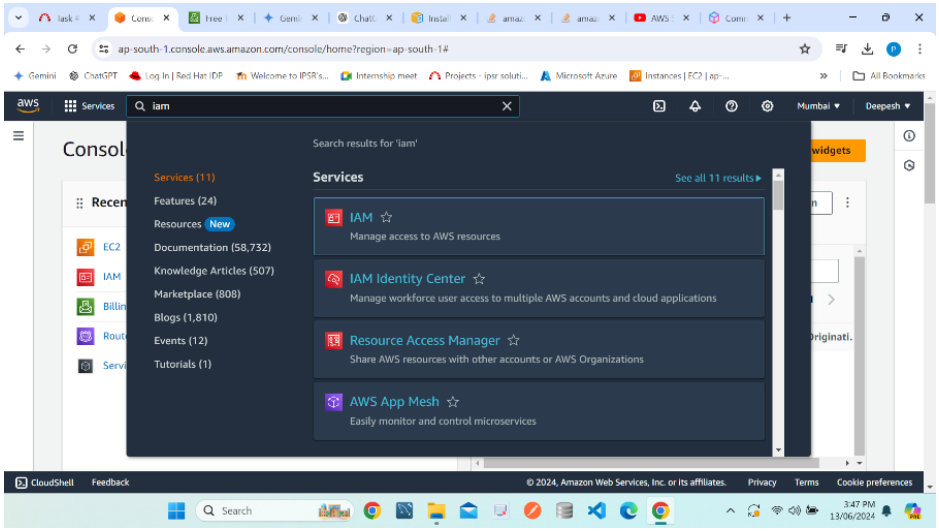
IAM User Creation

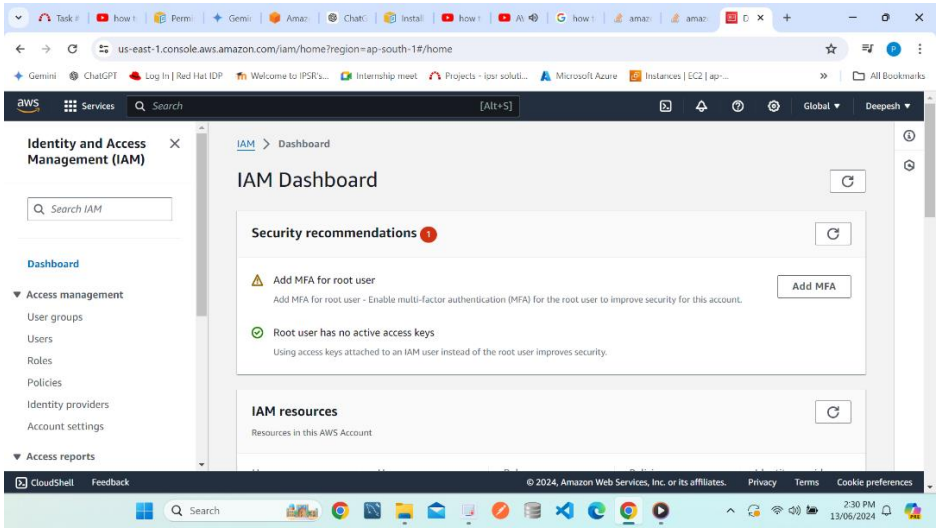
1. Create an IAM user from the root aws account
2. Set the policy or permission to the root user, so that it can only access aws-EC2 service
3. Login as the IAM user and verify the working of the policies attached with the user

   Note: Try the following
   - IAM user with AWS management console access
   - IAM user with programmatic access

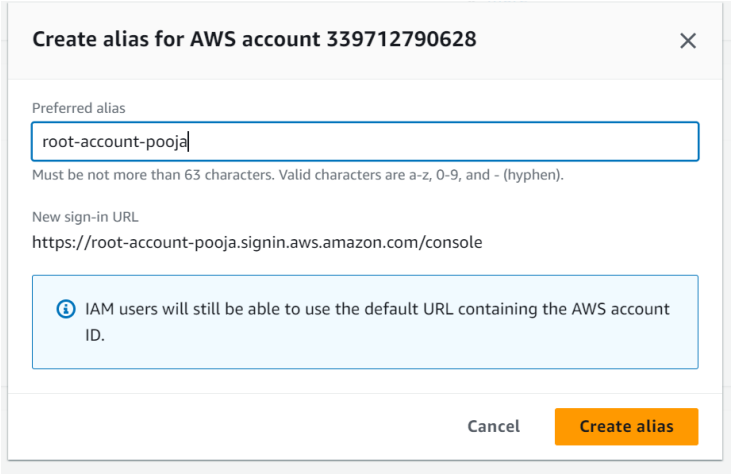
Steps for IAM user with AWS management console access

1. Sign in to the AWS Management Console:
2. Navigate to the IAM Console: Click on "Services" in the upper left corner, type "IAM" into the search bar, and select "IAM" from the options.



