same Availability Zone as the selected volume are displayed.

Device name Info

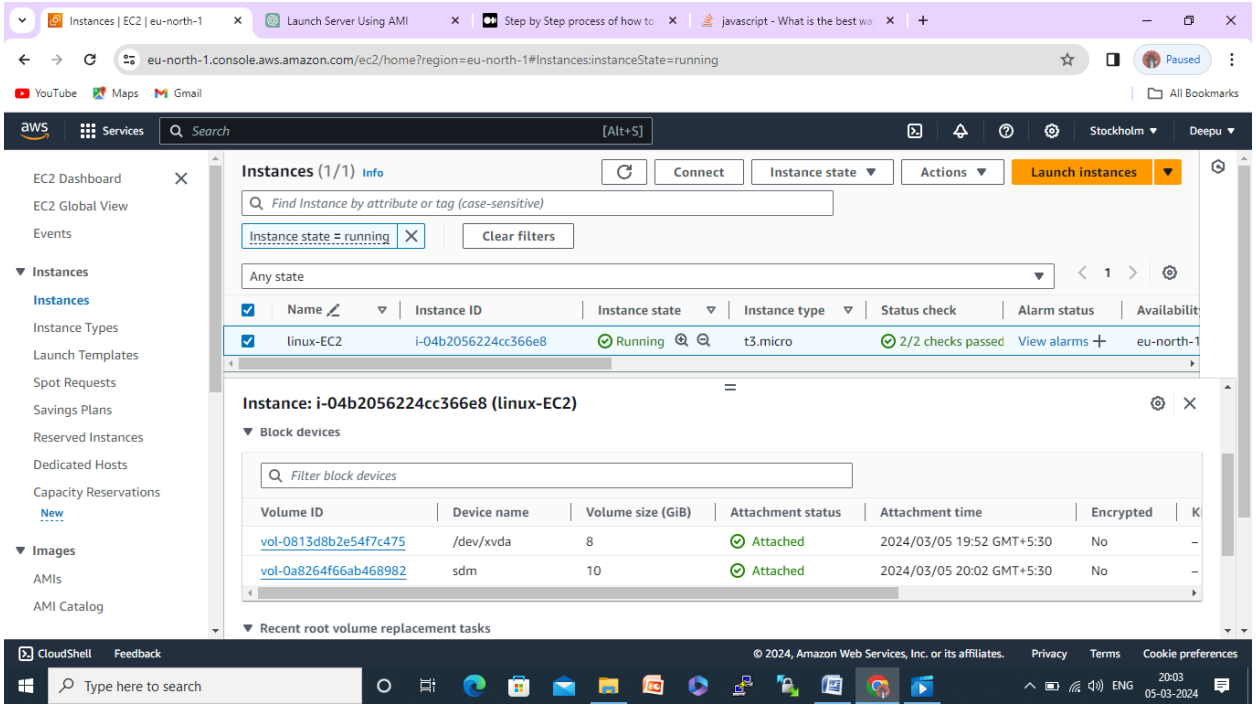
sdm

Recommended device names for Linux: /dev/sda1 for root volume. /dev/sd[f-p] for data volumes.

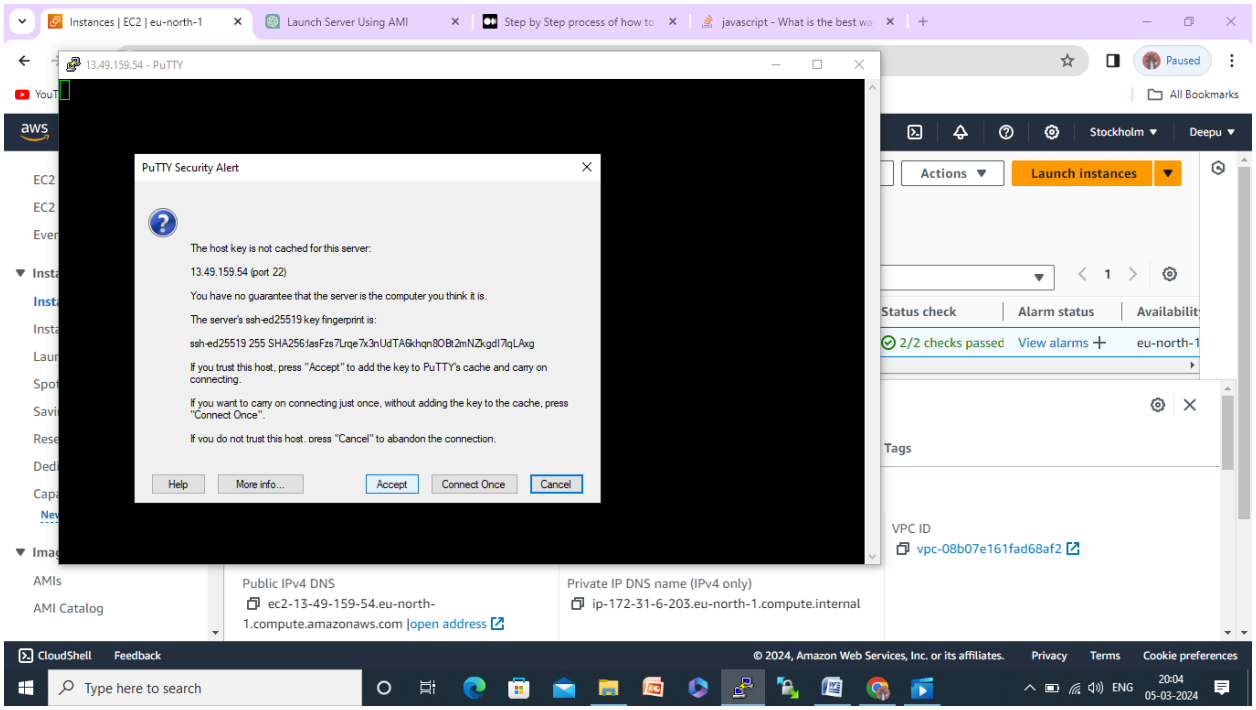
Newer Linux kernels may rename your devices to **/dev/xvdf** through **/dev/xvdp** internally, even when the device name entered here (and shown in the details) is **/dev/sdf** through **/dev/sdp.**

Cancel | Attach volume

/dev/xvda- root volume and sdm is newly created volume.



Login the EC2 instance server to mount the volume.



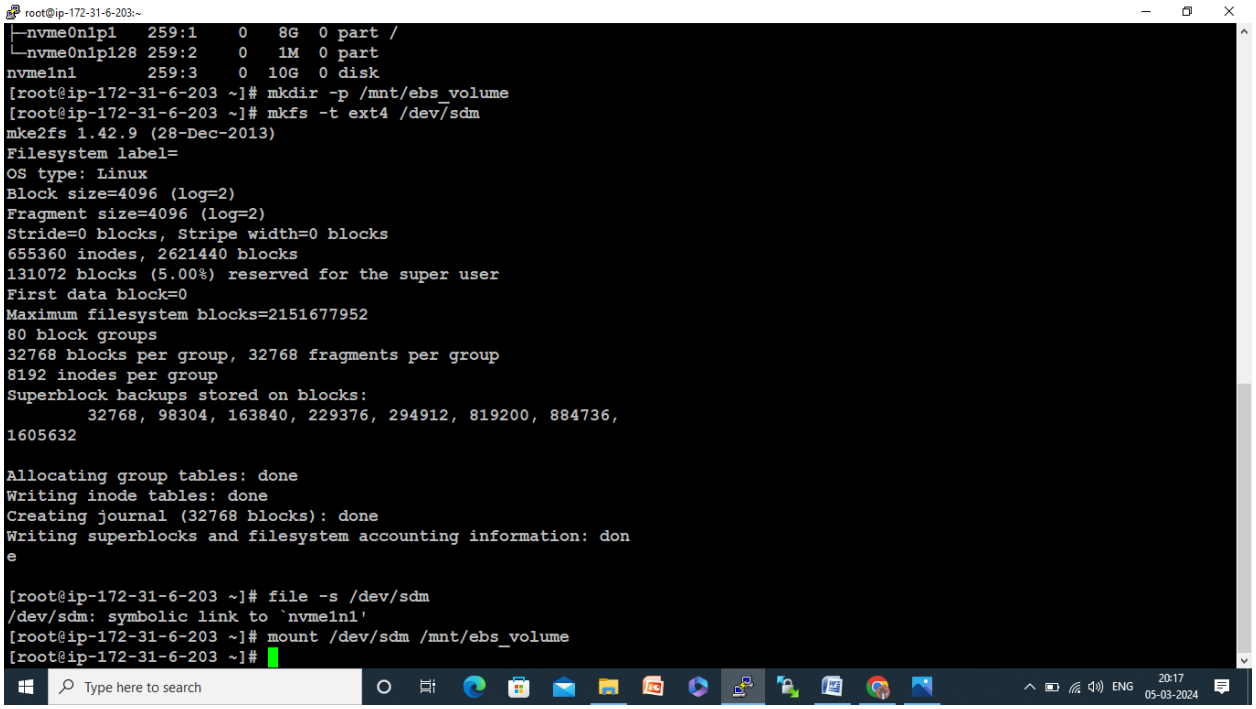
- **“lsblk” command to list the available block devices .**

```
root@ip-172-31-6-203:~
[ec2-user@ip-172-31-6-203 ~]$ lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme0n1       259:0    0   8G  0 disk
├─nvme0n1p1   259:1    0   8G  0 part /
└─nvme0n1p128 259:2    0   1M  0 part
nvme1n1       259:3    0  10G  0 disk
[ec2-user@ip-172-31-6-203 ~]$ mkdir -p/mnt/ebs_volume
mkdir: invalid option -- '/'
Try 'mkdir --help' for more information.
[ec2-user@ip-172-31-6-203 ~]$ mkdir -p /mnt/ebs_volume
mkdir: cannot create directory '/mnt/ebs_volume': Permission d
enied
[ec2-user@ip-172-31-6-203 ~]$ sudo -i
[root@ip-172-31-6-203 ~]# lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme0n1       259:0    0   8G  0 disk
├─nvme0n1p1   259:1    0   8G  0 part /
└─nvme0n1p128 259:2    0   1M  0 part
nvme1n1       259:3    0  10G  0 disk
[root@ip-172-31-6-203 ~]# mkdir -p /mnt/ebs_volume
[root@ip-172-31-6-203 ~]#
```

- **Create a directory to be used as the mount point “mkdir -p /mnt/ebs_volume”**
- **“ mkfs -t ext4 /dev/sdm” to create a file system on the attached volume**

```
root@ip-172-31-6-203:~
[root@ip-172-31-6-203 ~]# lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme0n1       259:0    0   8G  0 disk
├─nvme0n1p1   259:1    0   8G  0 part /
└─nvme0n1p128 259:2    0   1M  0 part
nvme1n1       259:3    0  10G  0 disk
[root@ip-172-31-6-203 ~]# mkdir -p /mnt/ebs_volume
[root@ip-172-31-6-203 ~]# mkfs -t ext4 /dev/sdm
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
655360 inodes, 2621440 blocks
131072 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736,
1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: don
e

[root@ip-172-31-6-203 ~]#
```

- **Now if we verify if the new file system exists use the below command and file -s /dev/xvdf**
- **Mount the EBS volume to the specified mount point mount /dev/xvdf /mnt/ebs_volume**



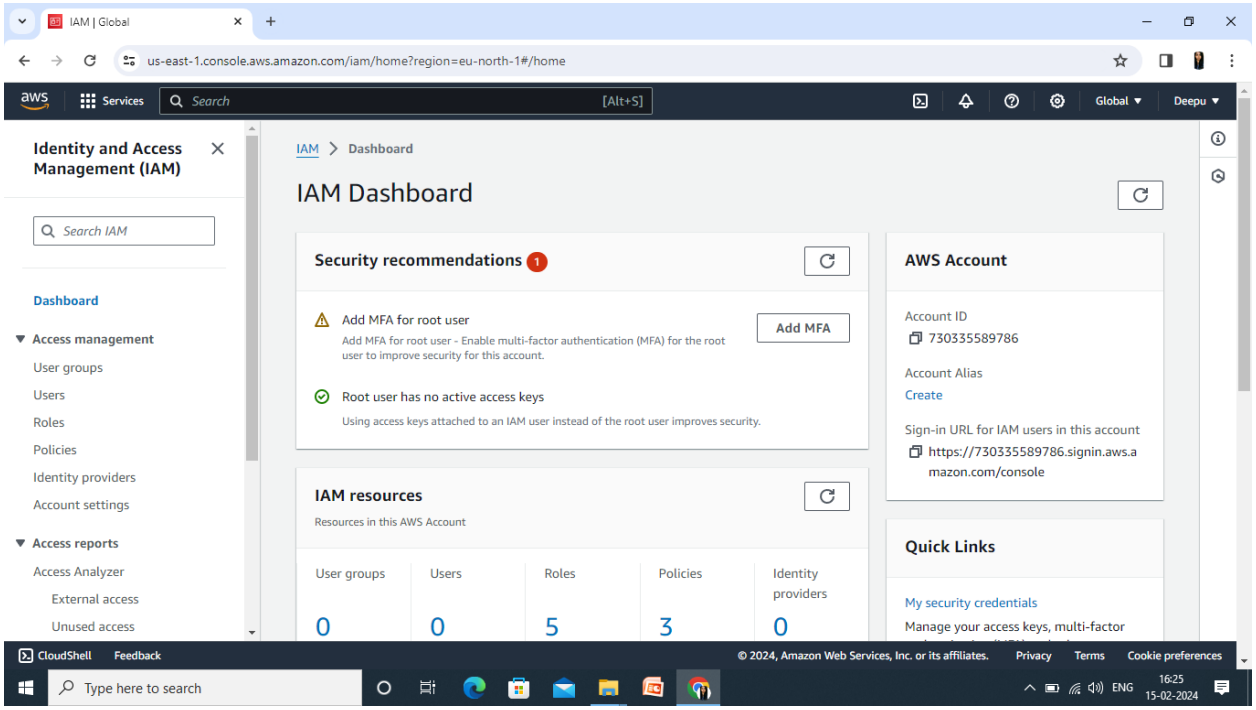
Now you should see the new EBS volume mounted to the directory you created by" df –h" and "lsblk

```
root@ip-172-31-6-203:~
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
655360 inodes, 2621440 blocks
131072 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736,
1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: don
e

[root@ip-172-31-6-203 ~]# file -s /dev/sdm
/dev/sdm: symbolic link to `nvme1n1'
[root@ip-172-31-6-203 ~]# mount /dev/sdm /mnt/ebs_volume
[root@ip-172-31-6-203 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        456M     0  456M   0% /dev
tmpfs           464M     0  464M   0% /dev/shm
tmpfs           464M  408K  464M   1% /run
tmpfs           464M     0  464M   0% /sys/fs/cgroup
/dev/nvme0n1p1  8.0G  1.7G  6.4G  22% /
tmpfs            93M     0   93M   0% /run/user/1000
/dev/nvme1n1    9.7G   24K  9.2G   1% /mnt/ebs_volume
[root@ip-172-31-6-203 ~]#
```

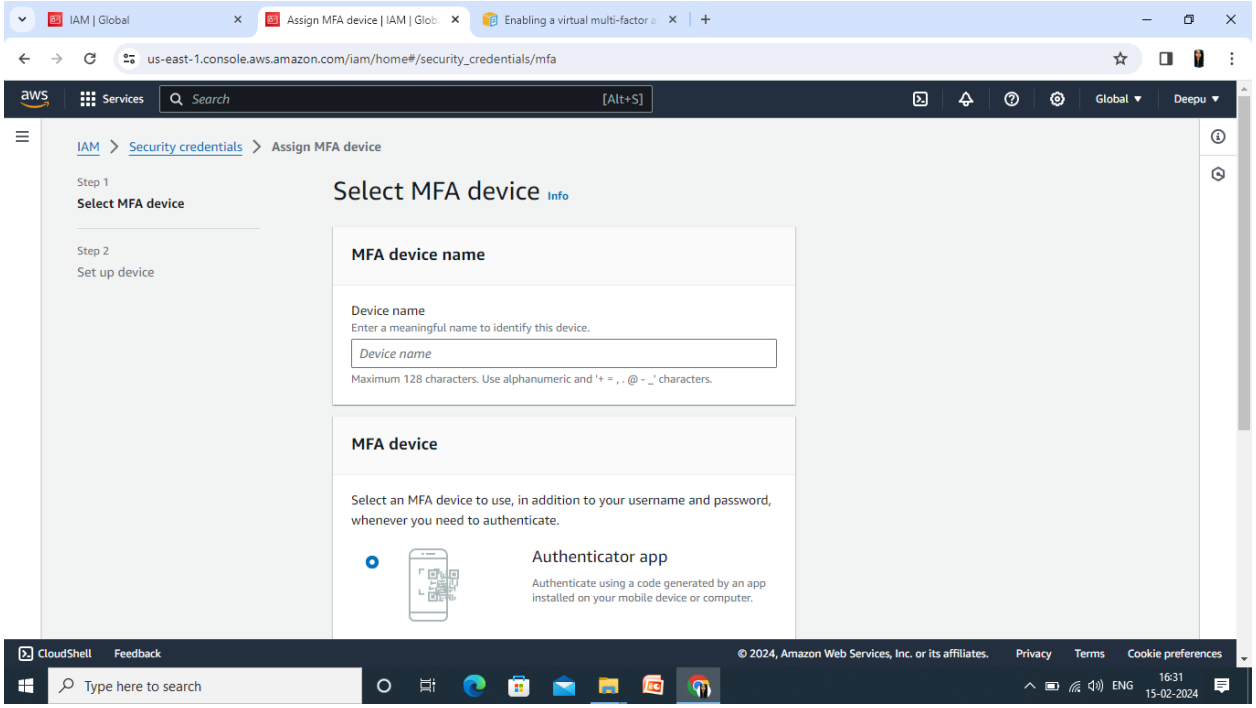
```
root@ip-172-31-6-203:~
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736,
1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: don
e

[root@ip-172-31-6-203 ~]# file -s /dev/sdm
/dev/sdm: symbolic link to `nvme1n1'
[root@ip-172-31-6-203 ~]# mount /dev/sdm /mnt/ebs_volume
[root@ip-172-31-6-203 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        456M     0  456M   0% /dev
tmpfs           464M     0  464M   0% /dev/shm
tmpfs           464M  408K  464M   1% /run
tmpfs           464M     0  464M   0% /sys/fs/cgroup
/dev/nvme0n1p1  8.0G  1.7G  6.4G  22% /
tmpfs            93M     0   93M   0% /run/user/1000
/dev/nvme1n1    9.7G   24K  9.2G   1% /mnt/ebs_volume
[root@ip-172-31-6-203 ~]# lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme0n1       259:0    0   8G  0 disk
├─nvme0n1p1   259:1    0   8G  0 part /
└─nvme0n1p128 259:2    0   1M  0 part
nvme1n1       259:3    0  10G  0 disk /mnt/ebs_volume
[root@ip-172-31-6-203 ~]#
```

