Om Shete
THADOMAL SHAHANI TSEC ENGINEERING COLLEGE
TE C32
2103163

Experiment No: 7

Aim: To study and implement Identity and access management (IAM) practices on AWS

Theory:

1. Explain the concept and need of access management

⇒ Access management (AM) is process of identifying and controlling and managing authorized or specified user access to a system, application or only IT instances.

- It is a board concept that encompases all policies, methodologies and tools to maintain access privilage.
- AM is primarily an information security, IT and data governance process used in gamming acceisses to valid users of prohibiting involved users.
- Typically AM is used in conjuction with identity access management IAM.
- Identify management creates, provision and controls the different users, roles and groups and policies whereas AM ensures that these roles and policies are allowed
- An AM based application states the different user roles and their policies.

• Explain IAM and its components

⇒ IAM is an identity and access management is the security discipline that enables the right individuals to access the right resources at the right reasons.

- These resources could be tools required to complete a job, access a database with mission critical data, on services and application hosted in cloud, etc.

- Components

It can be categorized into four components:-

1) Authentication
2) Authorisation
3) User Management
4) Central User Repository

• Compare the following in AWS

⇒

1) Root User and AWS IAM user

⇒ Root user is the first cloud service identity created by default when you create your cloud service provider account.

- It is important to note all cloud services providers have some form of root elements.
- AWS IAM users can be created by a root user or another IAM user who has entitlements on create additional IAM user.

- Can authenticate on start a remote session using their credentials on alias.
- Can corresponds to human, application process on another machine based identity.

2) Roles and Policies

⇒

Roles	Policies
i) Intended for guaranting temporary access for entities like application of service.	i) Defines permission and can be attached to user groups or roles.
ii) AWS resources on services.	ii) Attached to the IAM users, groups.
iii) Temporary access.	iii) Permanent permission.
iv) Defines who can assume the role.	iv) Trust relationship is not applicable as they do not involve.
v) Provides a way to grant precise permissions to a specific entity.	v) Defines a set of permissions that can be attached to multiple entities.

- Explain Inline and custom policies in AWS

⇒ An online policy is a policy created for a single IAM identity.

- Inline policies maintain a strict one to one relationship between a policy and identity either you can create a policy and embed it in an identity.
- An AWS managed policy is a standalone policy that is created and administration by AWS.
- Standalone policy that the policy has its own ARN that includes the policy name.
- You can create standalone policy in your own AWS account that you can attach to principal entities.

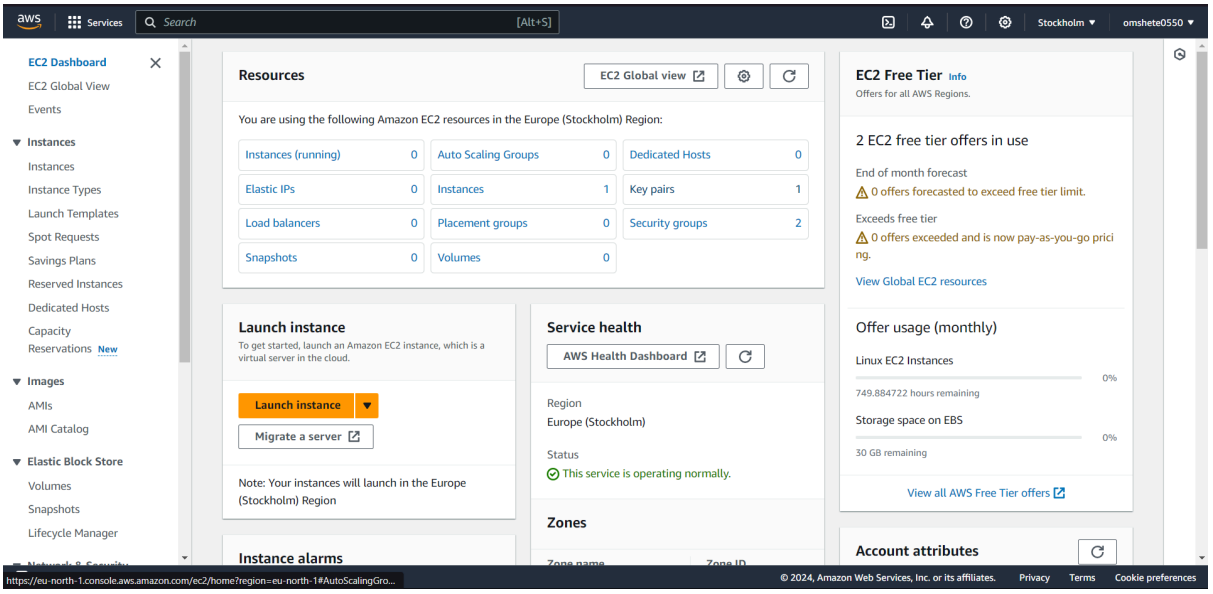
- Explain Multifactor Authentication in AWS