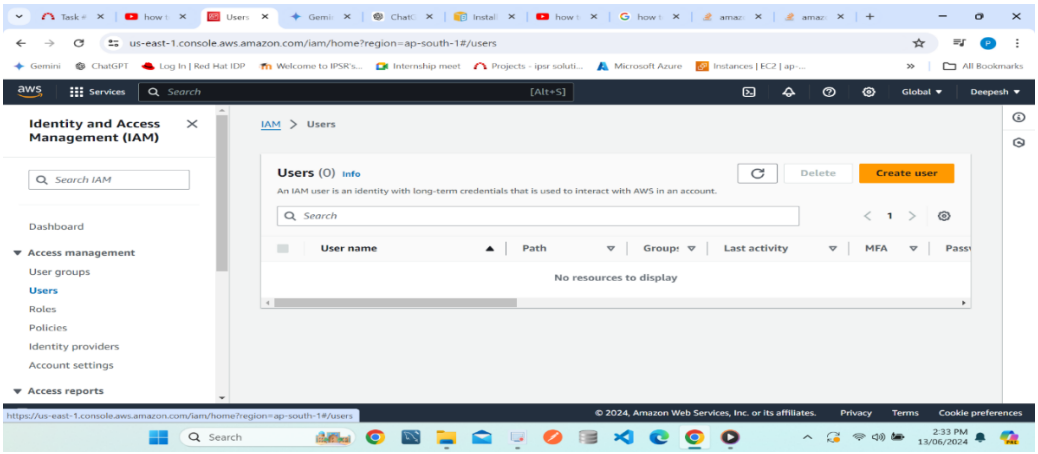


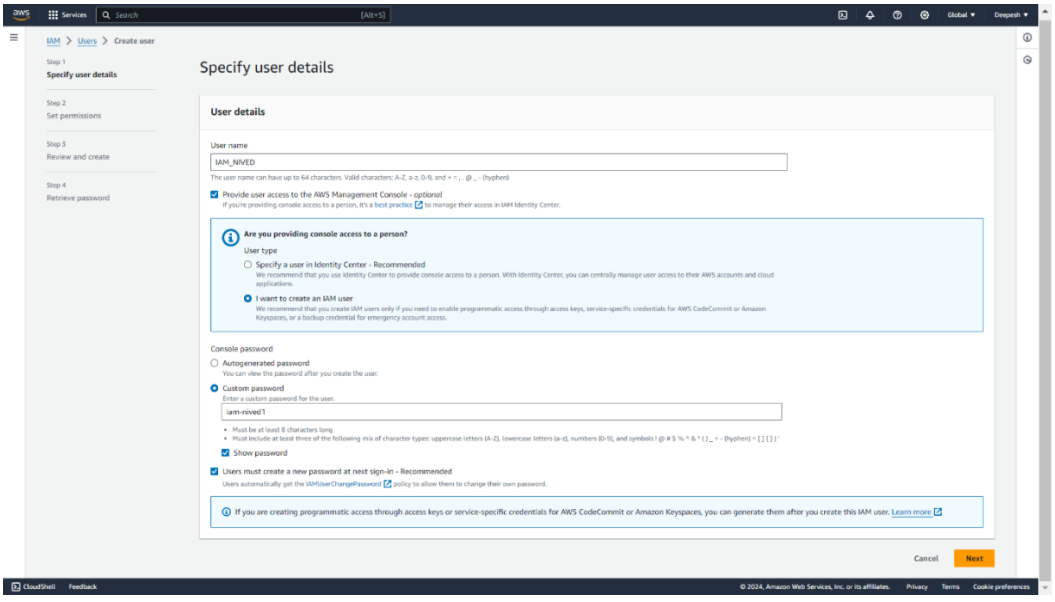
Mask the account number bt creating alias for AWS account



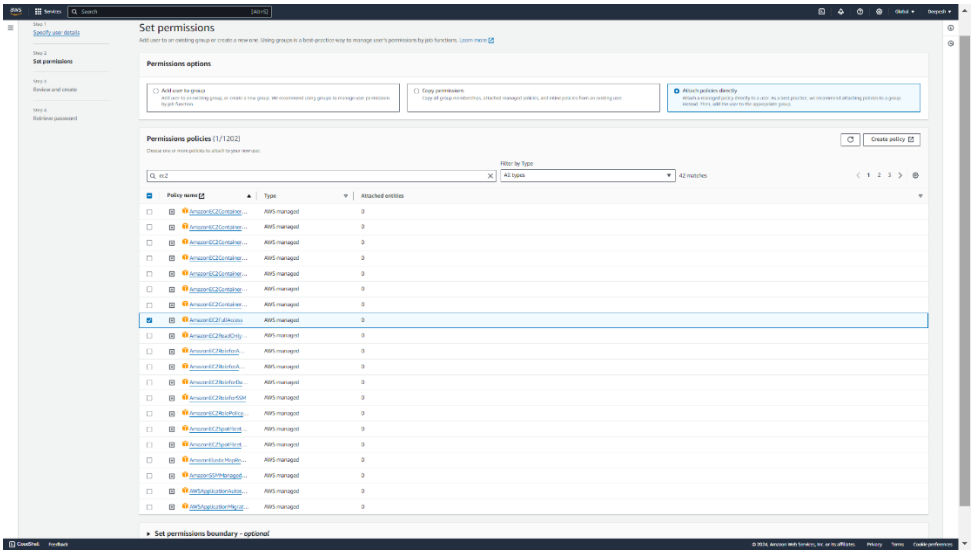
3. Create a New IAM User:

- In the IAM console, click on "Users" in the left-hand menu, and then click on "Add user".