6. How to protect your server from all user?

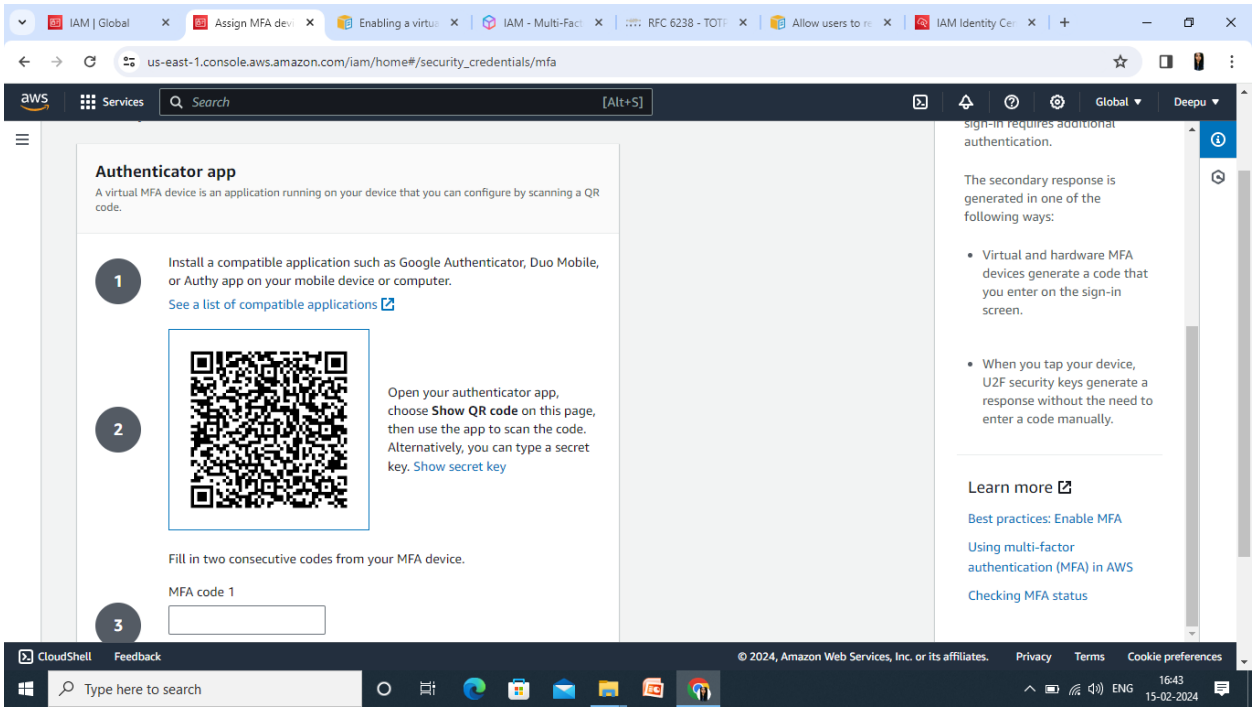
- **To protect your server from unauthorized access by all users, you need to implement Multi-Factor Authentication (MFA) for AWS IAM users accessing the AWS Management Console.**
- **Before creating MFA in AWS account**



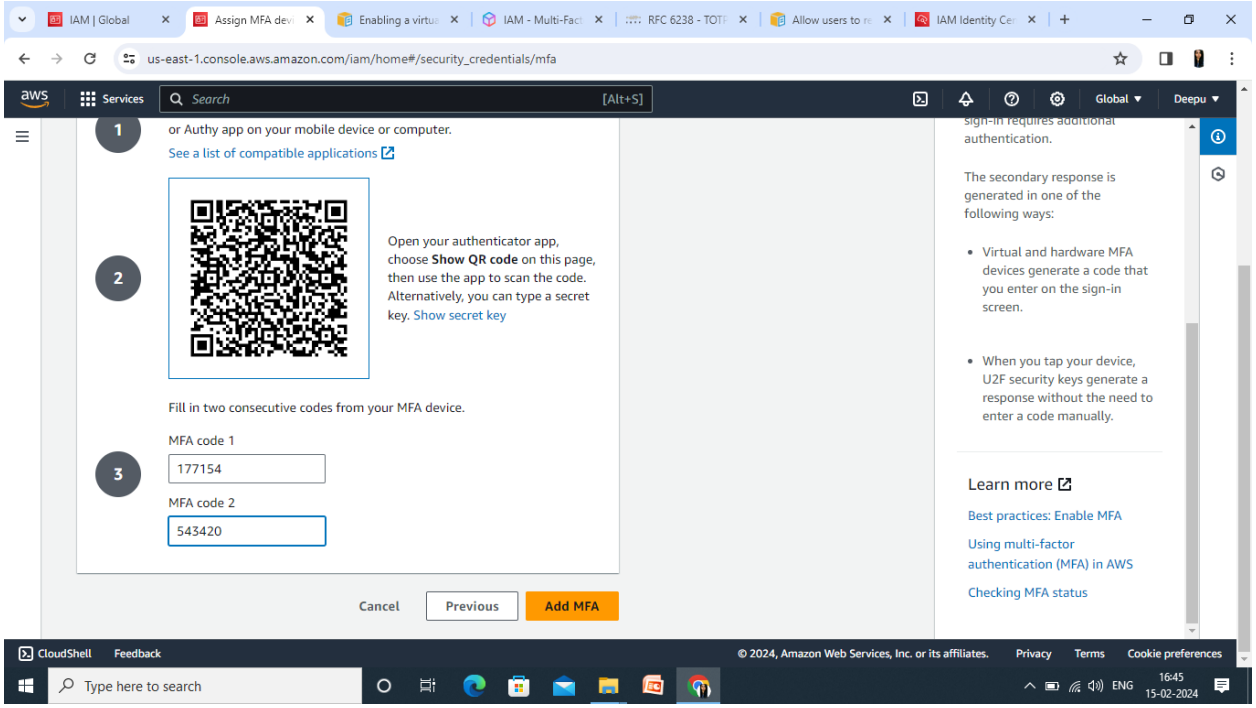
Selecting the device name and MFA Device in 3 types like Authenticating app, U2F Security key and Hardware MFA Device



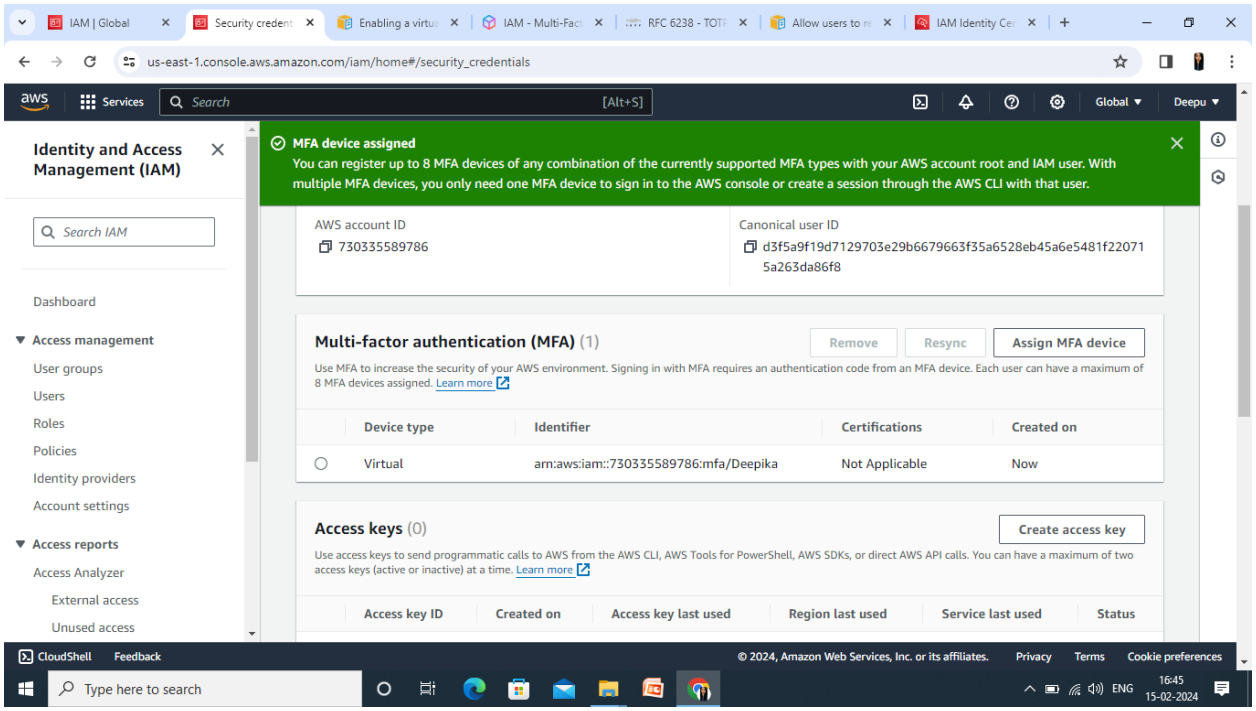
Selecting Authenticating app and scaning the QRcode



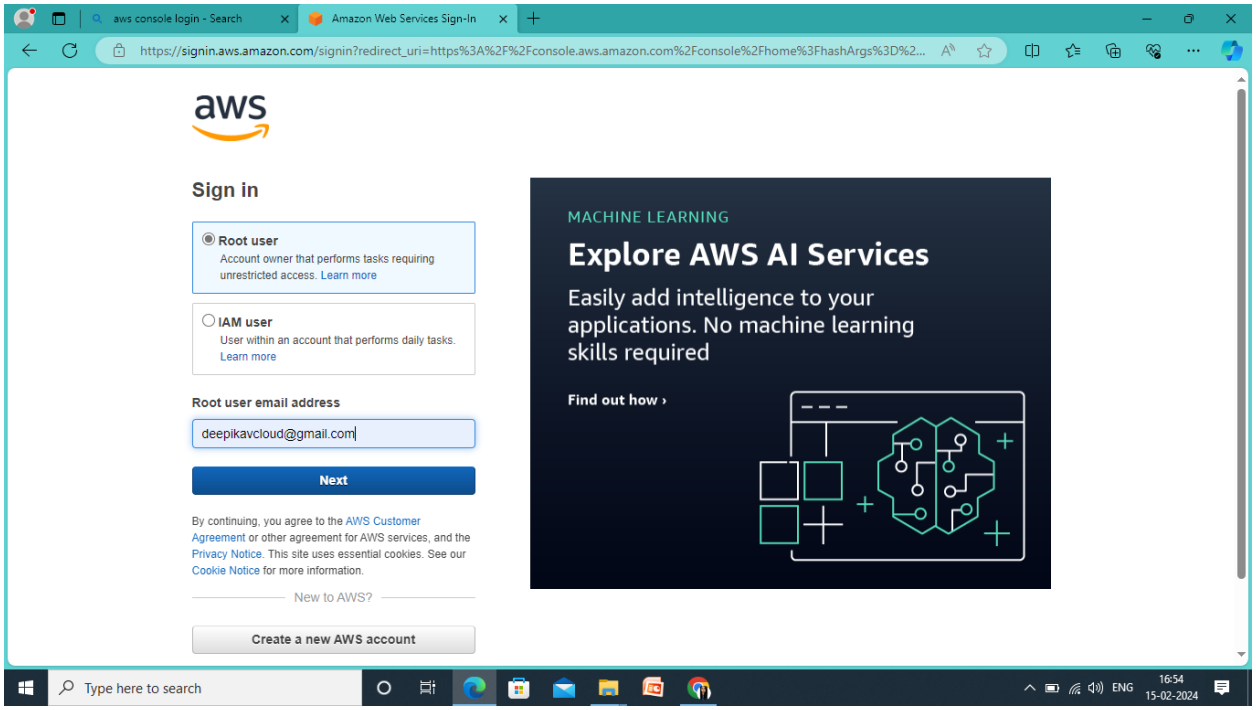
Entering the MFA code given in the Authenticator device like Mobile or Laptop after installing the application for Authenticating.

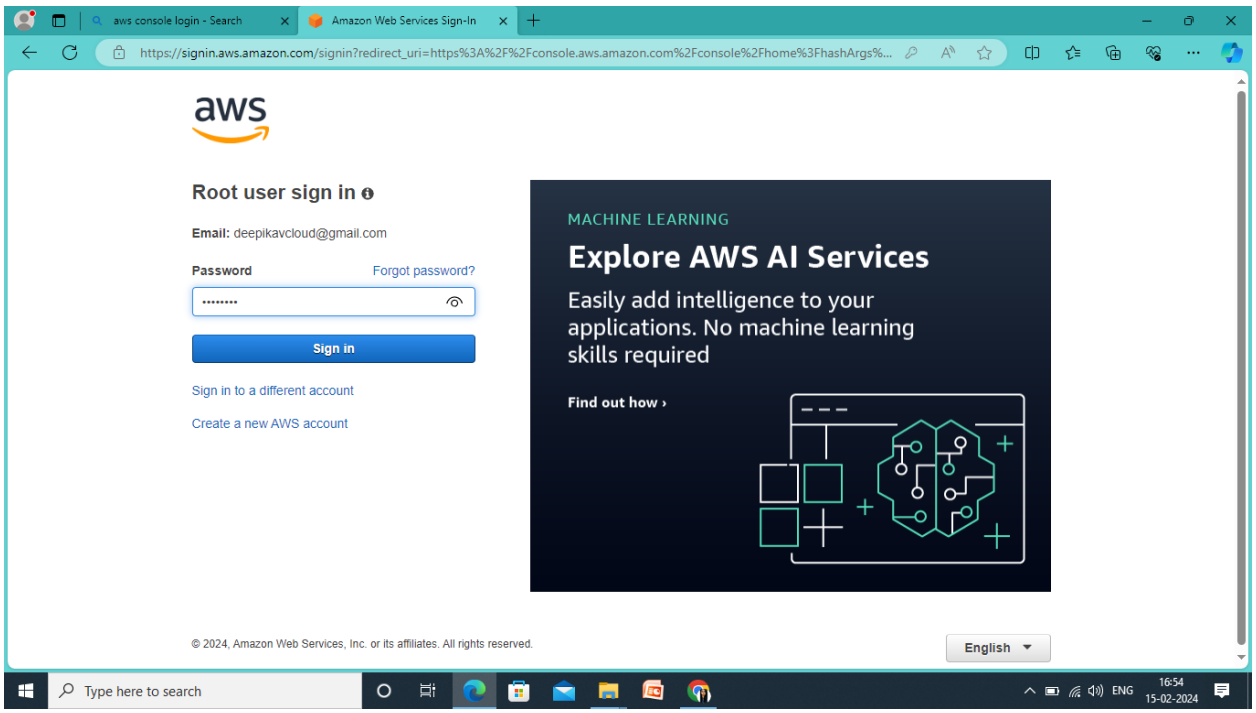


Sucessfully Assigned MFA for the AWS Account

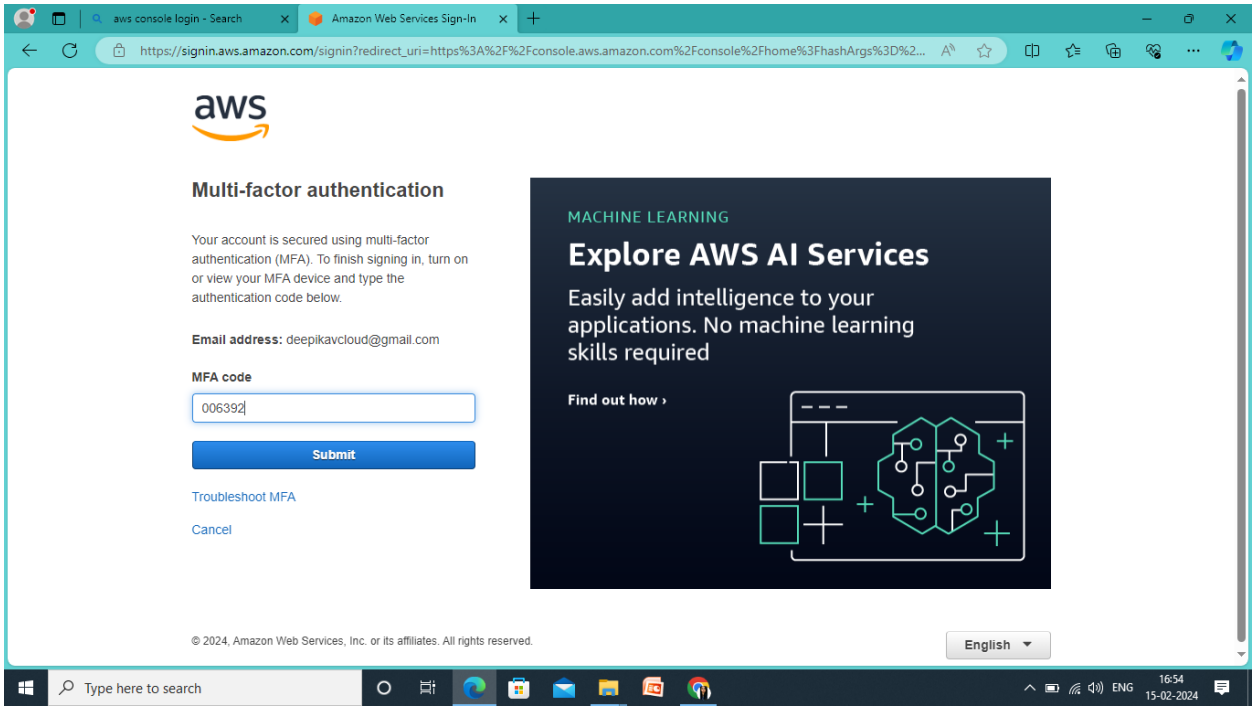


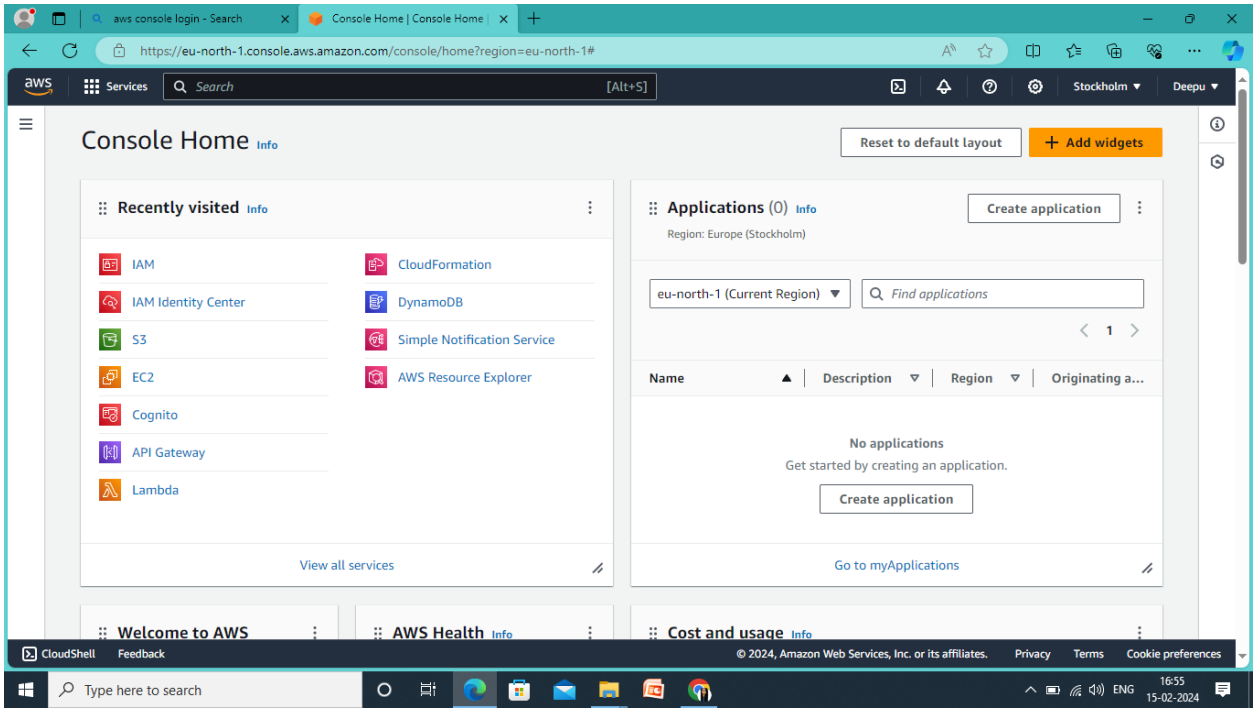
Signing-in in another Web browser to check the MFA