⇒ It is an AWS entity identity and Access Management best practice that requires a second authentication factor in addition.

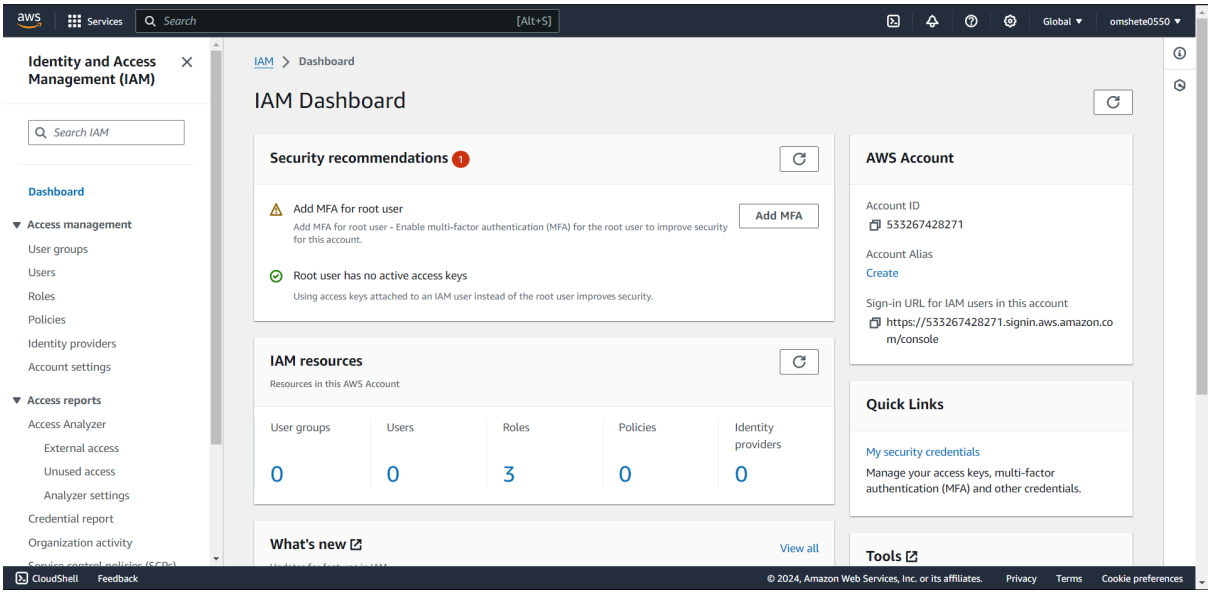
(A) 15/3/2024

Output:

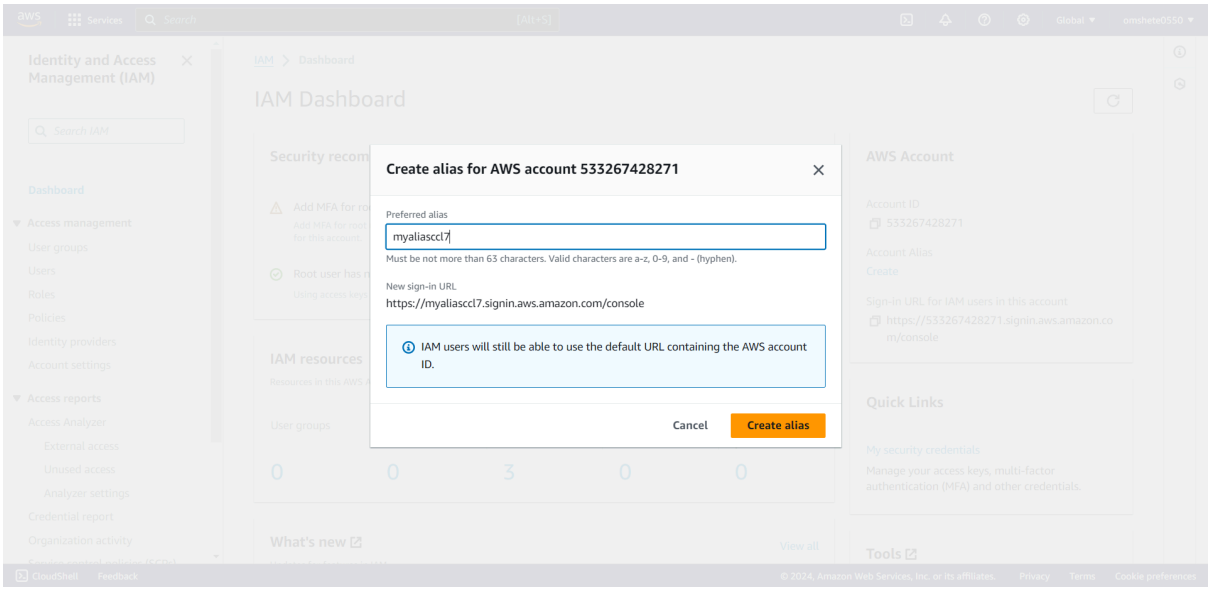
1. Login to AWS console Make sure to check all Ec2 dashboard parameters