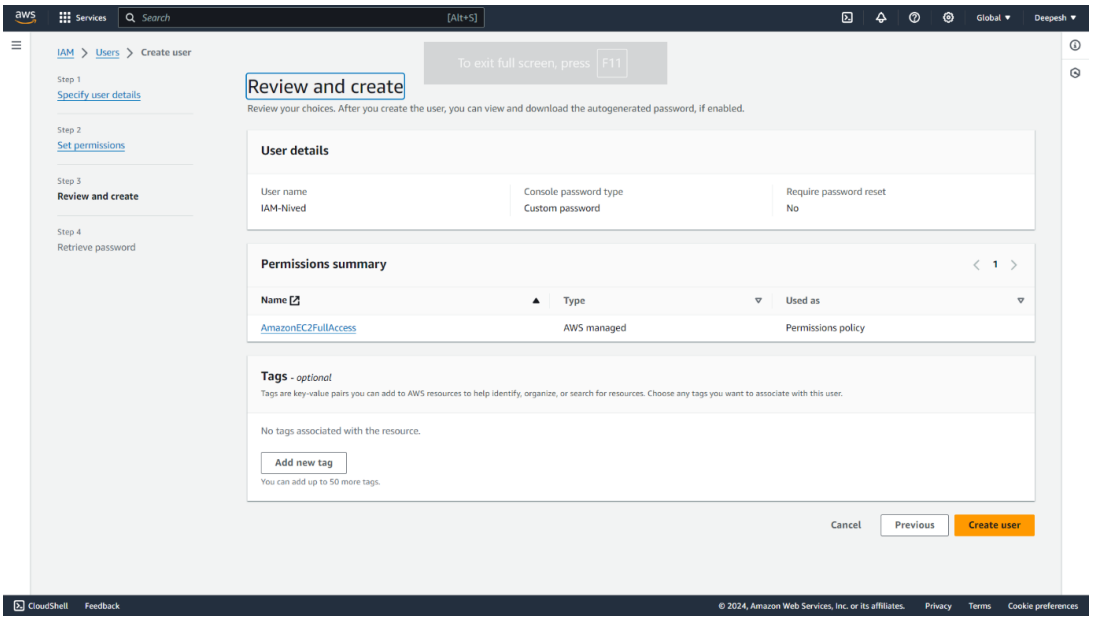




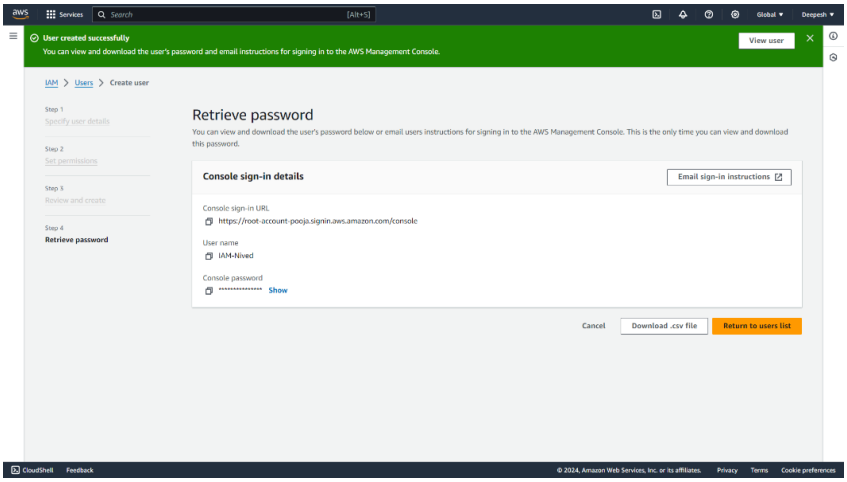
- Set User Details:
    - Enter a username for the new IAM user.
    - Choose the type of access as "AWS Management Console access".
    - Set Console Password: set a password or allow IAM to auto-generate one.
    - Set permission for that choose attach policies directly and select the permission policy needed or custom policy create. Here in this case choose AmazonEC2FullAccess

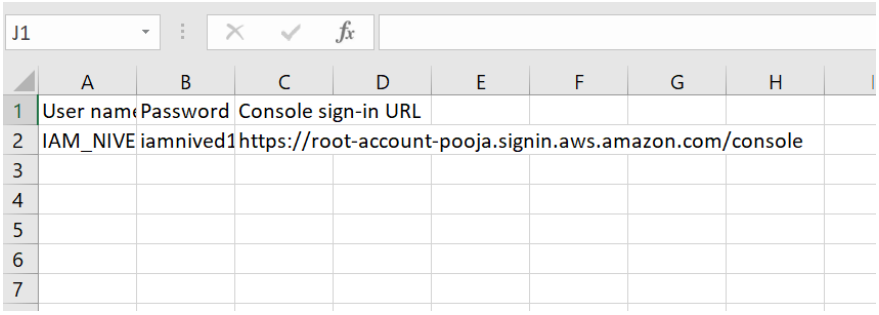


    - Review and create the user



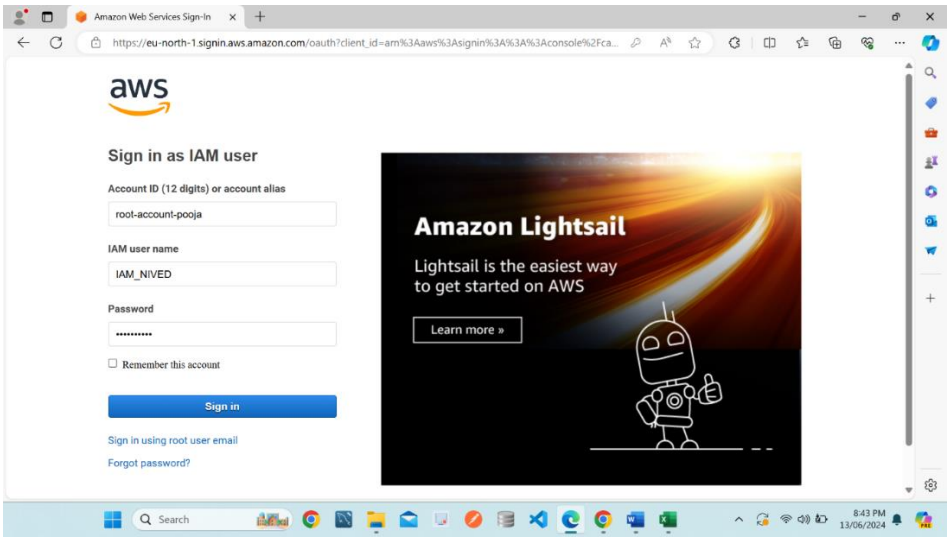
Then we can download the IAM user login credential