Again entering the MFA code for the sign-in





Other ways to prevent server from unauthorized access:

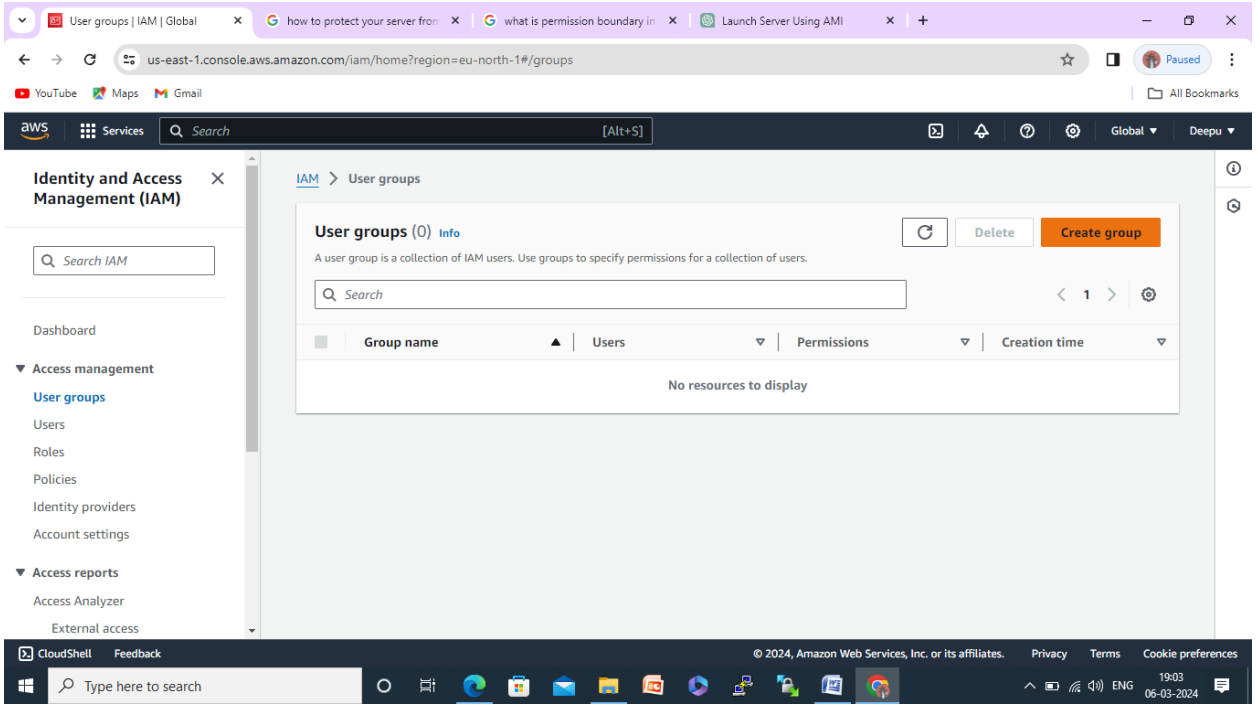
- **Utilize SSH key pairs for accessing Linux servers. Never use password-based authentication for SSH.**
- **Configure security groups and network ACLs to restrict inbound and outbound traffic to your server.**
- **Use VPC (Virtual Private Cloud) and subnet configurations to isolate your server from the public internet if it's not necessary for your application.**
- **Assign IAM roles with the minimum required permissions to AWS users, limiting access only to necessary resources.**
- **Utilize IAM policies and resource-based policies (such as S3 bucket policies) to control access to AWS service.**
- **Keep your server's operating system and software up to date with the latest security patches to protect against known vulnerabilities.**
- **Implement logging and monitoring solutions to detect and respond to unauthorized access attempts or suspicious activities.**
- **Utilize AWS CloudTrail to log API calls and AWS Config to monitor and manage AWS resource configurations.**
- **Create regular backups of your server's data and configurations to ensure you can recover quickly in the event of data loss or corruption.**

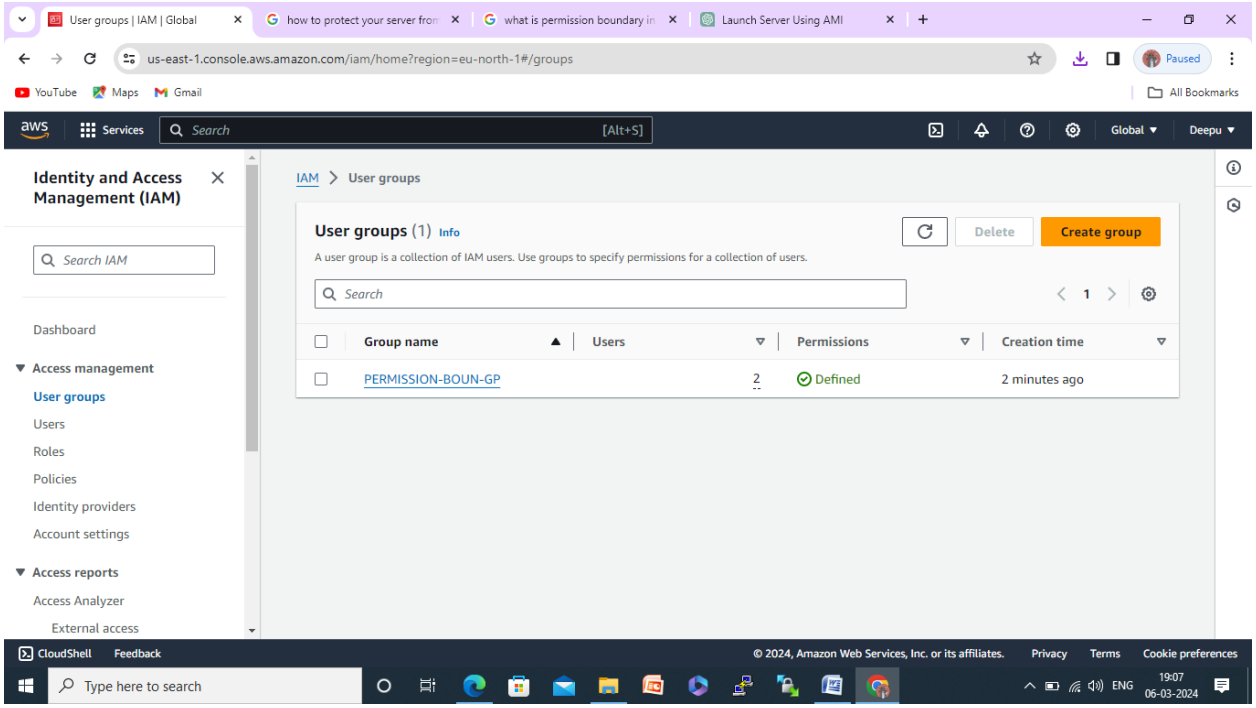
7. What is IAM permission boundaries?

A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. An entity's permissions boundary allows it to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries.

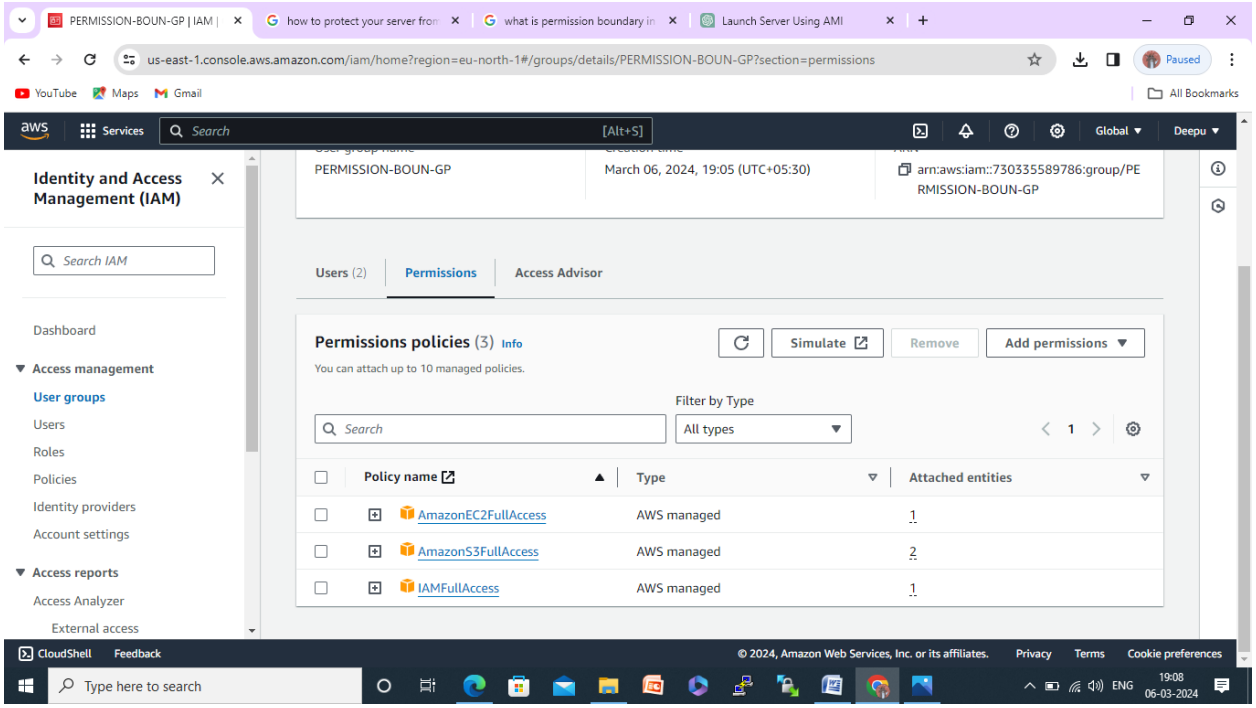
A permission boundary in AWS IAM is like a safety net or boundary that you put around an IAM entity (such as a user or role) to limit the maximum permissions it can have. It's like setting a maximum level of access that cannot be exceeded, regardless of any policies attached to the IAM entity.

Creating a group to set policies for a users in this group

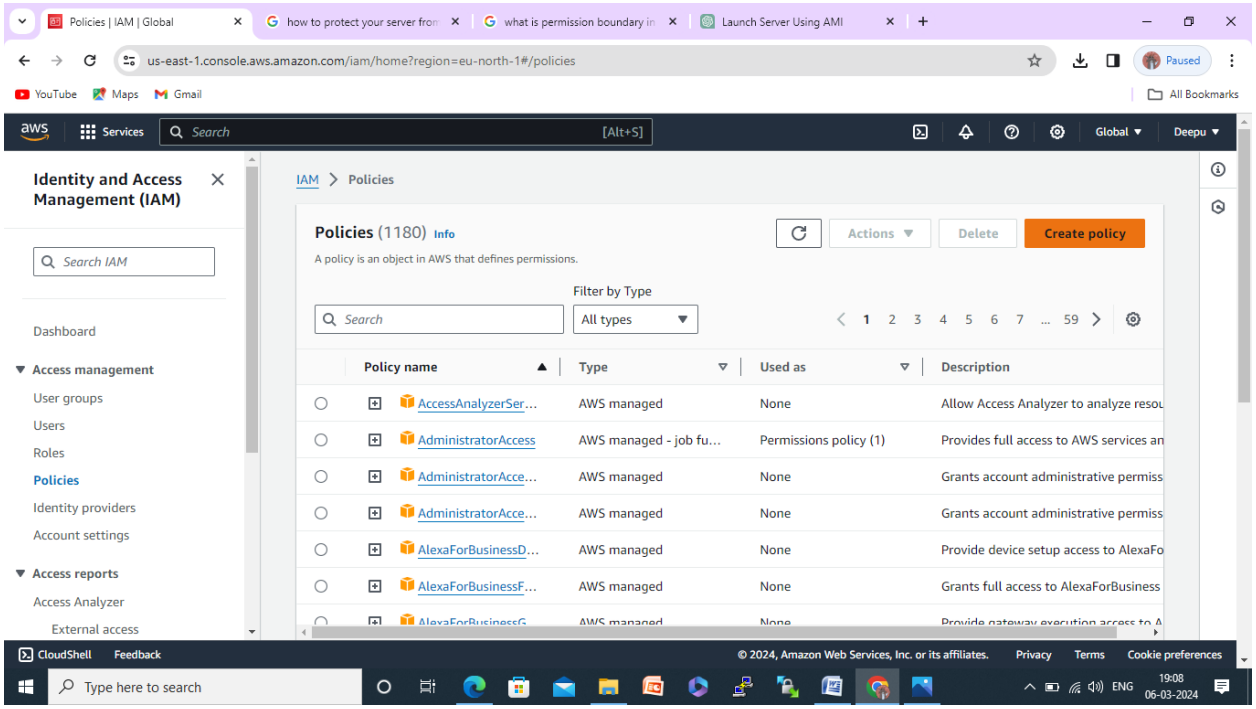




Allowing full access to IAM,EC2 and S3 for that group.



Creating a Custom IAM list and read policy for a testuser in that group to set as a permission boundaries.



Create policy | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

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

Policy editor Visual JSON Actions

IAM

Set permissions for IAM

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

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect
Allow Deny

Manual actions | Add actions

All IAM actions (iam:*)

Create policy | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

IAM

Allow 38 Actions

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

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect
Allow Deny

Manual actions | Add actions

All IAM actions (iam:*)

Access level

Expand all | Collapse all

List (Selected 38/38)

All list actions

GetAccountSummary Info	GetLoginProfile Info	ListAccessKeys Info
ListAccountAliases Info	ListAttachedGroupPolicies Info	ListAttachedRolePolicies Info
ListAttachedUserPolicies Info	ListCloudFrontPublicKeys Info	ListEntitiesForPolicy Info
ListGroupPolicies Info	ListGroups Info	ListGroupsForUser Info

Create policy | IAM | Global

how to protect your server from

what is permission boundary in

Launch Server Using AMI

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

Paused

YouTube Maps Gmail

All Bookmarks

aws Services Search [Alt+S] Global Deepu

IAM

Allow 70 Actions

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

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect

Allow Deny

Manual actions | Add actions

All IAM actions (iam:*)

Access level

Expand all | Collapse all

List (Selected 38/38)

Read (Selected 32/32)

Write (62)

Permissions management (23)

Tagging (16)

Required permissions not selected.

CloudShell Feedback

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

Privacy Terms Cookie preferences

Type here to search

ENG 19:09 06-03-2024

Create policy | IAM | Global

how to protect your server from

what is permission boundary in

Launch Server Using AMI

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

Paused

YouTube Maps Gmail

All Bookmarks

aws Services Search [Alt+S] Global Deepu

To grant permissions for the selected resource actions, you must include additional required actions

- iam:GenerateOrganizationsAccessReport requires 6 more actions.

Resources

Specify resource ARNs for these actions.

All

Specific

The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

Request conditions - *optional*

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

Add more permissions

Security: 0 Errors: 0 Warnings: 0 Suggestions: 2

Cancel Next

CloudShell Feedback

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

Privacy Terms Cookie preferences

Type here to search

ENG 19:09 06-03-2024

Create policy | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

Specify permissions

Step 2

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

IAM-CUSTOM-POLICY

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*

Add a short explanation for this policy.

IAM-LIST AND READ

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

Permissions defined in this policy Info

Edit

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

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 404 services)

Show remaining 403 services

Service	Access level	Resource	Request condition
IAM	Full: Read, List	All resources	None

Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

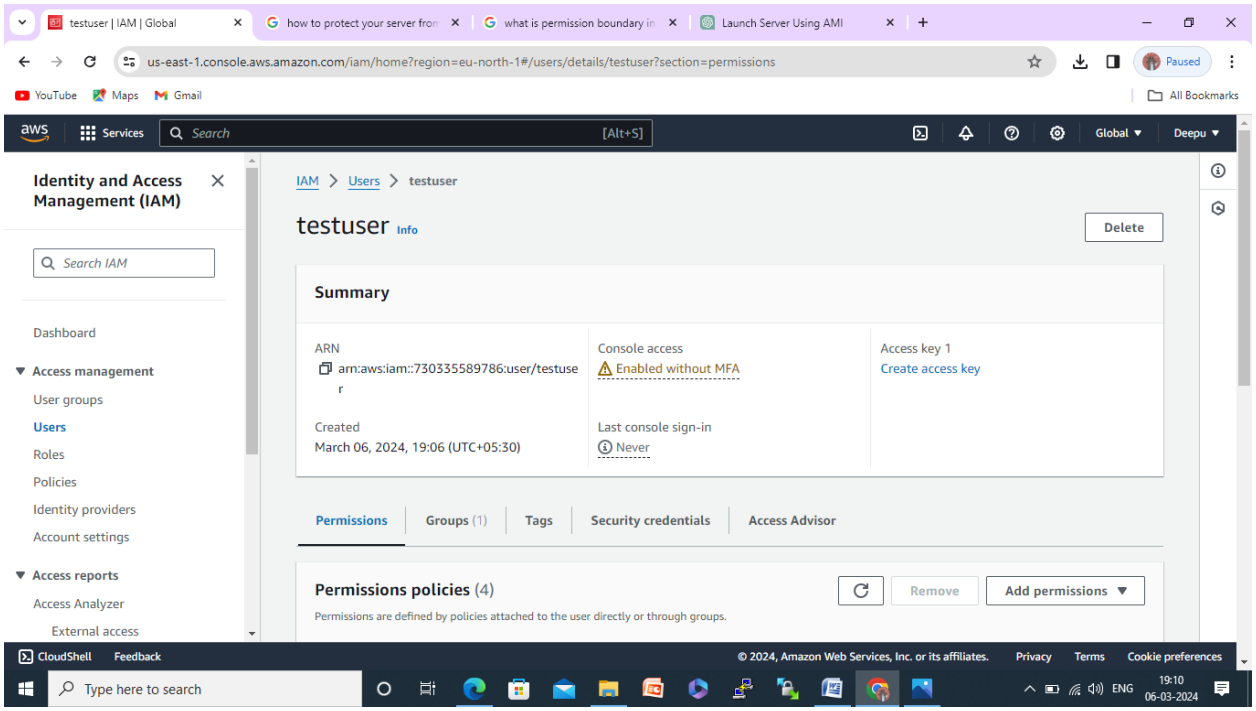
No tags associated with the resource.