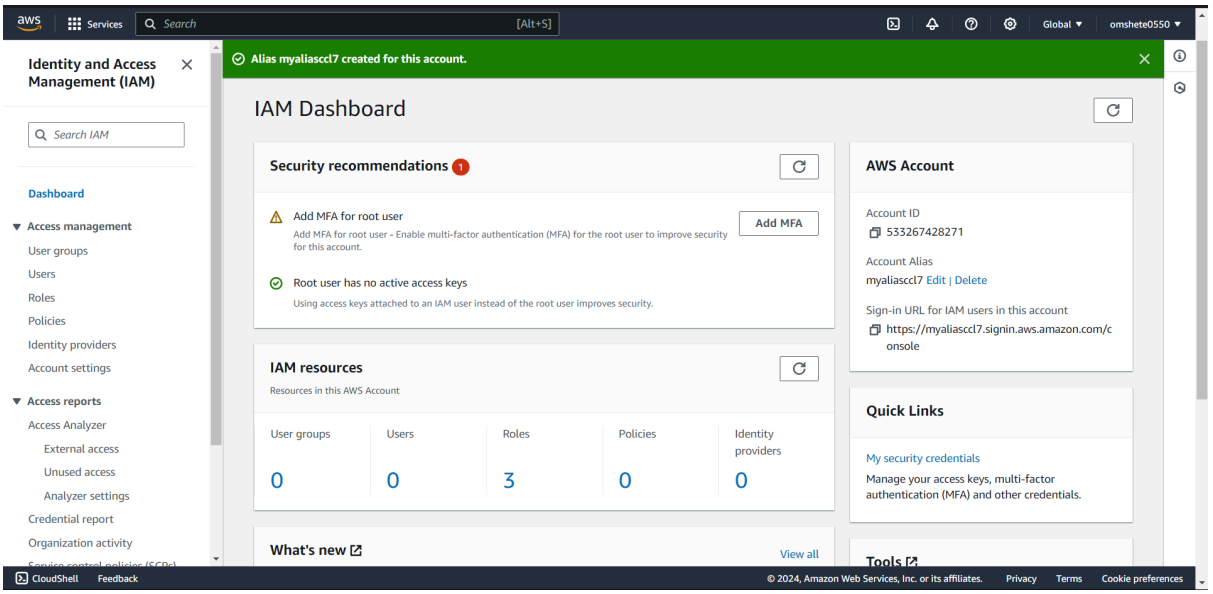


2. Go to IAM dashboard

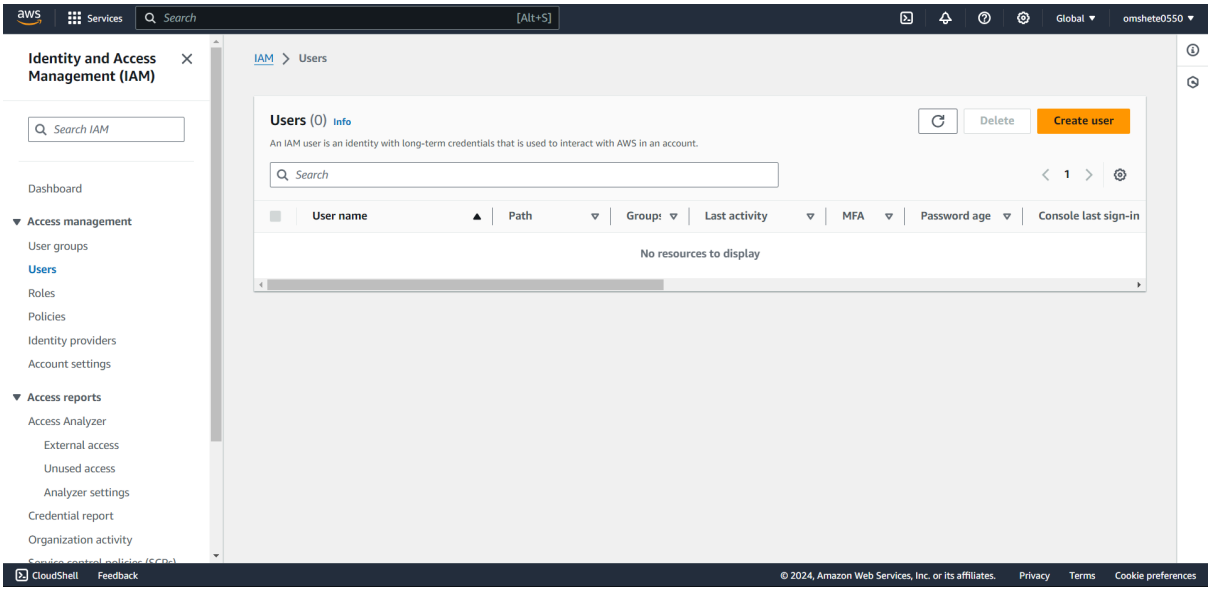


3. Click on create option under Account