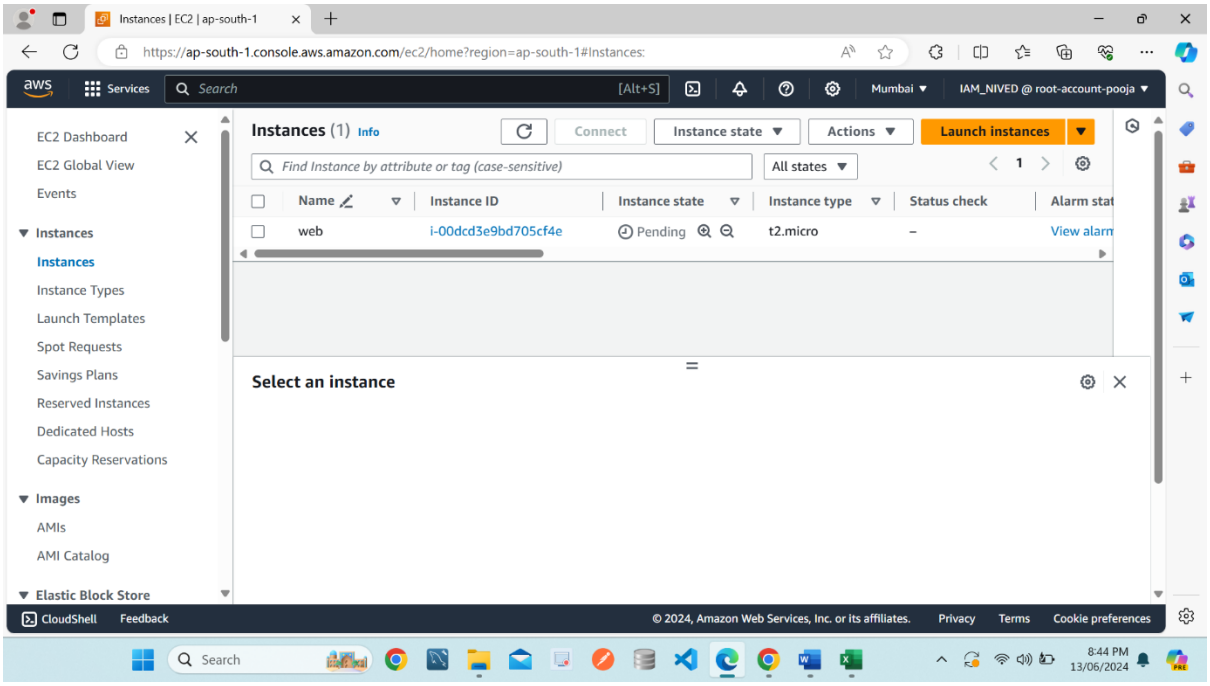


4. Verify Access:

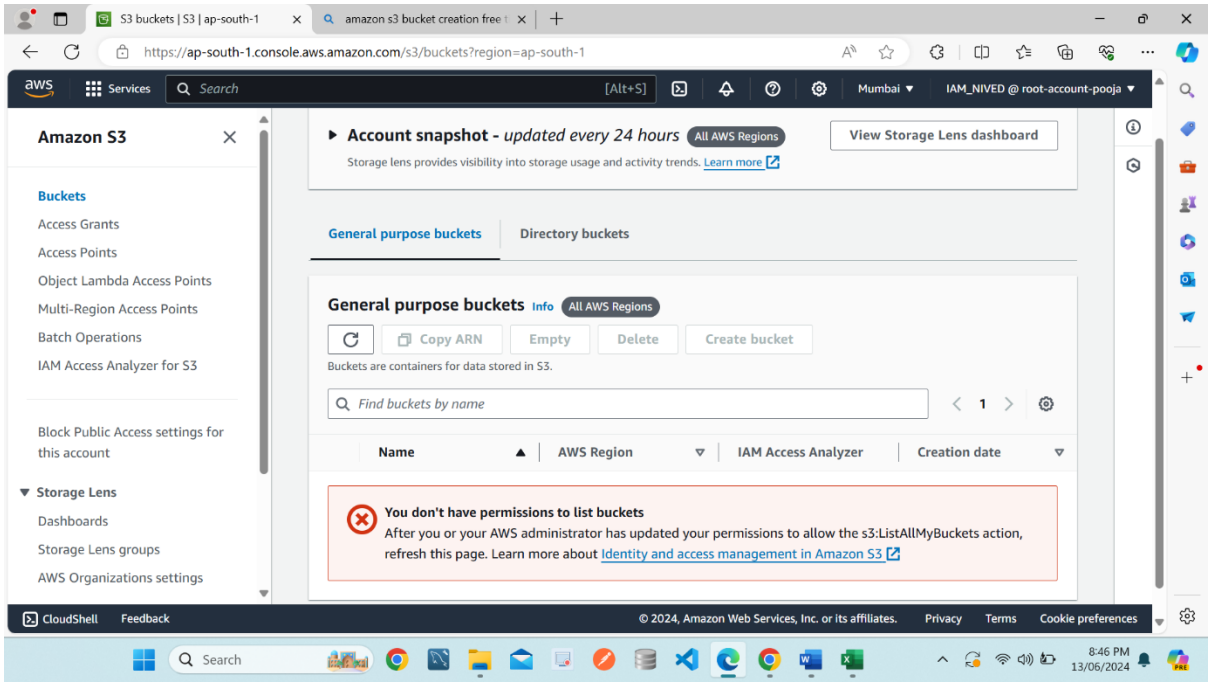
- We can access IAM User Sign-in page via consol sign in URL
- Sign in using the IAM user credentials we downloaded
- Navigate to the EC2 Dashboard or try to perform EC2-related actions to verify access. Ensure you can only interact with EC2 resources as per the permissions set in the policy.