Add new tag

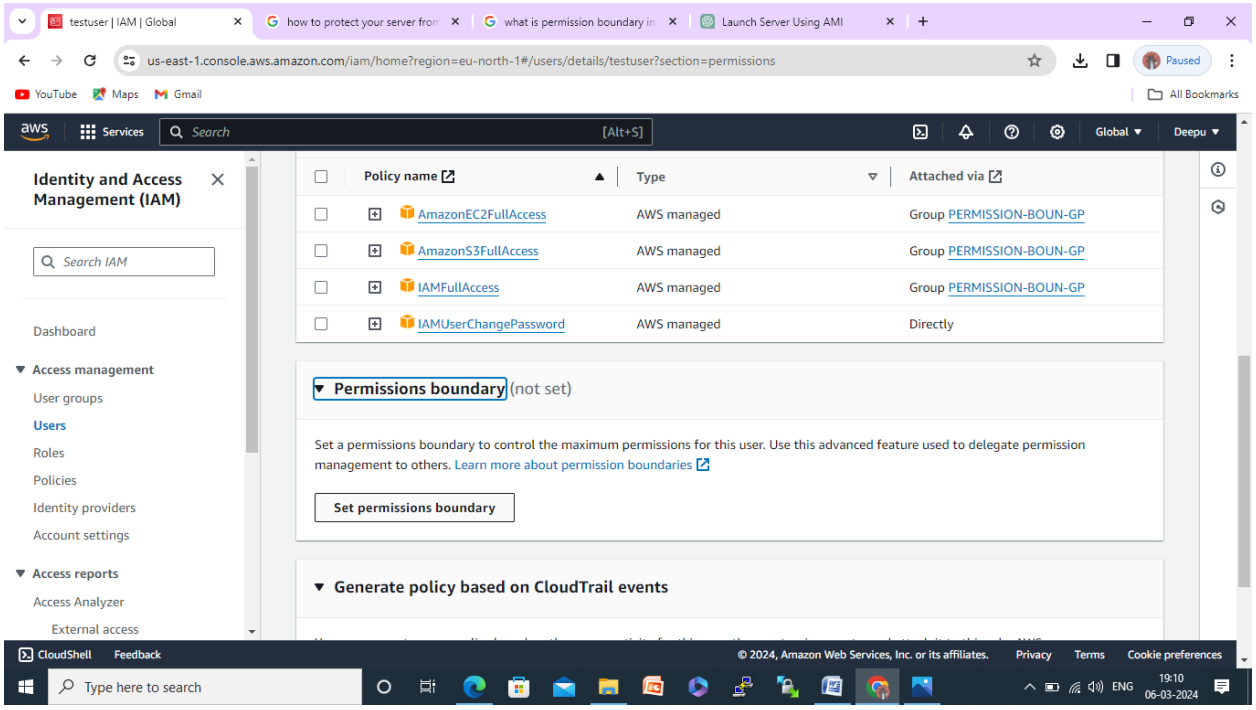
You can add up to 50 more tags.

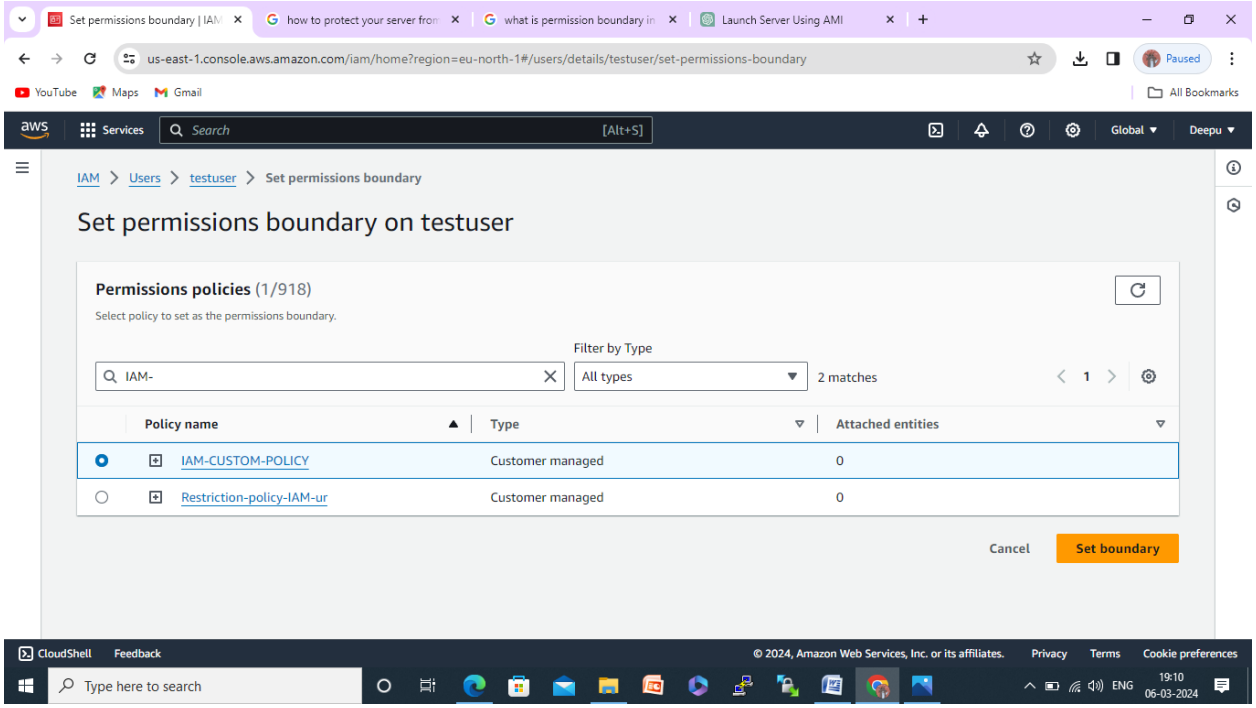
Cancel | Previous | Create policy

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

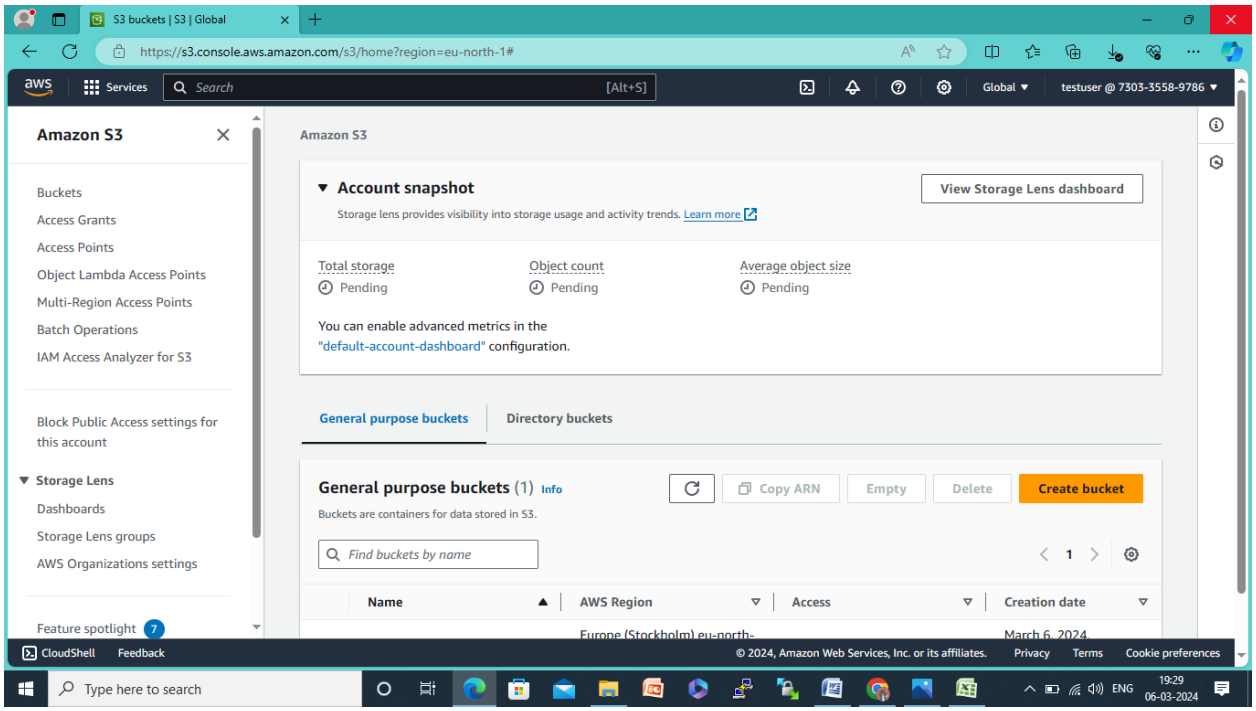


Now setting that IAM custom policy as a permission boundary for the testuser.

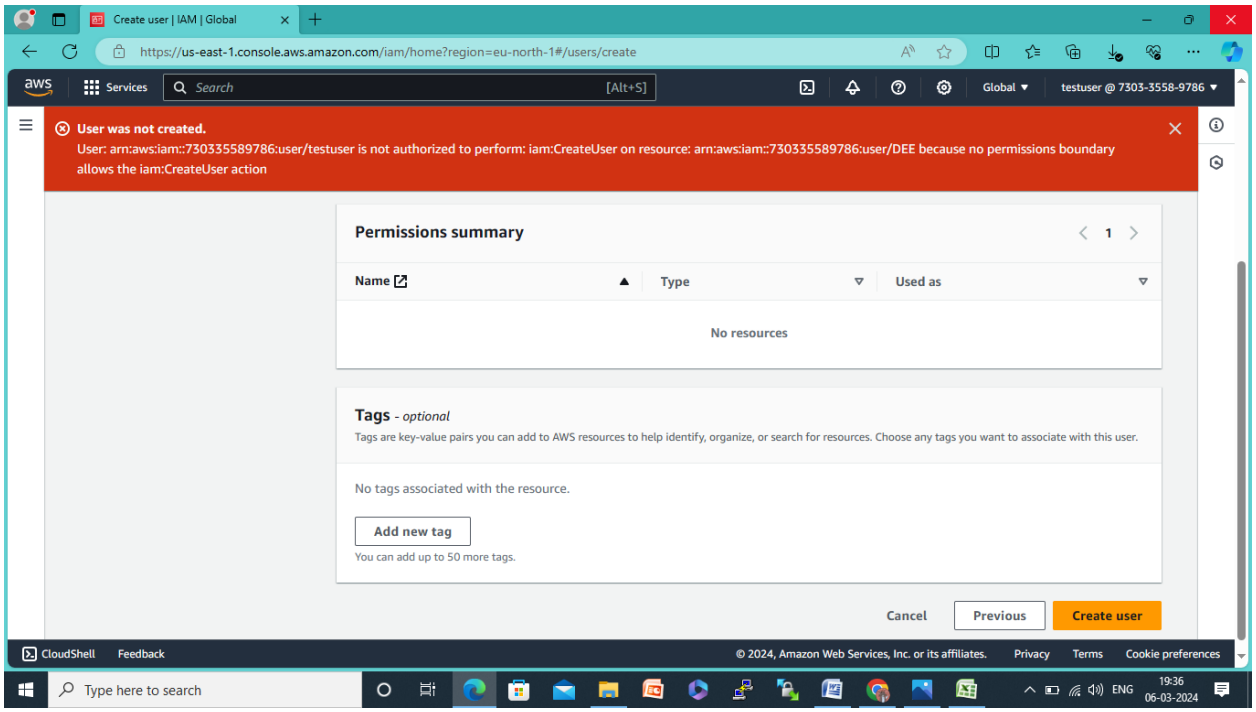


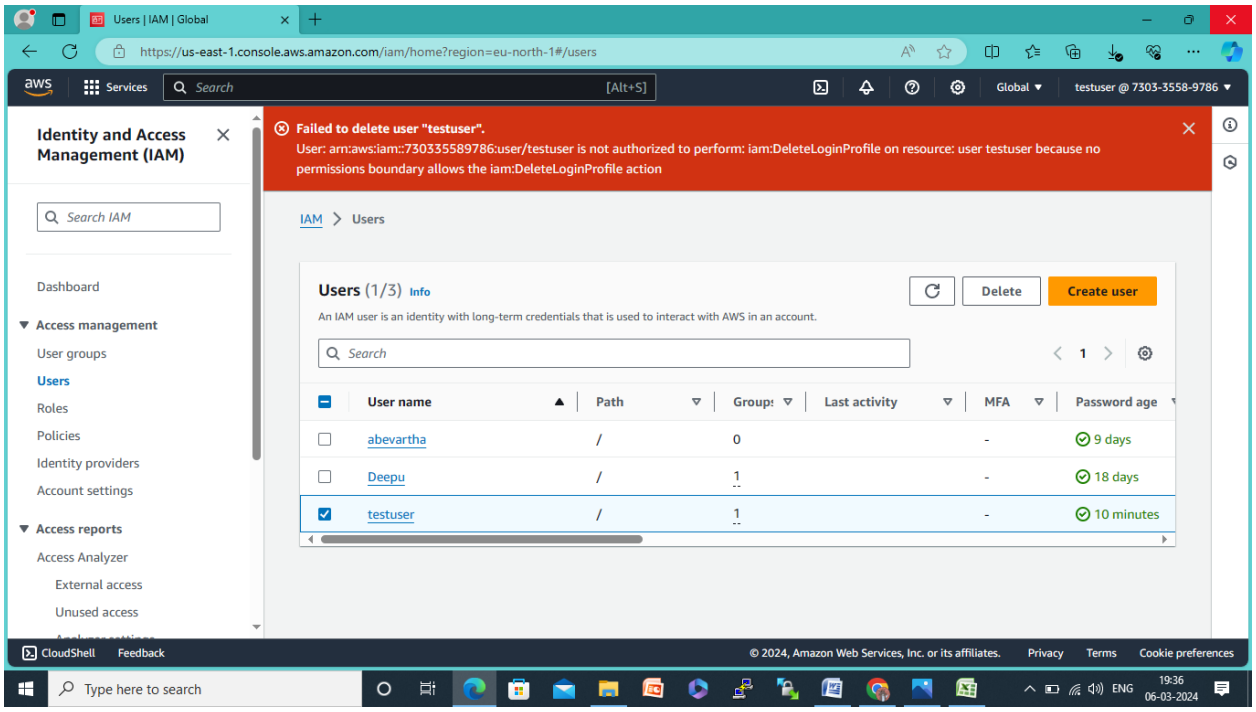


Now logining into the testuser account to check the permission boundary for that testuser



The testuser only have the permissions for LIST and READ, so failed to create and delete the user in the group level also.



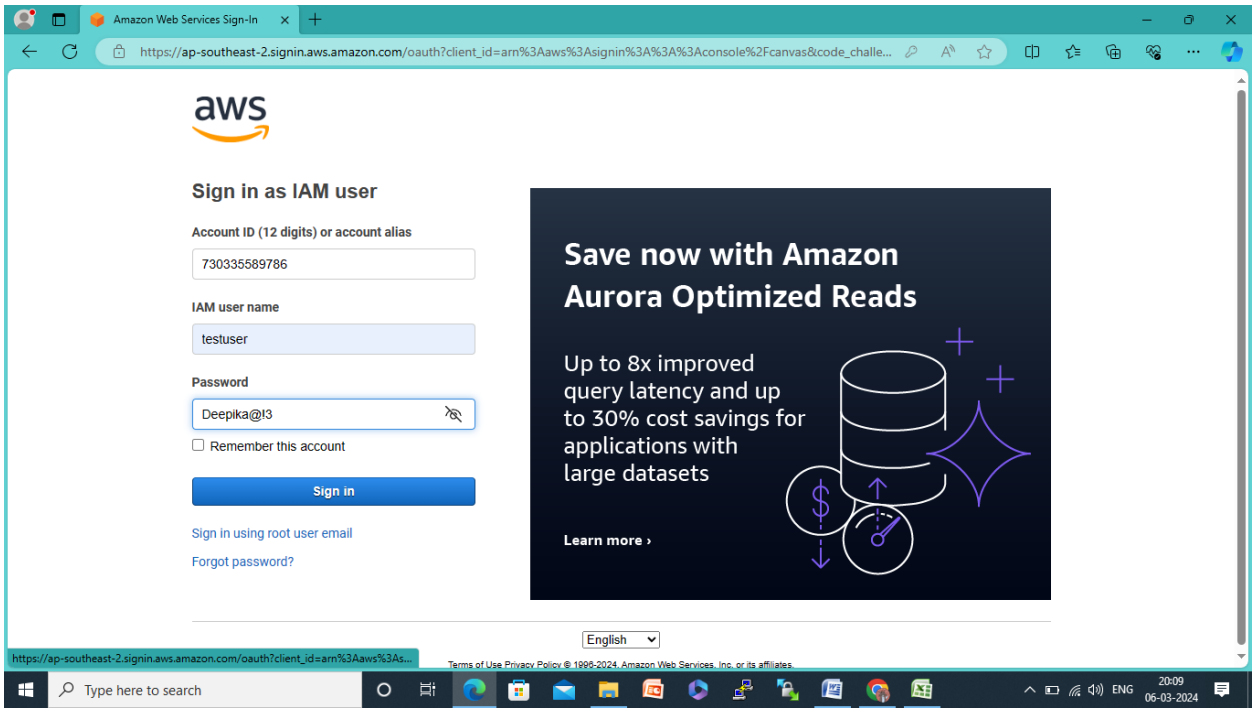


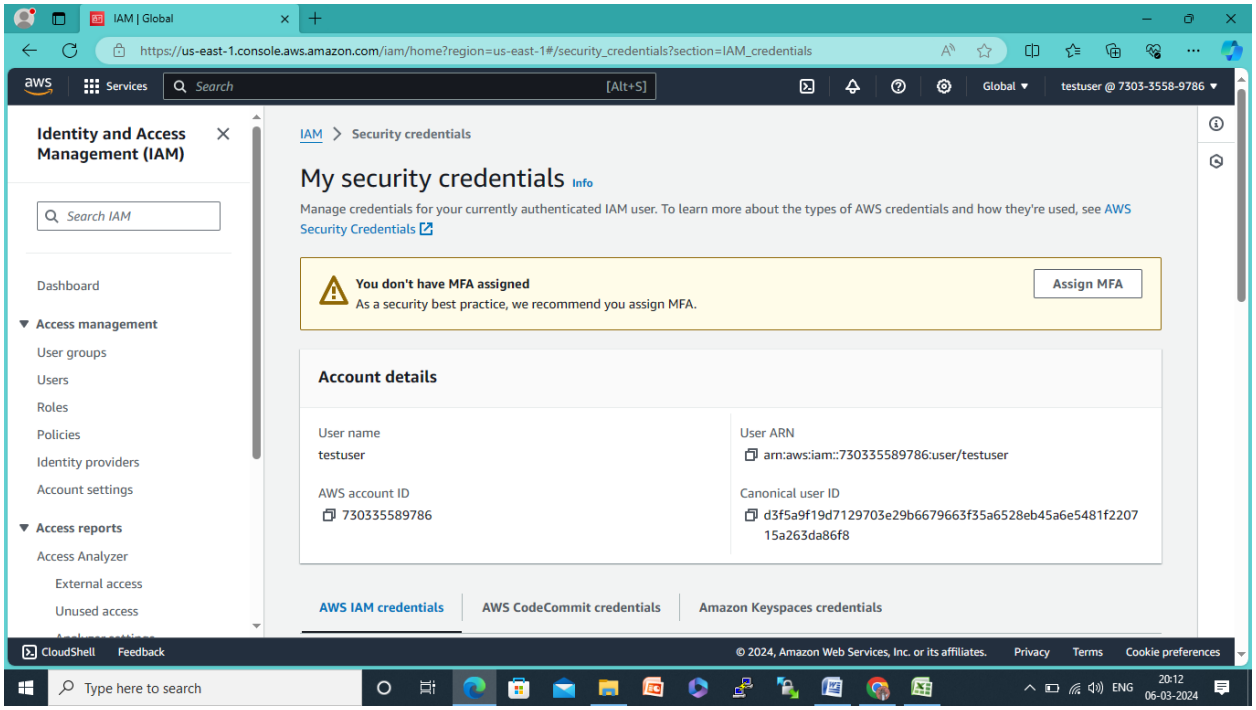
8. IAM user can change them password if yes means how if no means why?