Alias and give a valid name; save changes

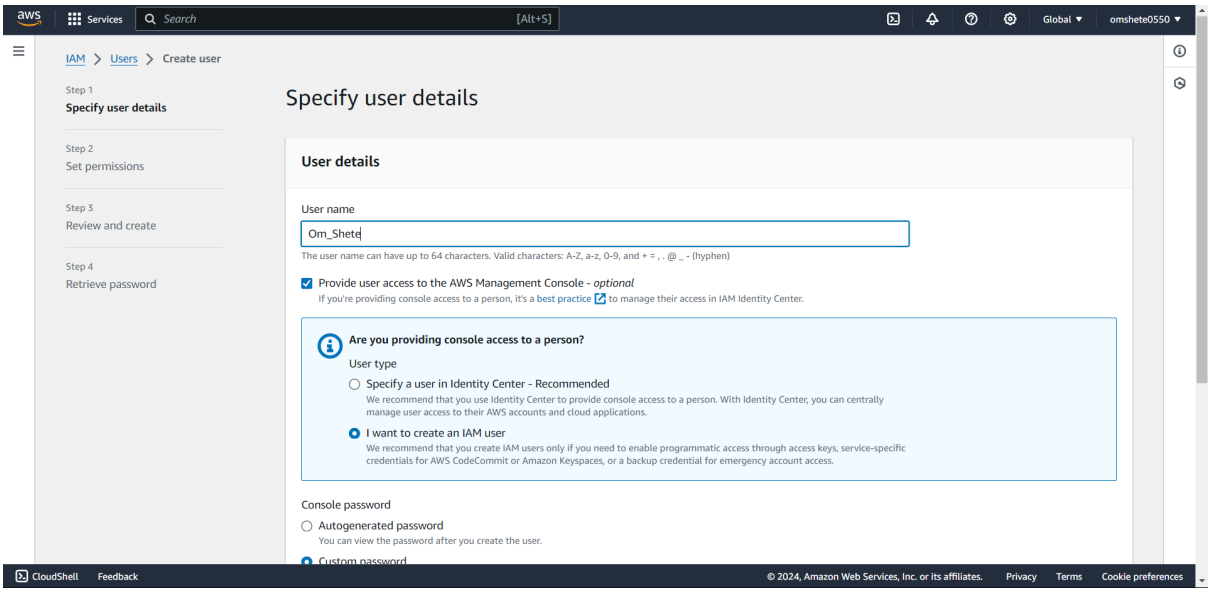


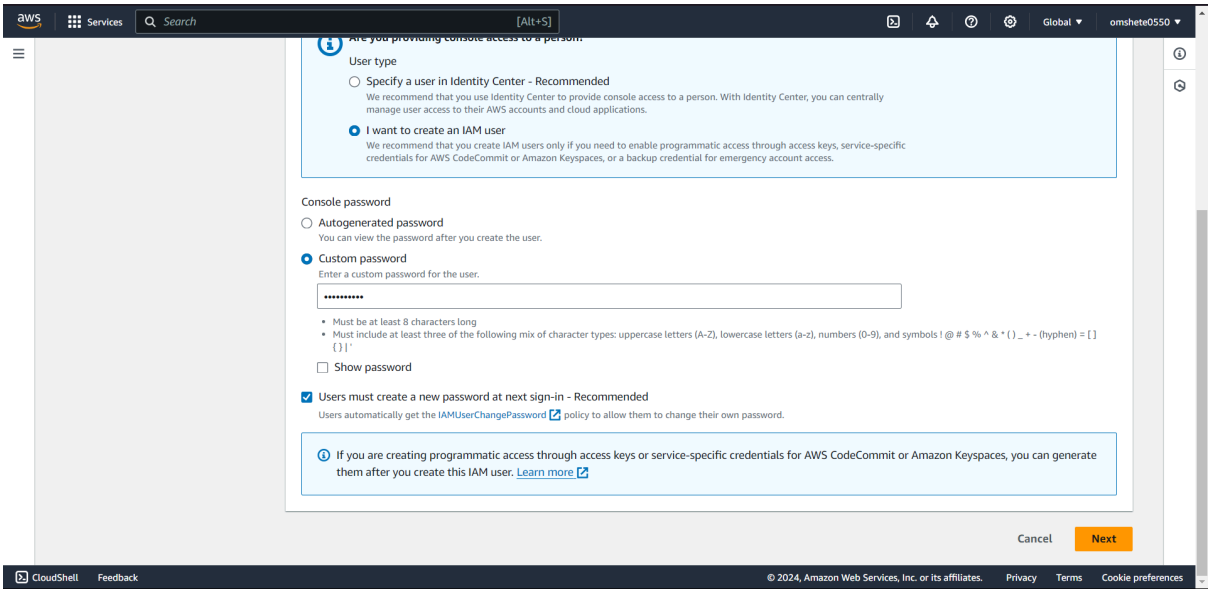