EC2 Access Success

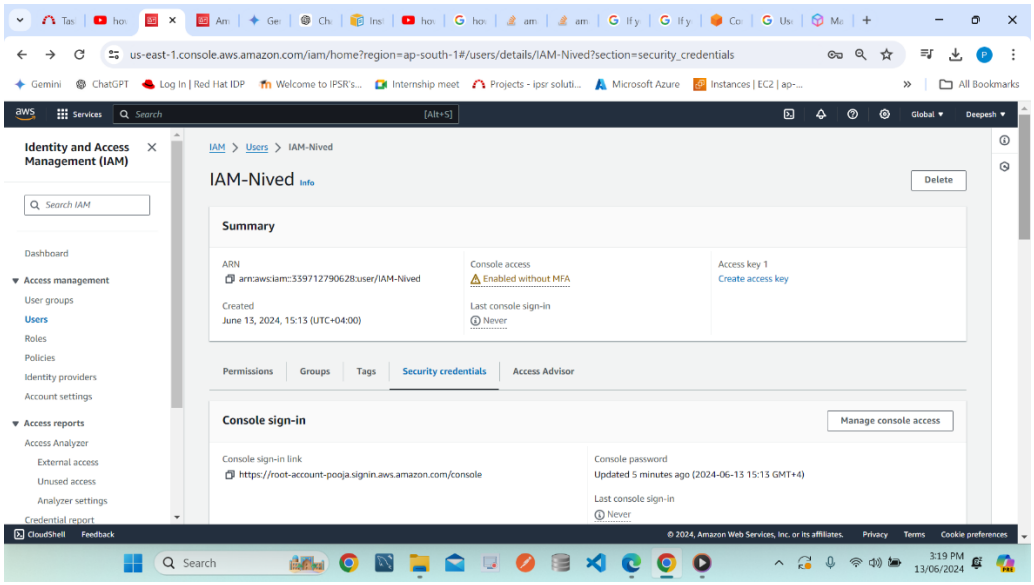


S3 Service Denied

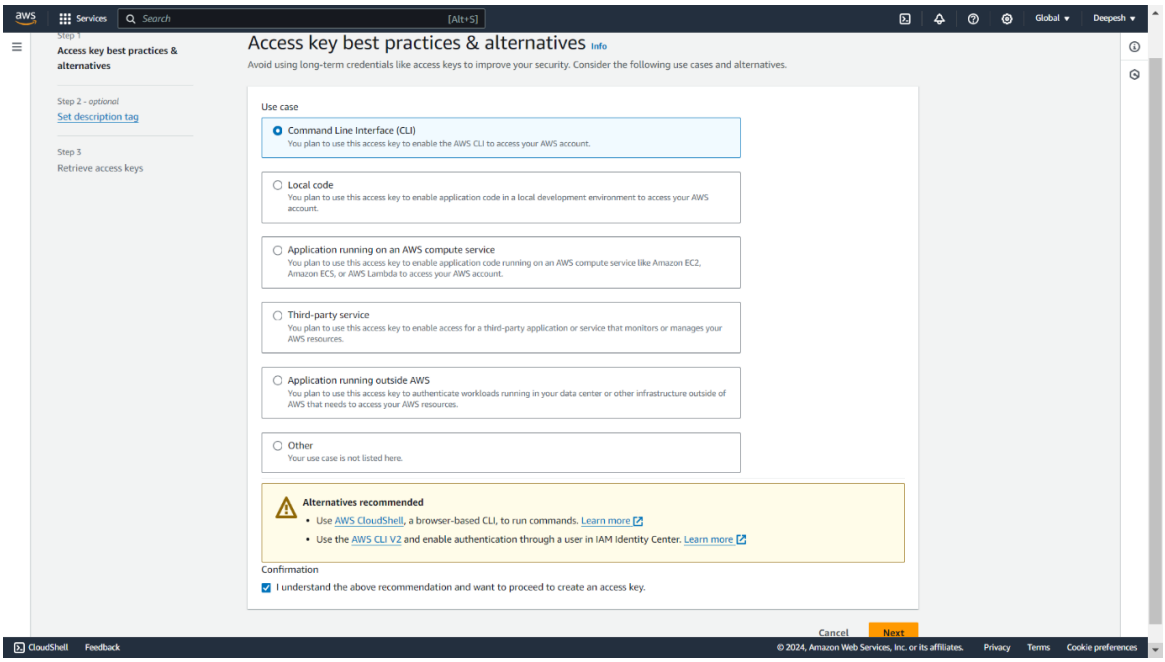


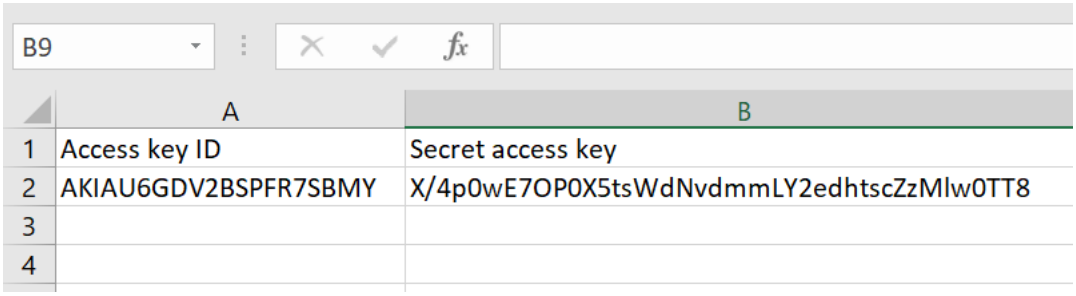
Steps for IAM user with programmatic access

1. Follow the step 1 to 3 same as above until review and create user
2. Select the user we needed and click to create the access key via following step

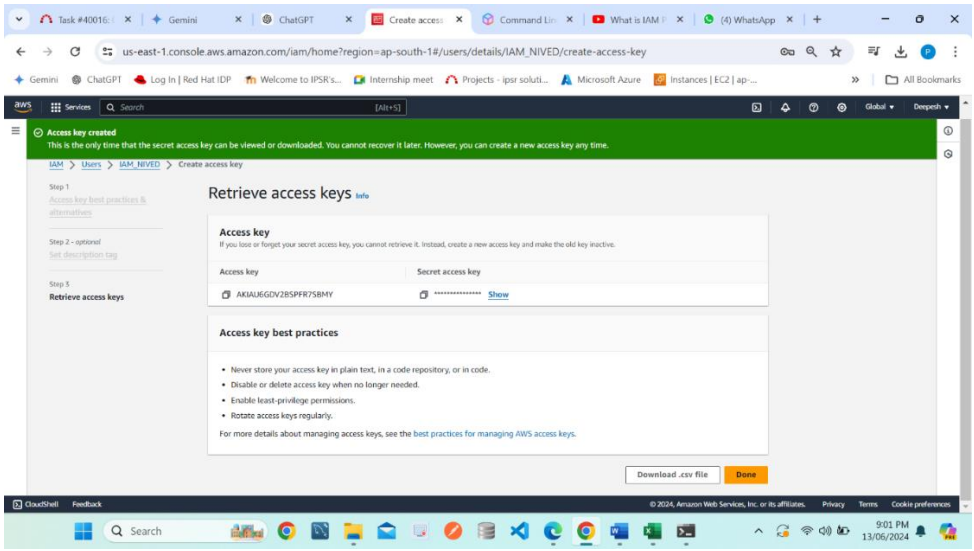


3. Choose command line interface and we can generate a access key and Secret access key and also download it for further use