Yes, IAM users can change their own passwords in AWS.

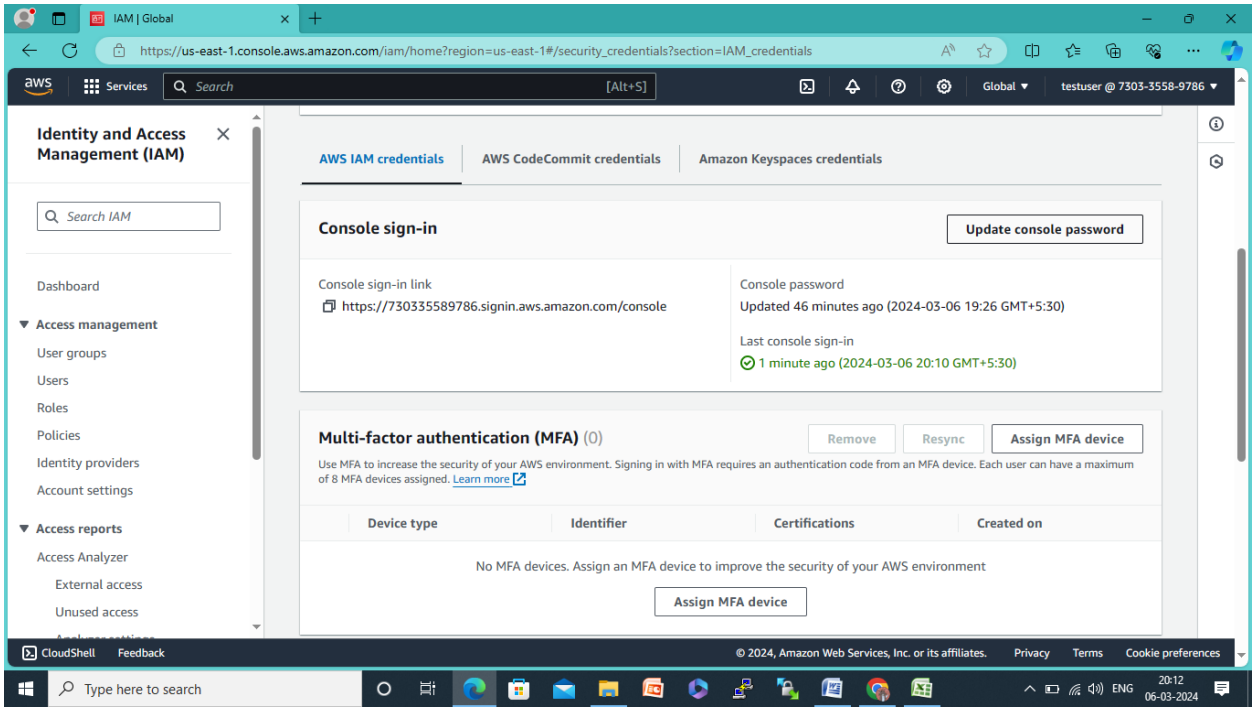
AWS IAM allows users to manage their own credentials, including changing their passwords, provided they have the necessary permissions to do so..

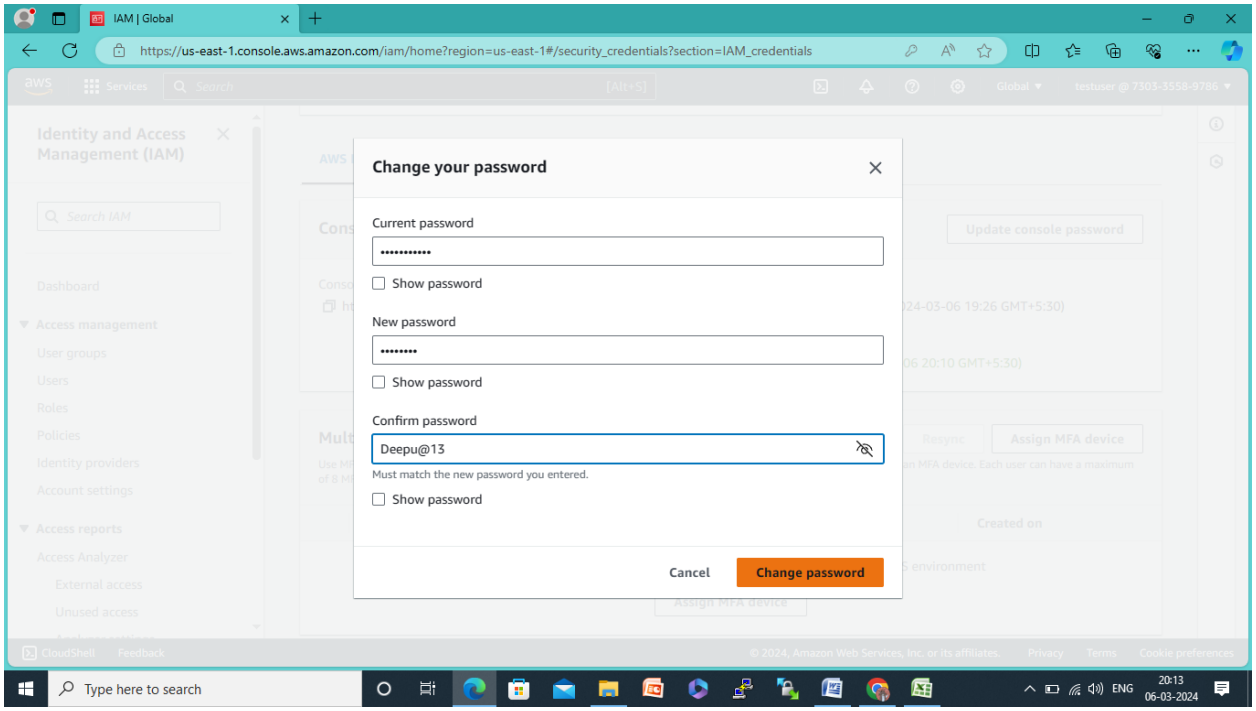
Signing in the IAM user account.

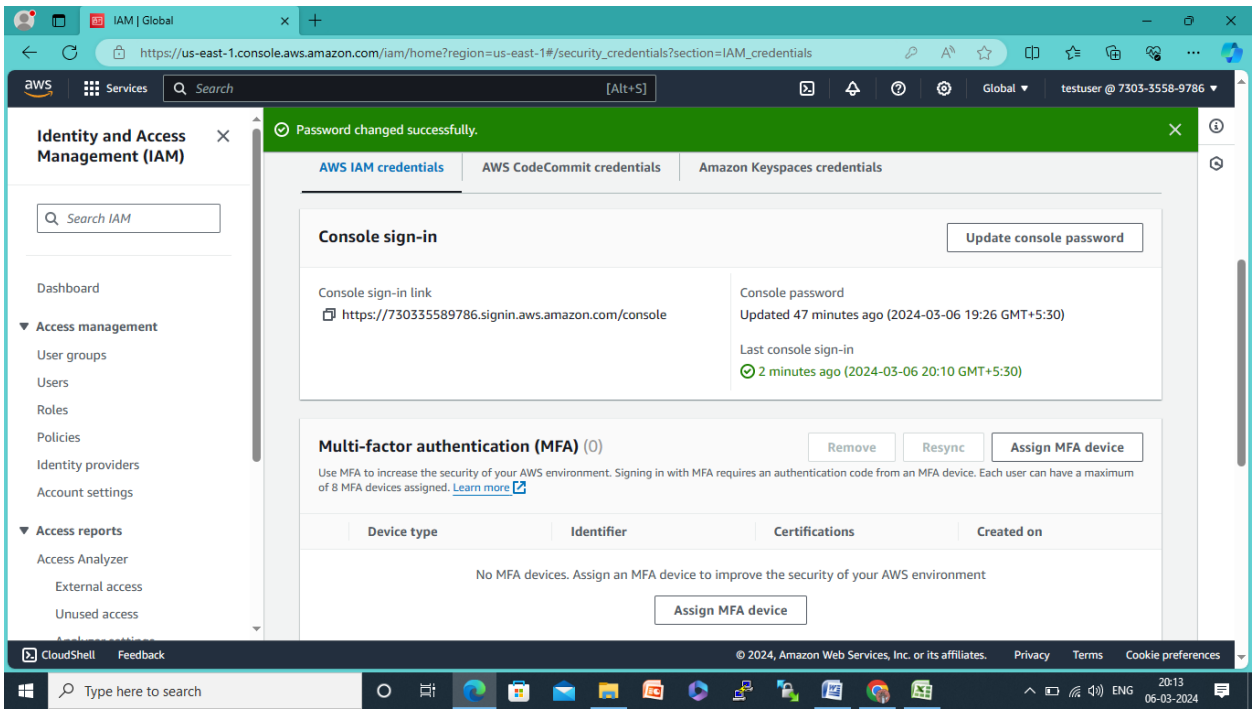



IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/security_credentials?section=IAM_credentials
Services
Search
[Alt+S]
Global
testuser @ 7303-3558-9786
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
IAM > Security credentials
My security credentials Info
Manage credentials for your currently authenticated IAM user. To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials
You don't have MFA assigned
As a security best practice, we recommend you assign MFA.
Assign MFA
Account details
User name
testuser
User ARN
arn:aws:iam::730335589786:user/testuser
AWS account ID
730335589786
Canonical user ID
d3f5a9f19d7129703e29b6679663f35a6528eb45a6e5481f2207 15a263da86f8
AWS IAM credentials
AWS CodeCommit credentials
Amazon Keyspaces credentials
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
20:12
06-03-2024

•


IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/security_credentials?section=IAM_credentials
Services
Search
[Alt+S]
Global
testuser @ 7303-3558-9786
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
AWS IAM credentials
AWS CodeCommit credentials
Amazon Keyspaces credentials
Console sign-in
Update console password
Console sign-in link
https://730335589786.signin.aws.amazon.com/console
Console password
Updated 46 minutes ago (2024-03-06 19:26 GMT+5:30)
Last console sign-in
1 minute ago (2024-03-06 20:10 GMT+5:30)
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Device type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
20:12
06-03-2024

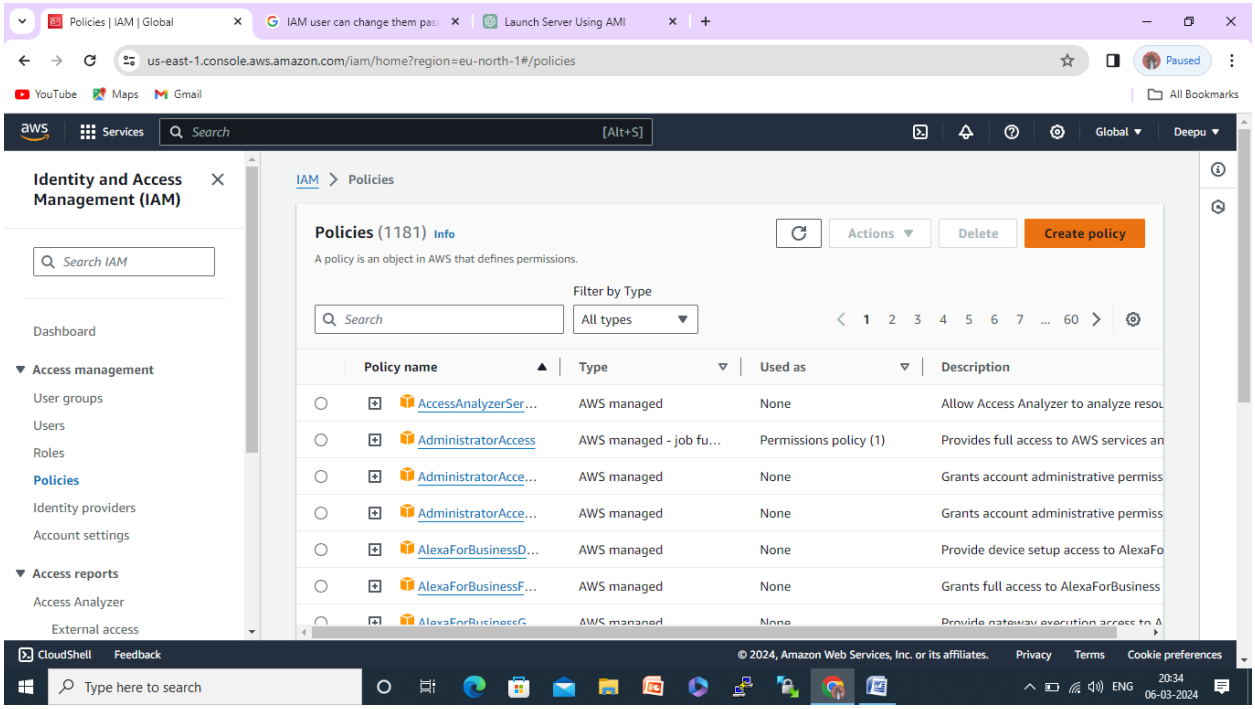

IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/security_credentials?section=IAM_credentials
Change your password
Current password
Show password
New password
Show password
Confirm password
Deepu@13
Must match the new password you entered.
Show password
Cancel
Change password
Type here to search


IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/security_credentials?section=IAM_credentials
Services
Search
[Alt+S]
Global
testuser @ 7303-3558-9786
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Password changed successfully.
AWS IAM credentials
AWS CodeCommit credentials
Amazon Keyspaces credentials
Console sign-in
Update console password
Console sign-in link
https://730335589786.signin.aws.amazon.com/console
Console password
Updated 47 minutes ago (2024-03-06 19:26 GMT+5:30)
Last console sign-in
2 minutes ago (2024-03-06 20:10 GMT+5:30)
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Device type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search

We can also restrict the IAM user to not to change their password :

- **IAM administrators can also reset passwords for IAM users if needed.**
- **Additionally, IAM policies can control whether IAM users are allowed to change their own passwords and what password policies must be followed.**

Creating custom policy for restrict the IAM user to not to change the password.