	A	B
1	Access key ID	Secret access key
2	AKIAU6GDV2BSPFR7SBMY	X/4p0wE7OP0X5tsWdNvdmmLY2edhtscZzMlw0TT8
3		
4		



4. Verify Permissions Using the CLI

- Download the AWS CLI Installer:
  - Go to the AWS CLI installation page: AWS CLI Installer for Windows.
  - Click on the link to download the Windows installer.
  - Run the Installer:
  - Locate the downloaded .msi file and double-click it to run the installer.
  - Follow the on-screen instructions to complete the installation.
- Verify the Installation
  - Check the AWS CLI Version: Type the following command to verify the installation on windows command prompt. The path must be AWS CLI installed location.

```
C:\Program Files\Amazon\AWSCLIV2>
C:\Program Files\Amazon\AWSCLIV2>aws --version
aws-cli/2.16.7 Python/3.11.8 Windows/10 exe/AMD64
```

- Configure AWS CLI with IAM User Credentials:
  - Open a Command Prompt window and type the following command to start the configuration process

    # aws configure

Enter the Access Key ID, Secret Access Key, default region, and default output format when prompted. The Access Key ID and Secret Access Key are obtained from the .csv file or noted down during the creation of the IAM user.

```
C:\Program Files\Amazon\AWSCLIV2>aws configure
AWS Access Key ID [None]: AKIAU6GDV2BSPFR7SBMY
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: table
```

5. Verify EC2 Access

   List EC2 Instances:In the Command Prompt window, type

   # aws ec2 describe-instances

```
C:\Program Files\Amazon\AWSCLIV2>aws ec2 describe-instances
-------------------------------------------------------------------------
|                           DescribeInstances                           |
+-----------------------------------------------------------------------+
||                            Reservations                             ||
|+----------------------------+----------------------------------------+|
||  OwnerId                   |  339712790628                          ||
||  ReservationId             |  r-0bc1585ece5b56c63                   ||
|+----------------------------+----------------------------------------+|
|||                             Instances                             |||
||+---------------------------+---------------------------------------+||
|||  AmiLaunchIndex           |  0                                    |||
|||  Architecture             |  x86_64                               |||
|||  BootMode                 |  uefi-preferred                       |||
|||  ClientToken              |  effc60d0-bfcd-43cf-a96b-573d05d51386 |||
|||  CurrentInstanceBootMode  |  legacy-bios                          |||
|||  EbsOptimized             |  False                                |||
|||  EnaSupport               |  True                                 |||
       |||
       |||
[33m||
```

   This command should return information about your EC2 instances, confirming that the IAM user has the correct permissions.

Test Restricted Access:

Attempt to access a service that the IAM user does not have permission to use, such as S3