Create policy | IAM | Global

IAM user can change them pas

Launch Server Using AMI

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

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

Policy editor

Visual | JSON | Actions

```
1 {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Effect": "Deny",
6             "Action": "iam:ChangePassword",
7             "Resource": "*"
8         }
9     ]
10 }
11
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search ENG 20:35 06-03-2024

Create policy | IAM | Global

IAM user can change them pas

Launch Server Using AMI

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

Step 2
Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

IAM-NOACCESS-PASSWORD

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

Edit

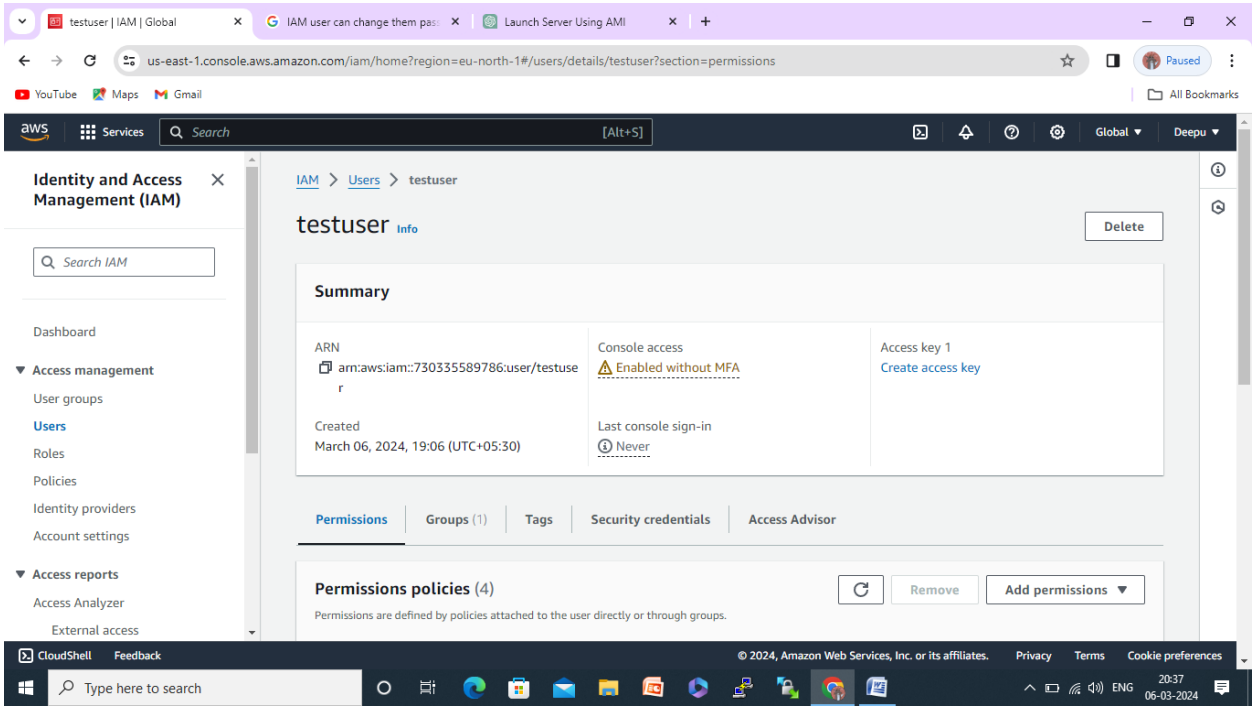
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

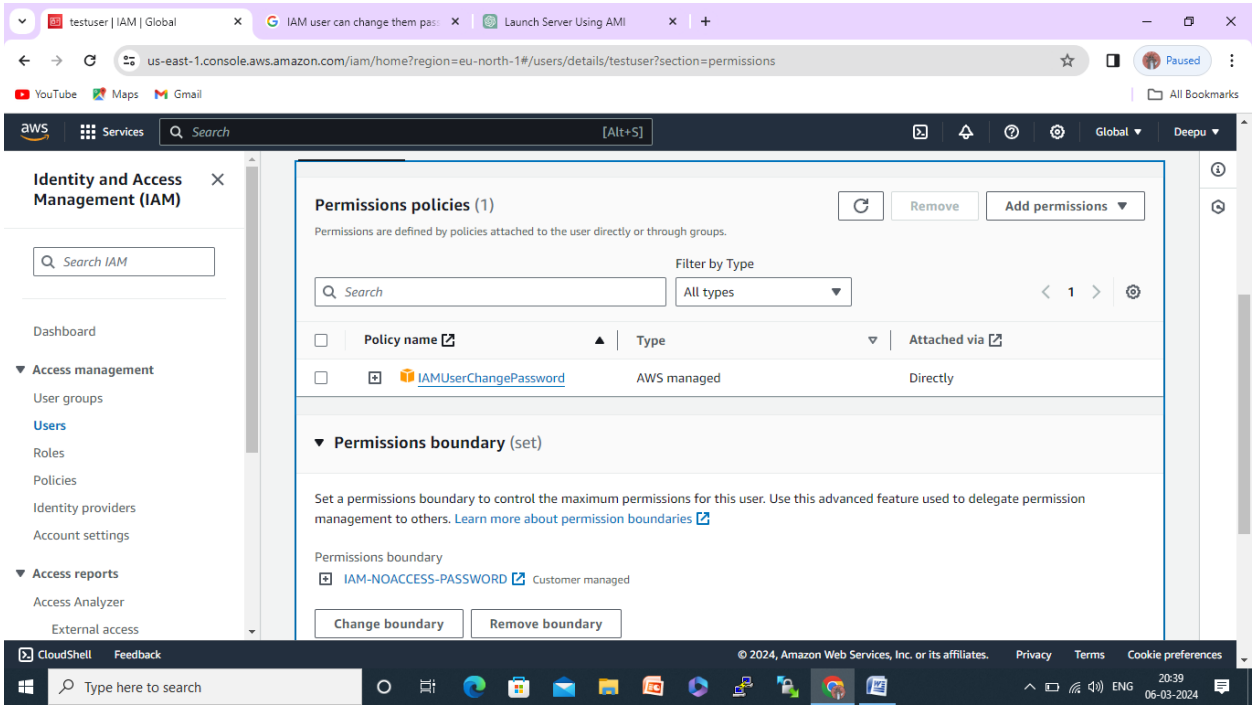
Search

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

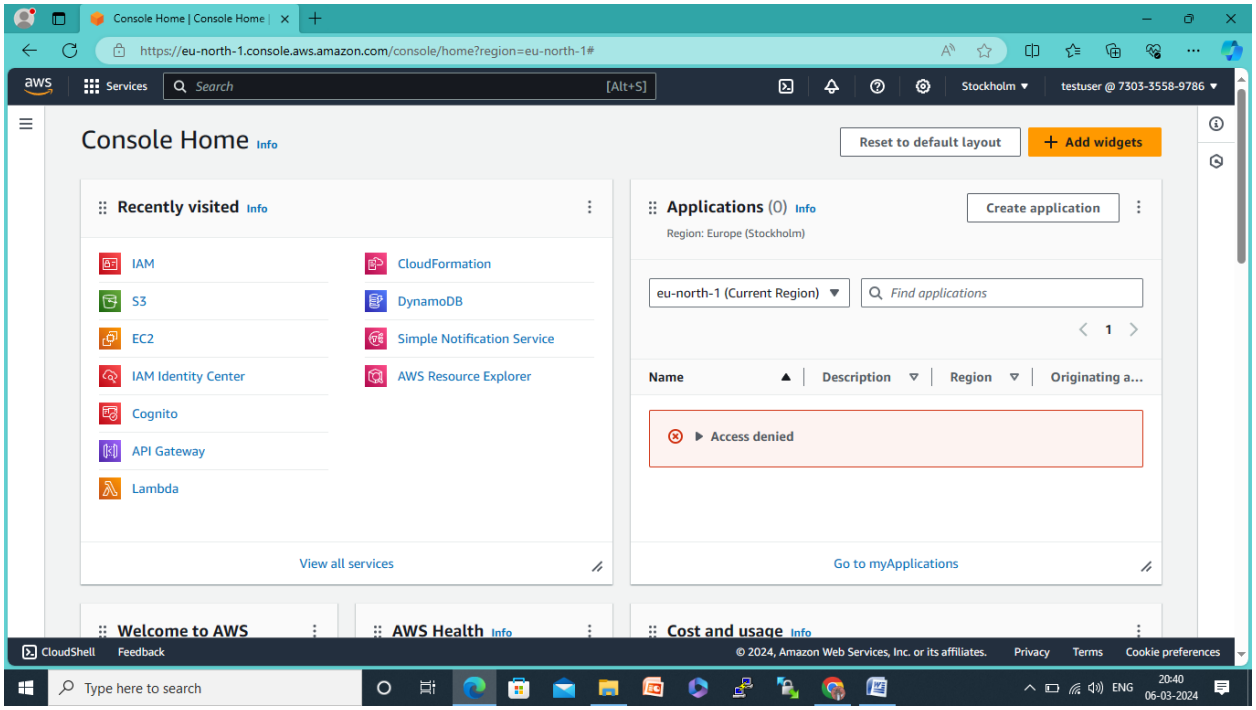
Type here to search ENG 20:37 06-03-2024

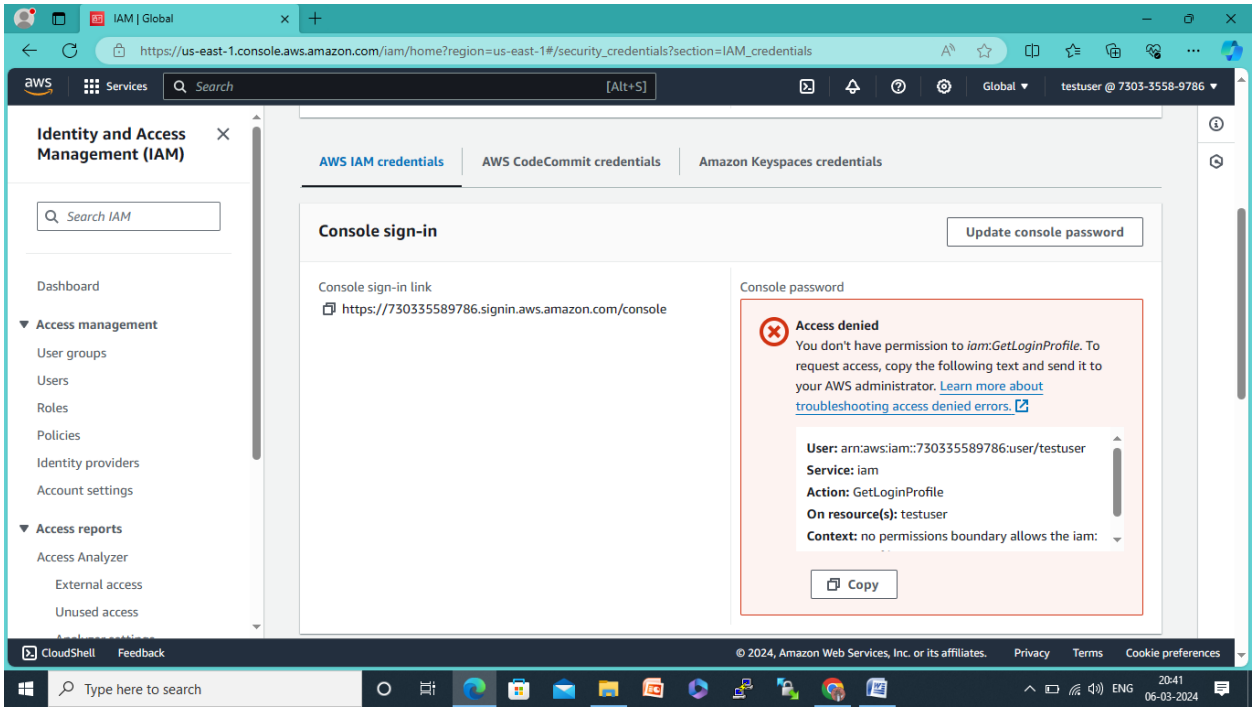
Setting the custom policy as Permission boundary for that IAM user to not to change the password.





Sigining in the IAM user console to change the password, its shows restriction.





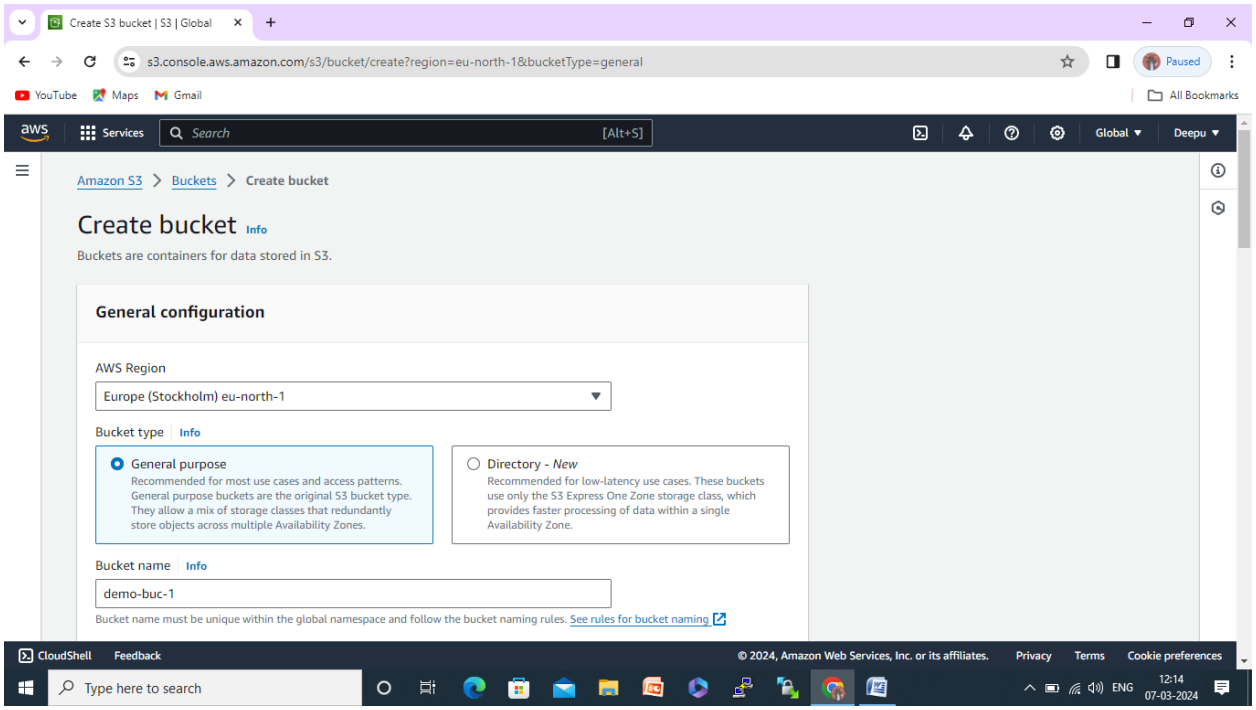
9. How many instances can create at the time?

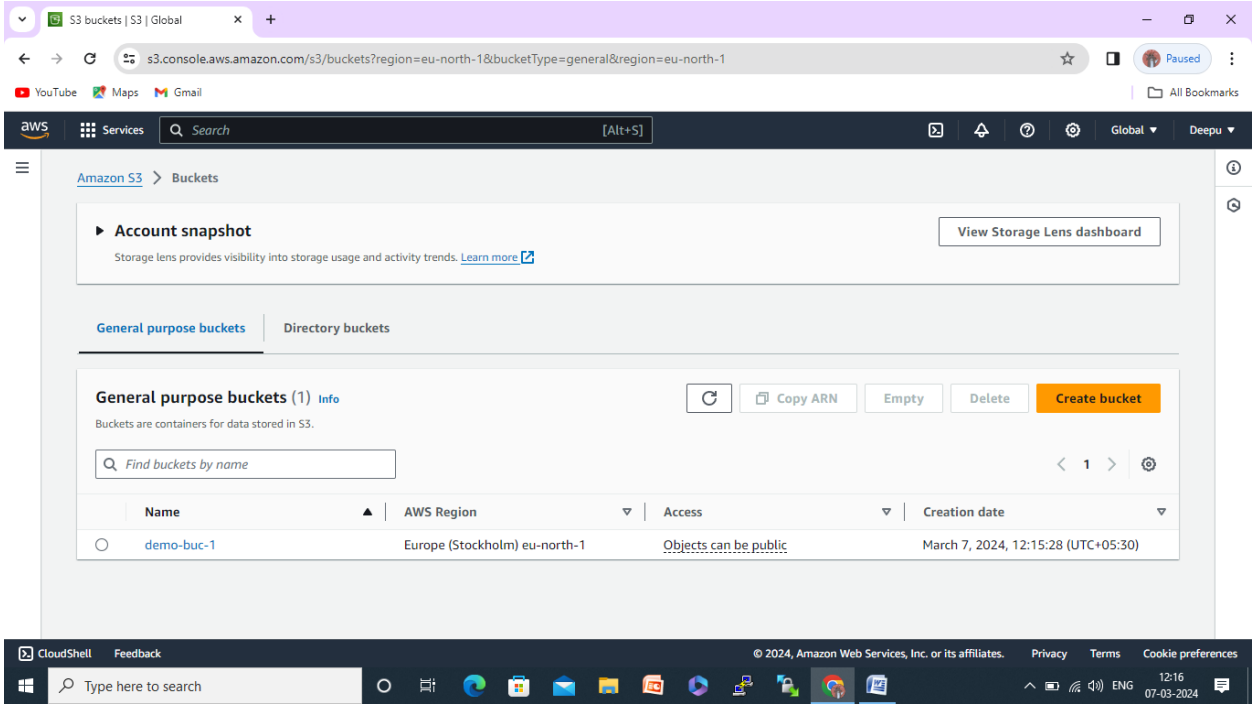
- **By default, AWS has a limit of 20 instances per region.**