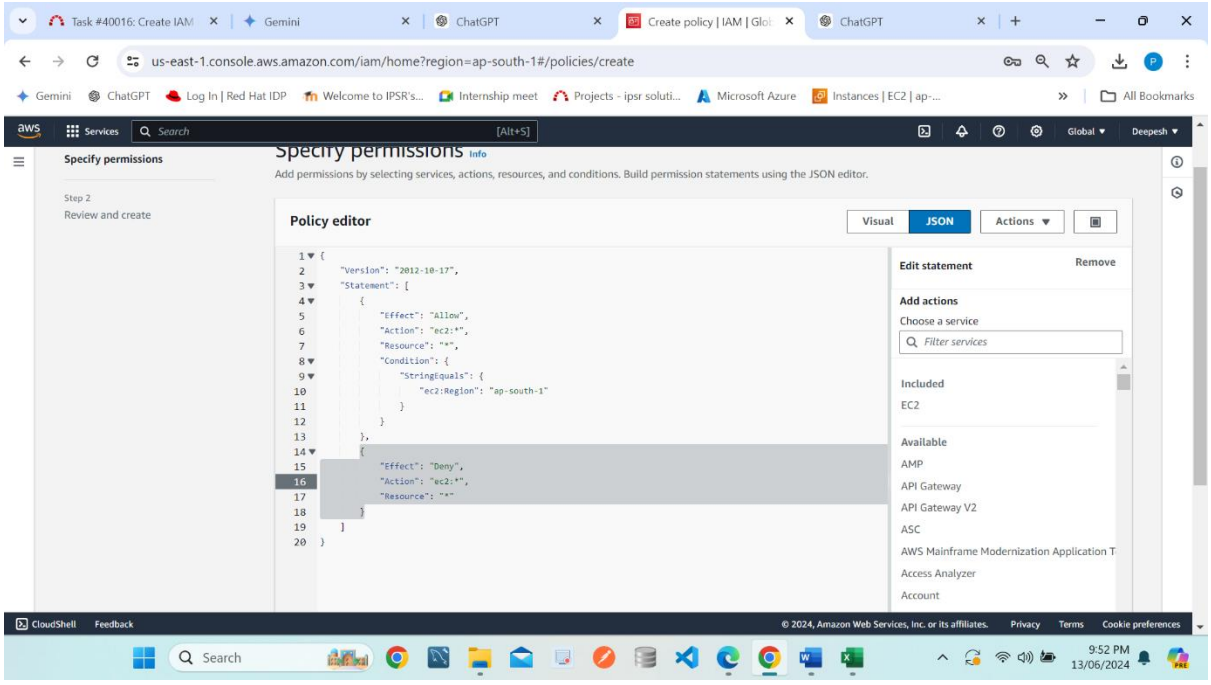
aws s3 ls

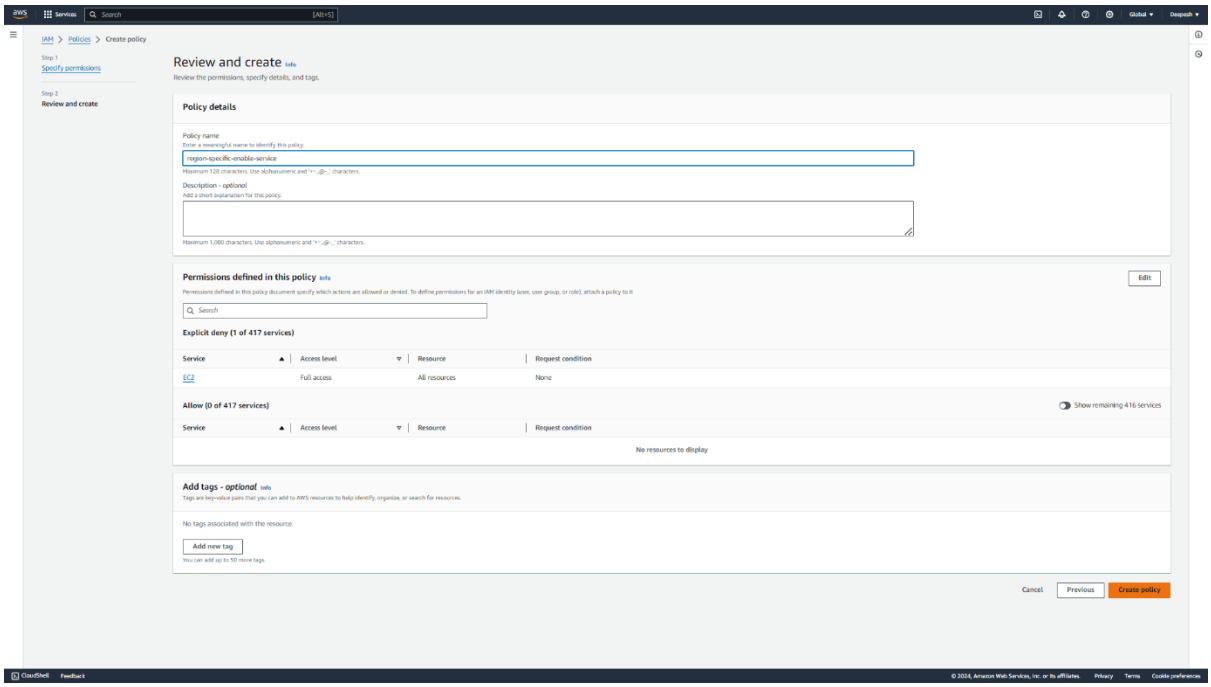
This should return an error indicating that access is denied, confirming that the IAM policy restricts access to only EC2.

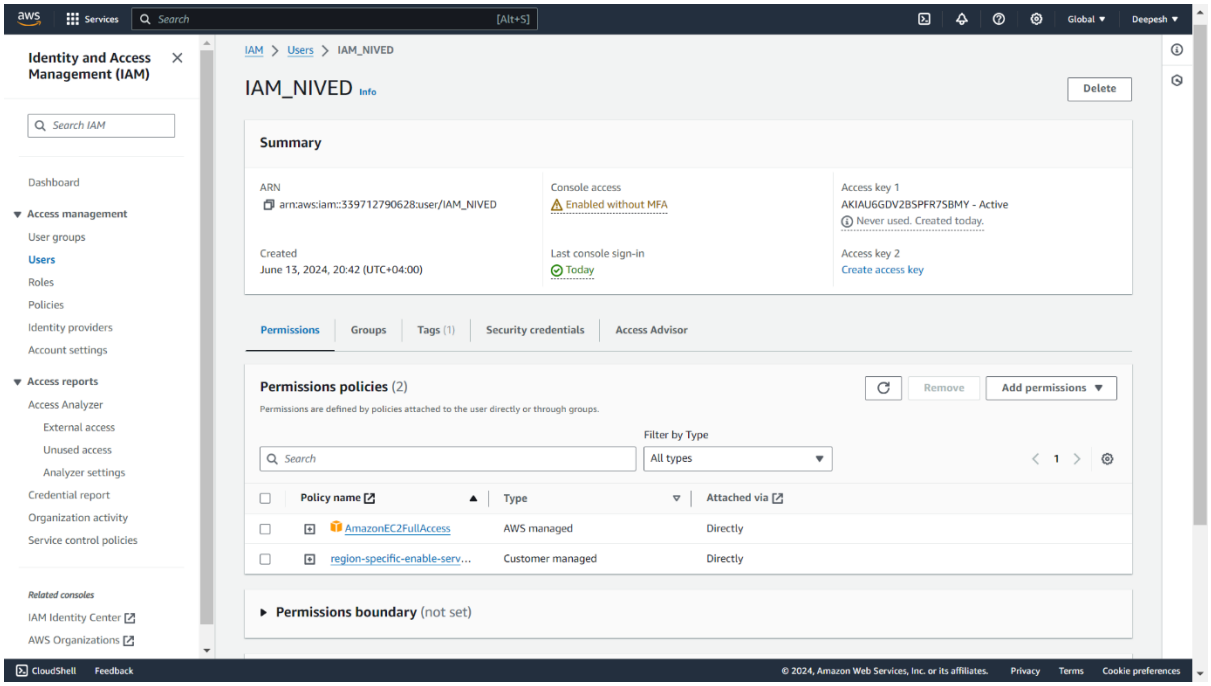
```
C:\Program Files\Amazon\AWSCLIV2>aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets operation: Access Denied
```

Region enable IAM User Access. (EC2 Service access only at the region where root created and also denied all other services.)