- **This includes all instances set up and configurations on your AWS account.**
- **To increase EC2 limits, request a higher limit by providing information about the new limit and regions where it should be applied.**

10. How to access object in private bucket?

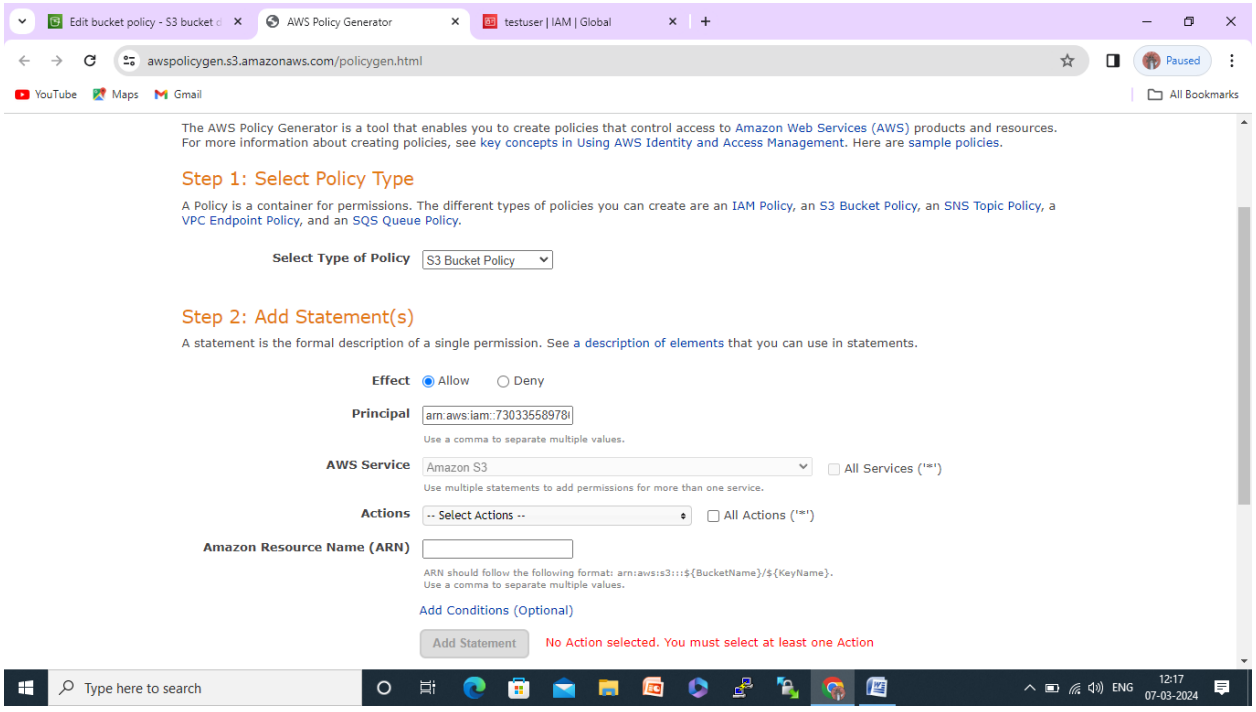
Through bucket policy the access will be limited to the contents of the specific bucket to Access it privately by the user.

Creating a bucket to create a bucket level policy for an IAM user.

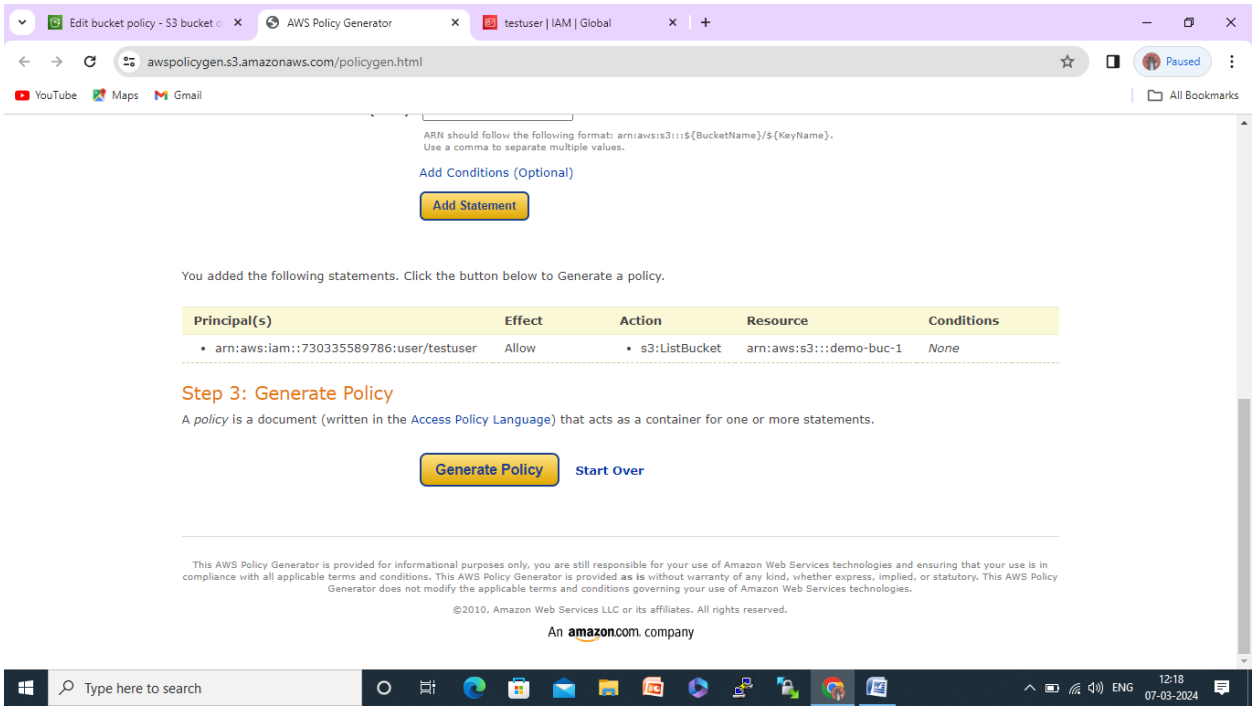


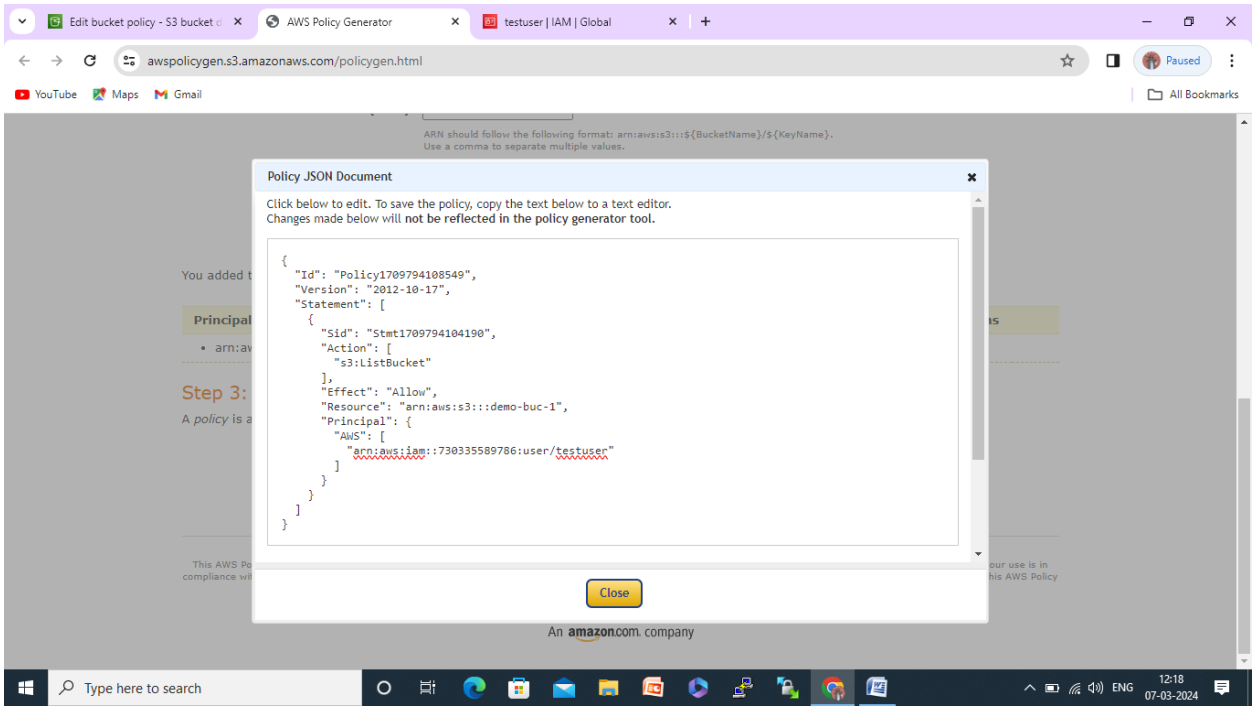


Then creating a bucket policy for that bucket using a policy generator

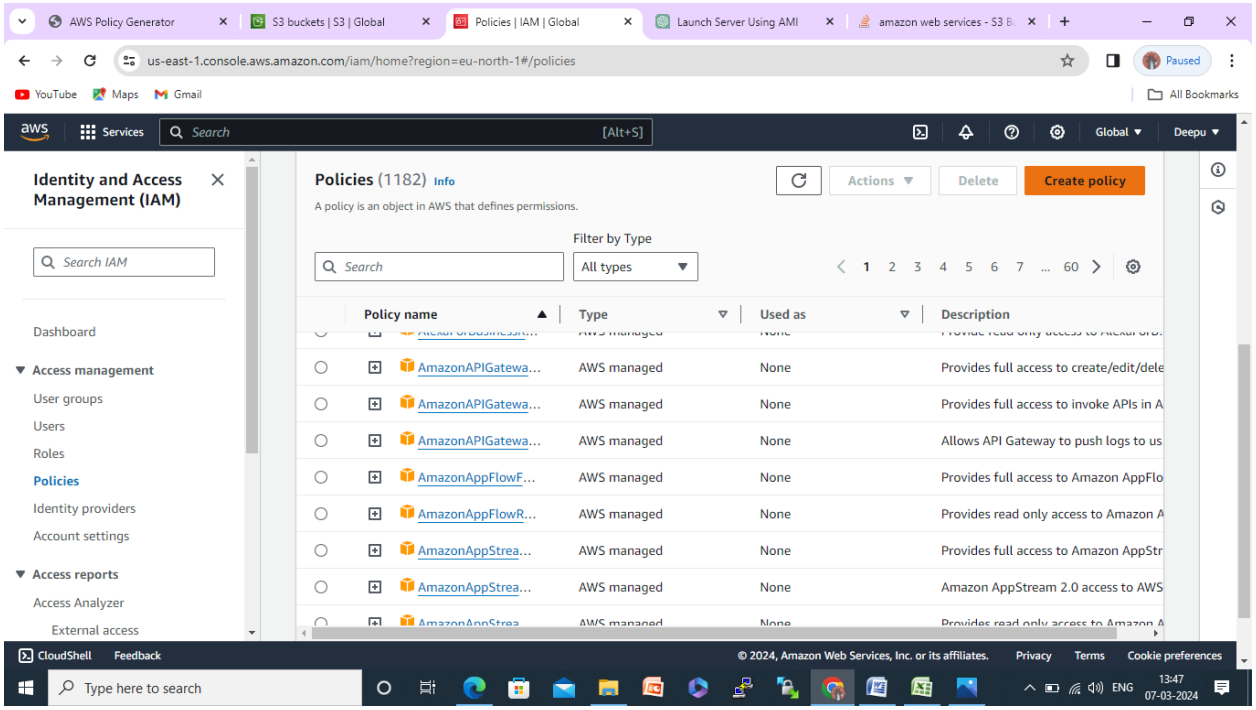


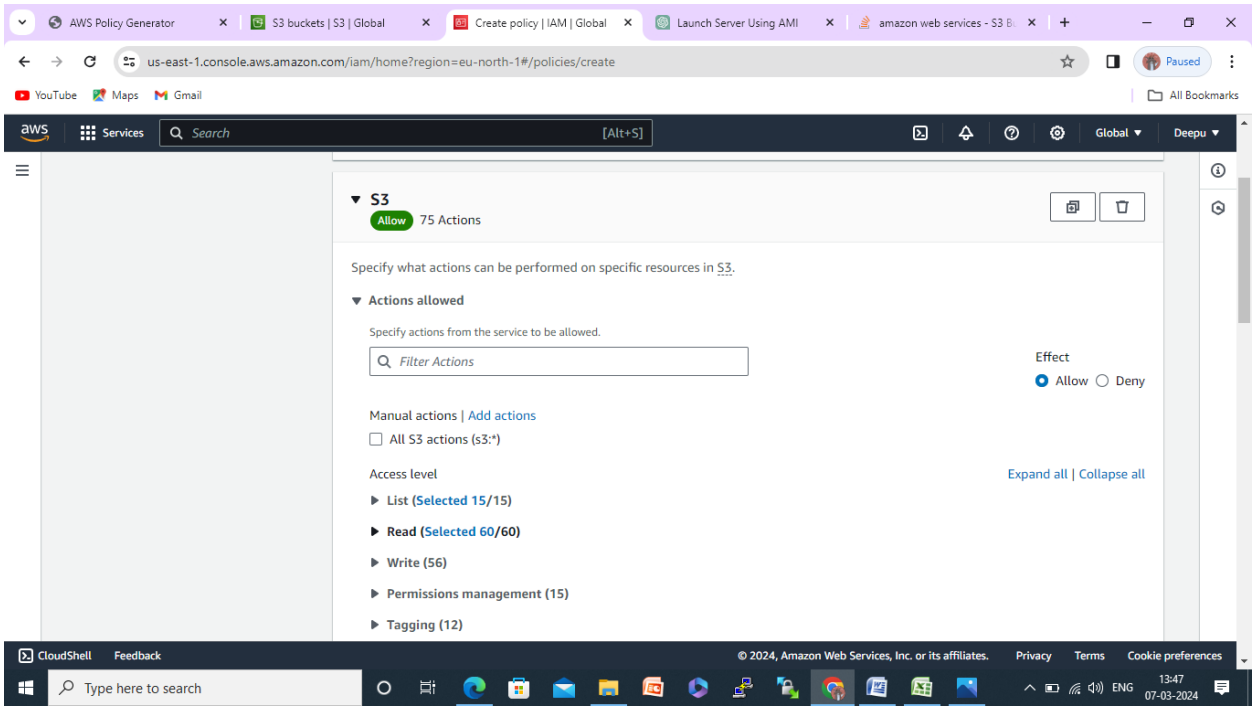
Creating only “ s3:ListBucket policy for that “demo-buc-1” bucket

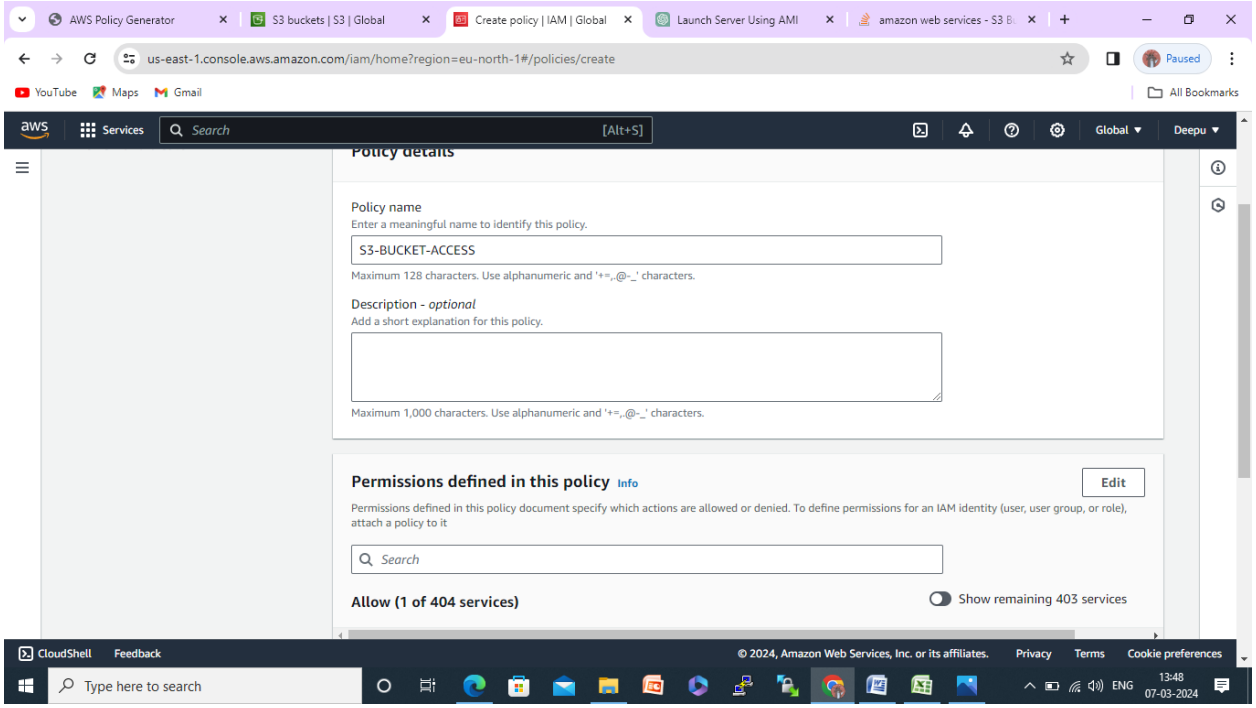


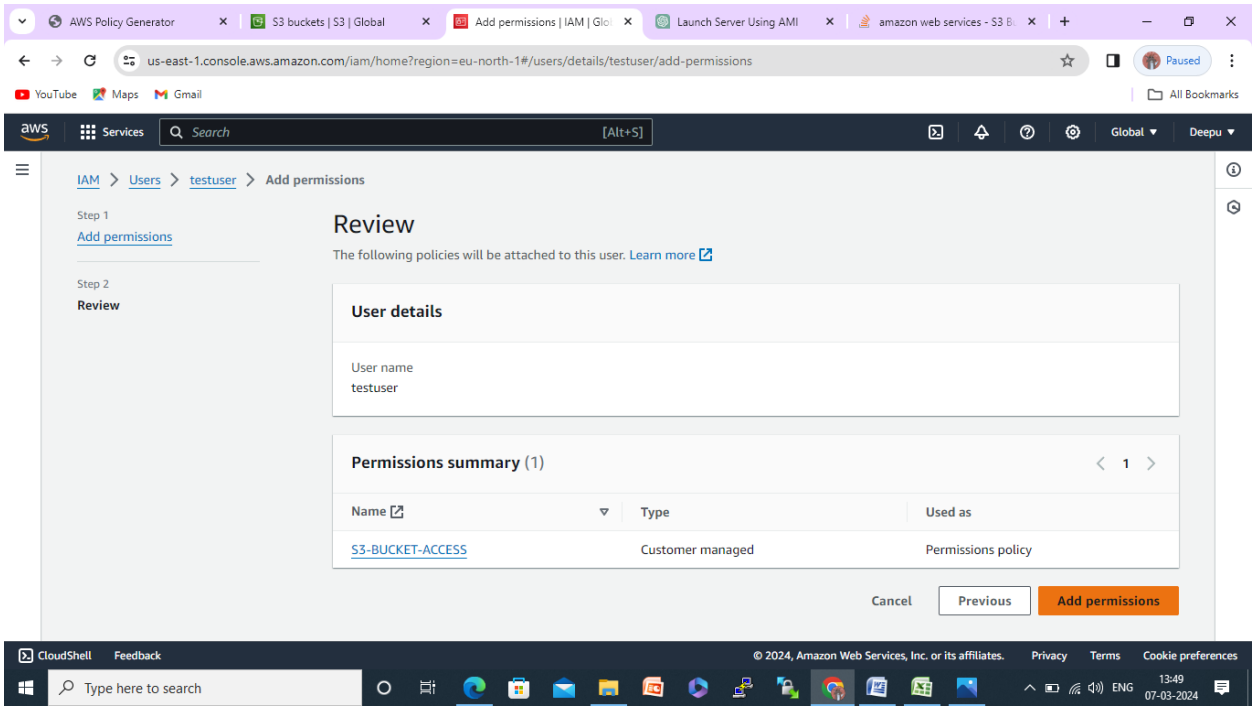


Creating a IAM custom policy for an “testuser” to have access only for list abd read.

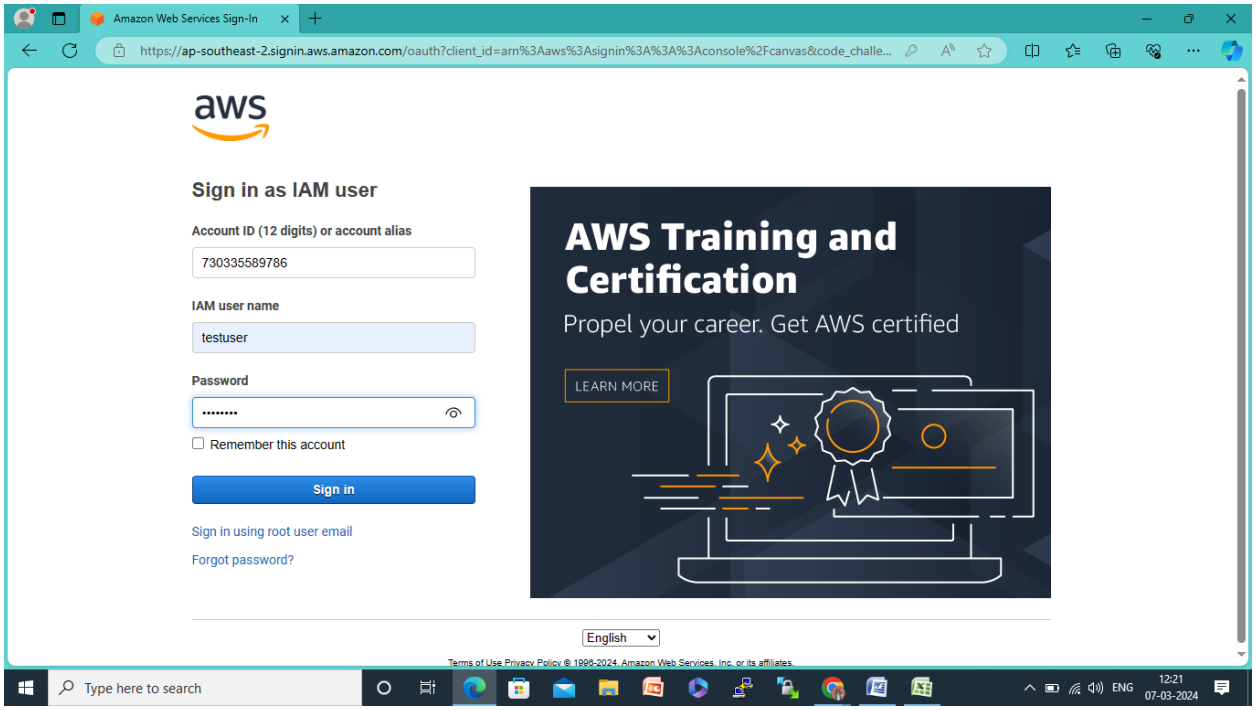




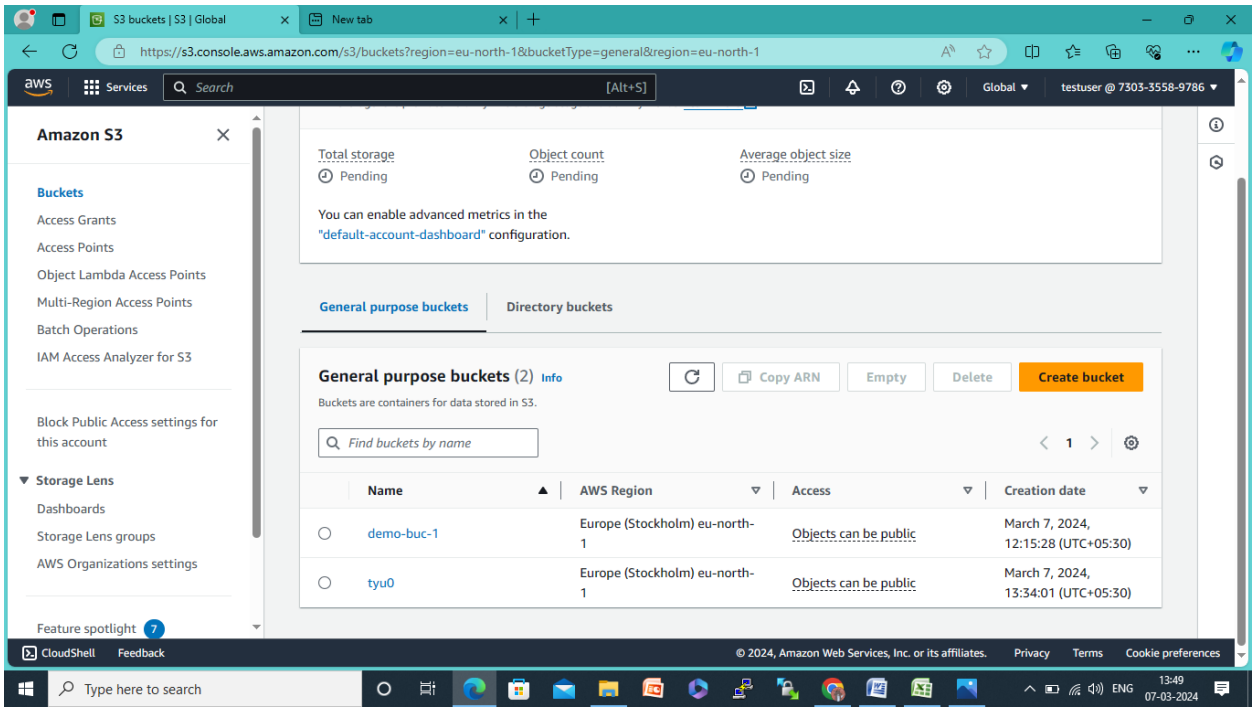

AWS Policy Generator
S3 buckets | S3 | Global
Create policy | IAM | Global
Launch Server Using AMI
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create
Policy details
Policy name
Enter a meaningful name to identify this policy.
S3-BUCKET-ACCESS
Maximum 128 characters. Use alphanumeric 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
Edit
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 404 services)
Show remaining 403 services