Follow the step 1 to 3 untill user creation and also create policy for region specific access, review and create the permission then attach it to the user

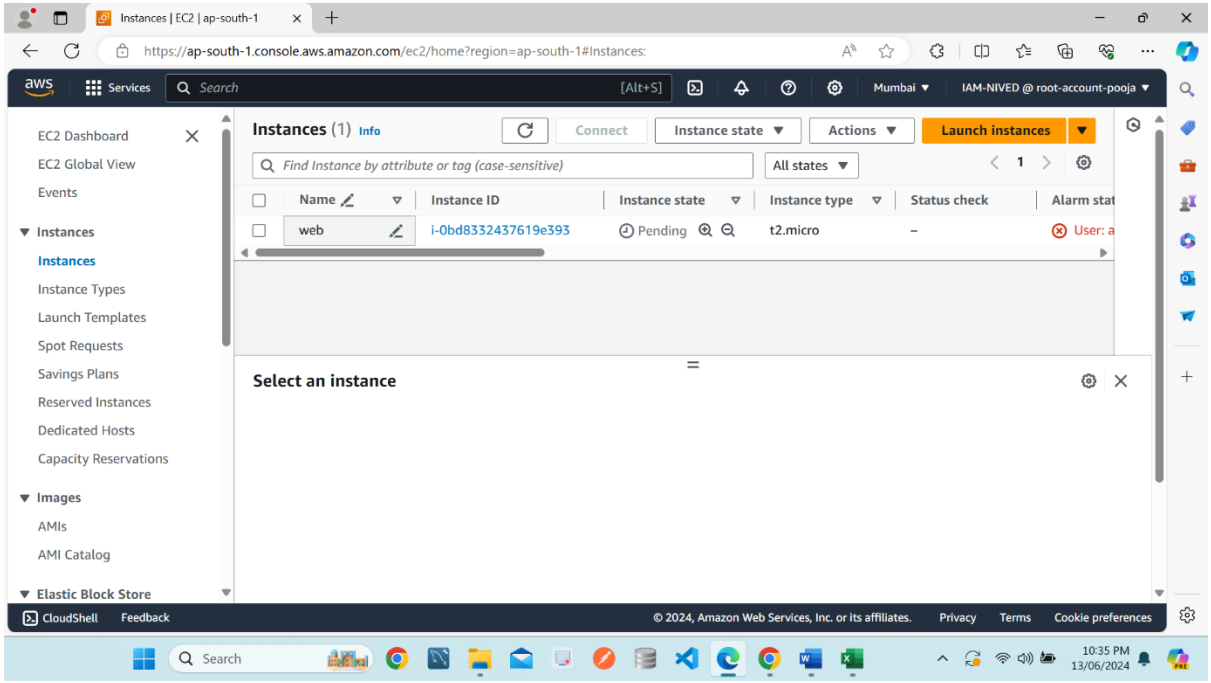




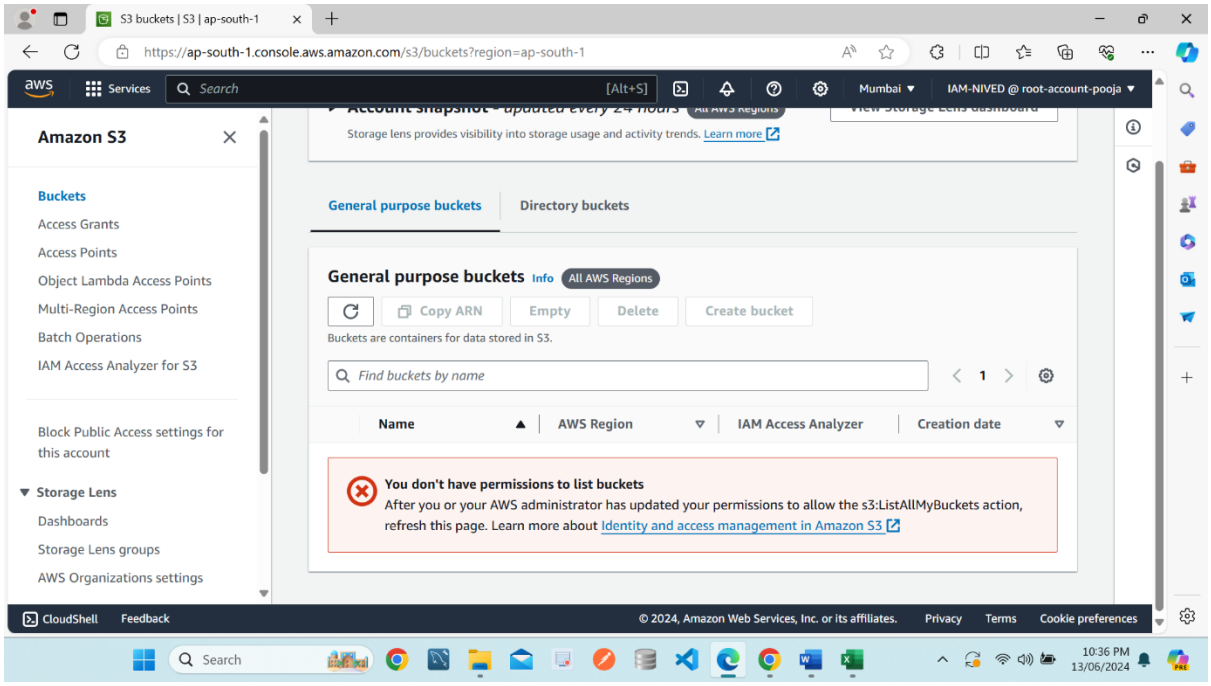


Verify the output

EC2 service Success for the region Mumbai



S3 service denied for the region Mumbai



EC2 service denied for the region Osaka