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
13:48
07-03-2024


AWS Policy Generator
S3 buckets | S3 | Global
Add permissions | IAM | Glo
Launch Server Using AMI
us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/testuser/add-permissions
IAM > Users > testuser > Add permissions
Step 1
Add permissions
Step 2
Review
Review
The following policies will be attached to this user. Learn more
User details
User name
testuser
Permissions summary (1)
Name
Type
Used as
S3-BUCKET-ACCESS
Customer managed
Permissions policy
Cancel
Previous
Add permissions
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
13:49
07-03-2024

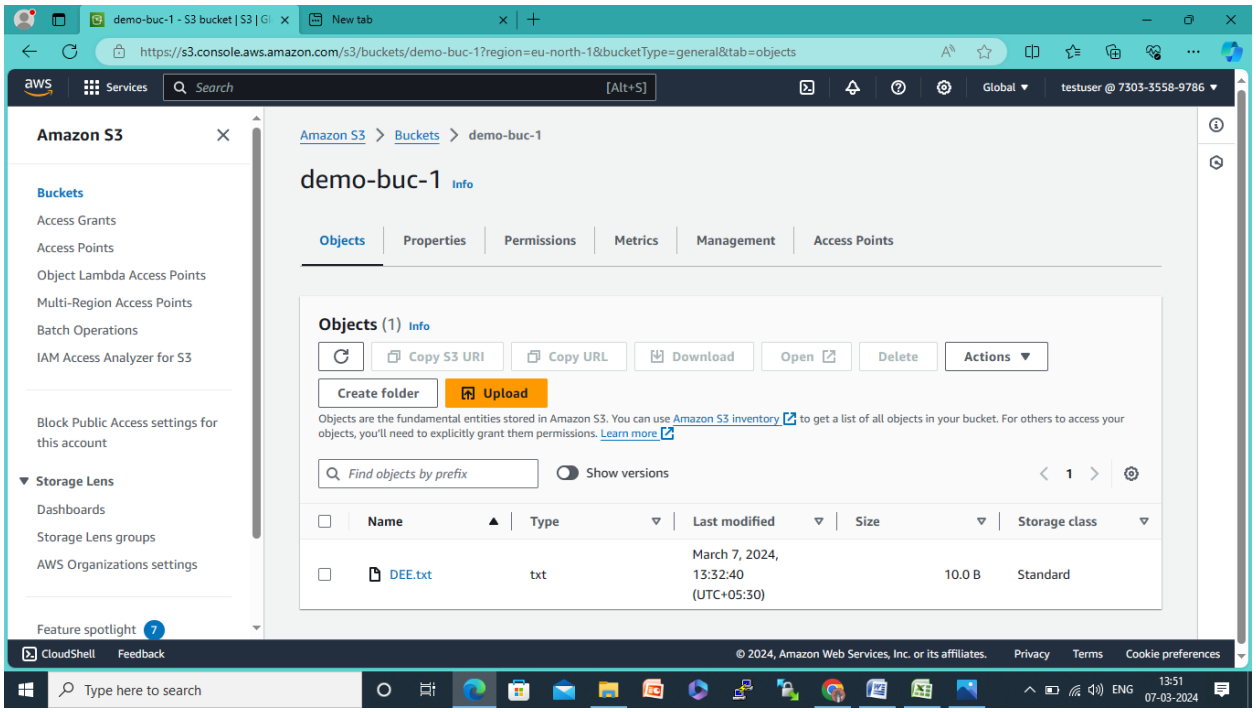
Sigining up to the “testuser” to check the access for list and read.



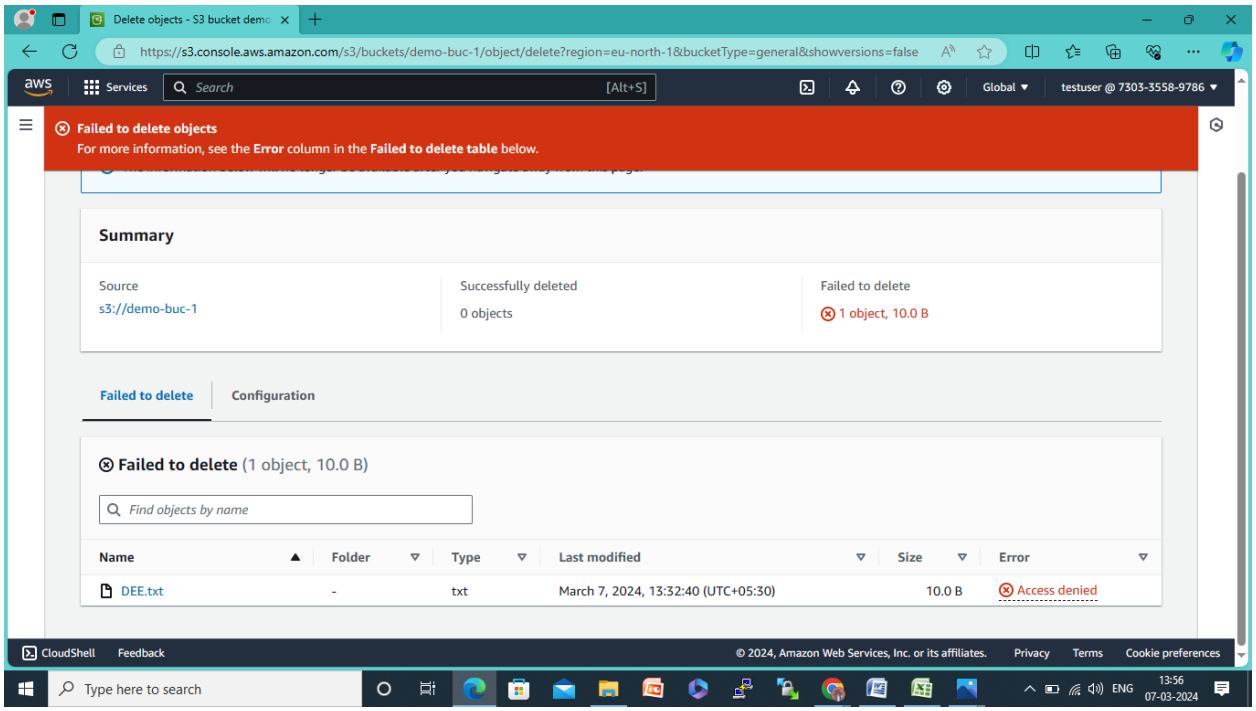
Also created a another bucket to check the bucket level access for that “testuser”.



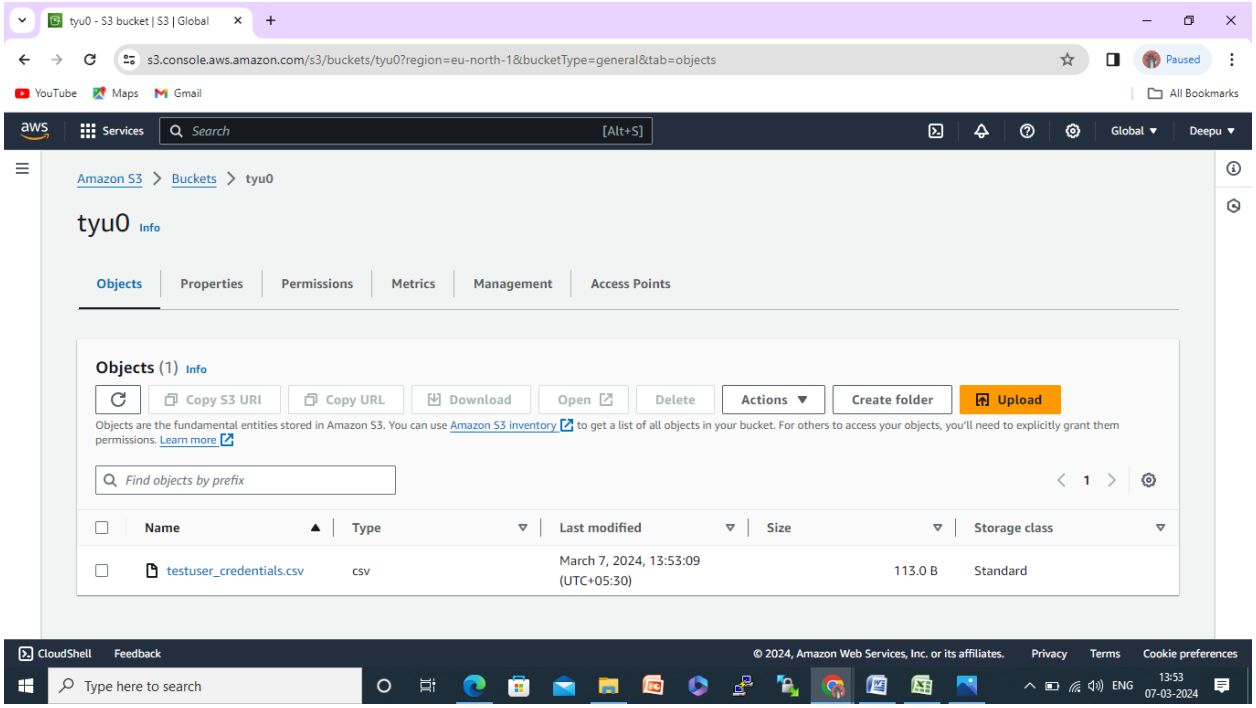
Can list and read by “testuser for that “demo-buc-1” bucket with that bucket policy for bucket level.



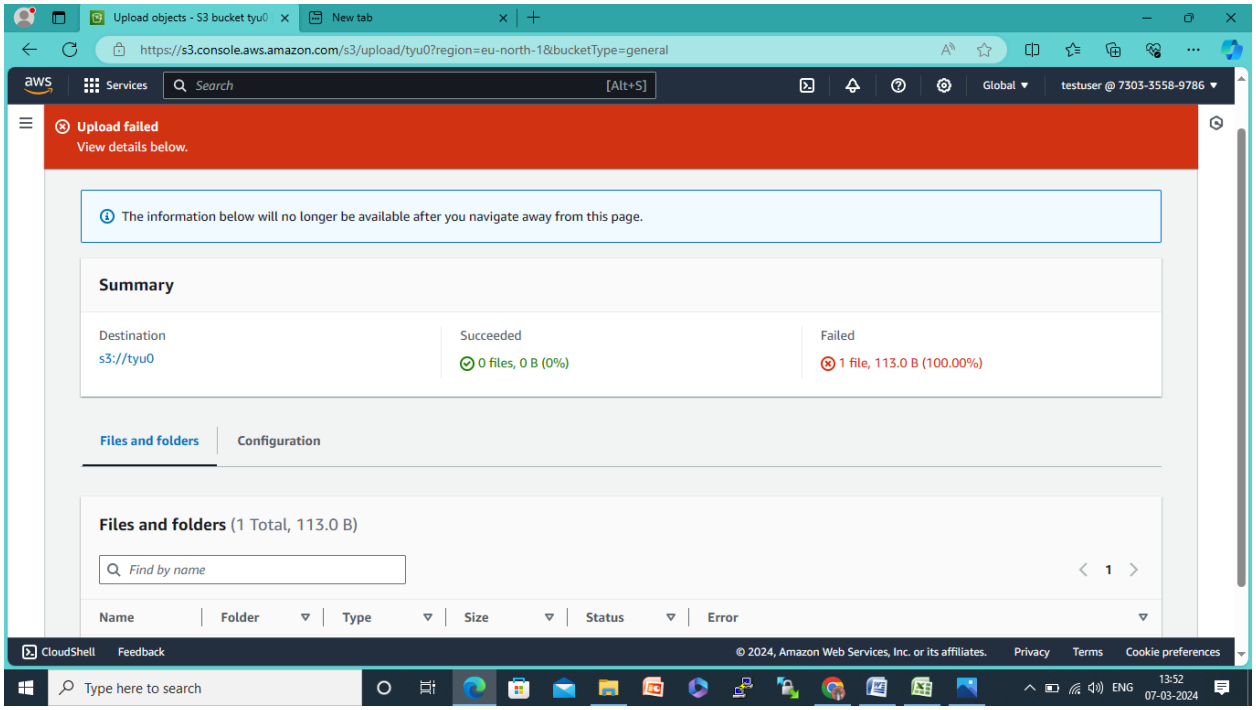
Failed to delete the object in that “demo-buc-1” bucket.



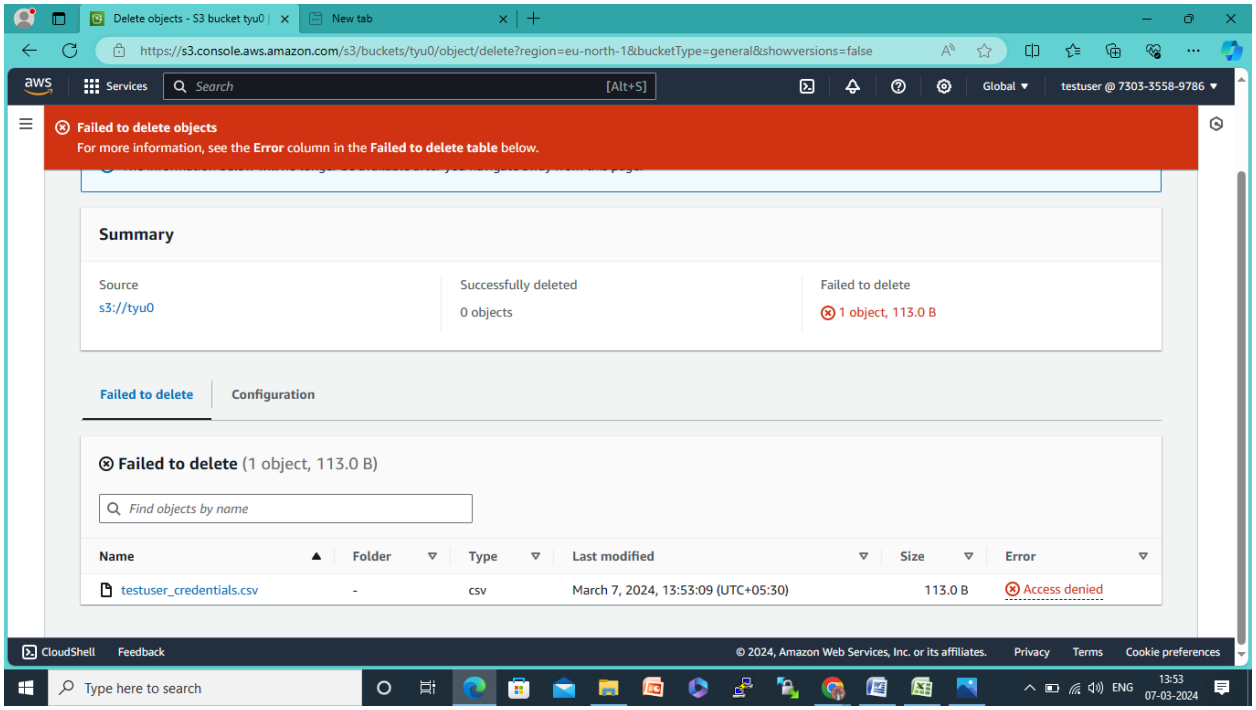
Checking the bucket level access for that “testuser” in another bucket ”tyu0”



Upload faild in another bucket for that “testuser”.



Also failed for deleting the object in that another bucket.



So, bucket policy is applied for a user to limit the access for an bucket level and also for access the objects privately for the user.