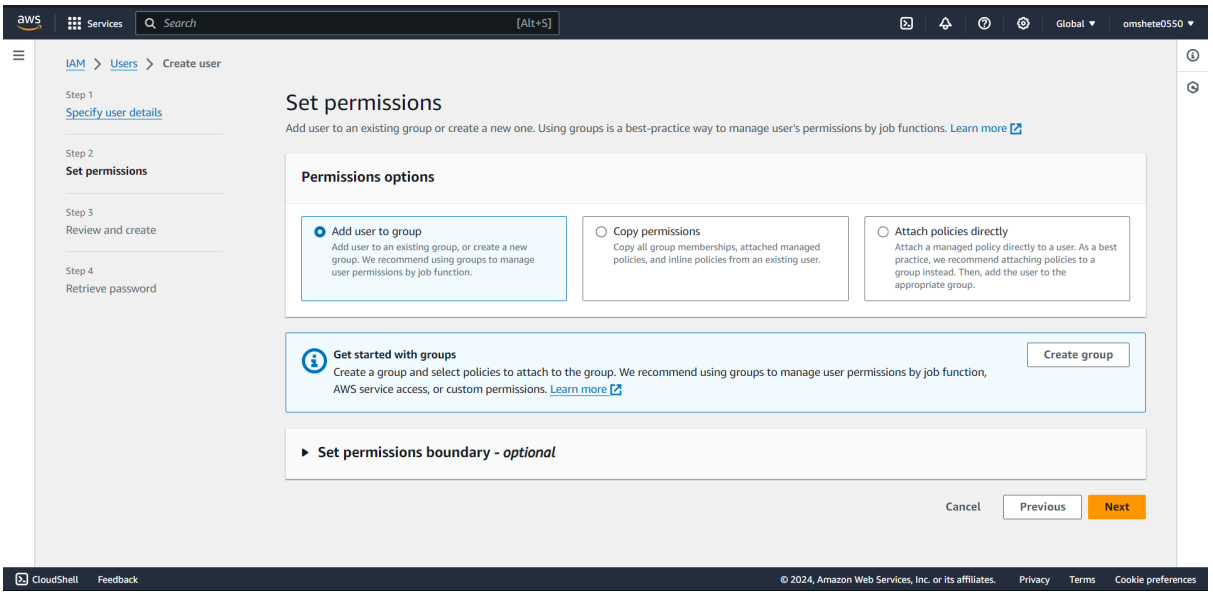
4. Click on “users” in the left column

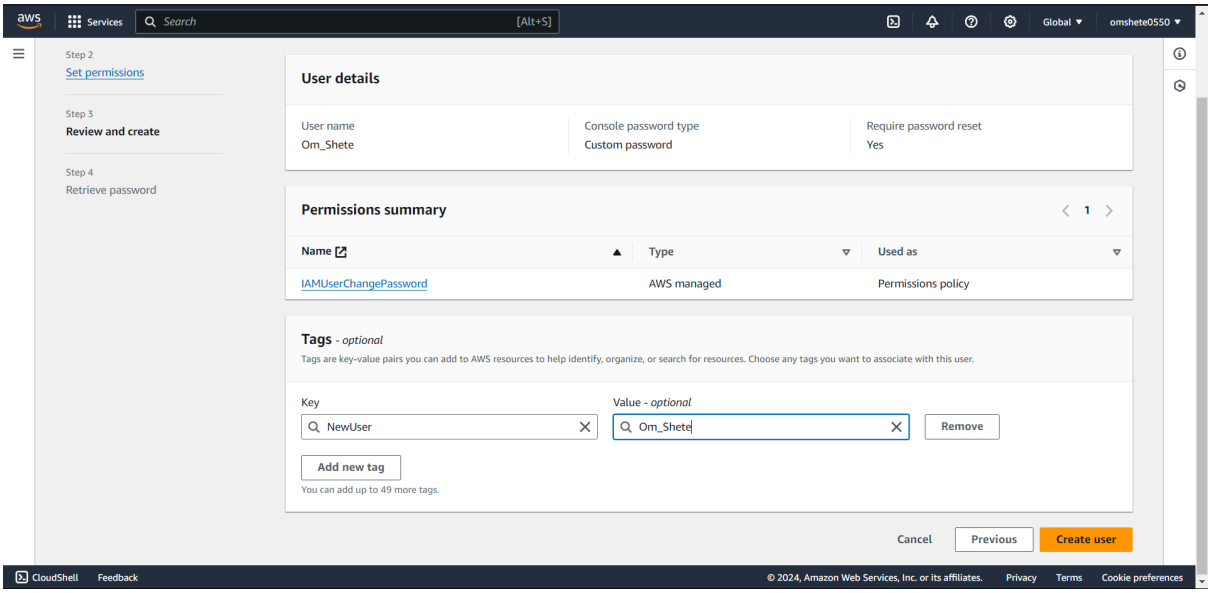


5. Click on the Create Users button

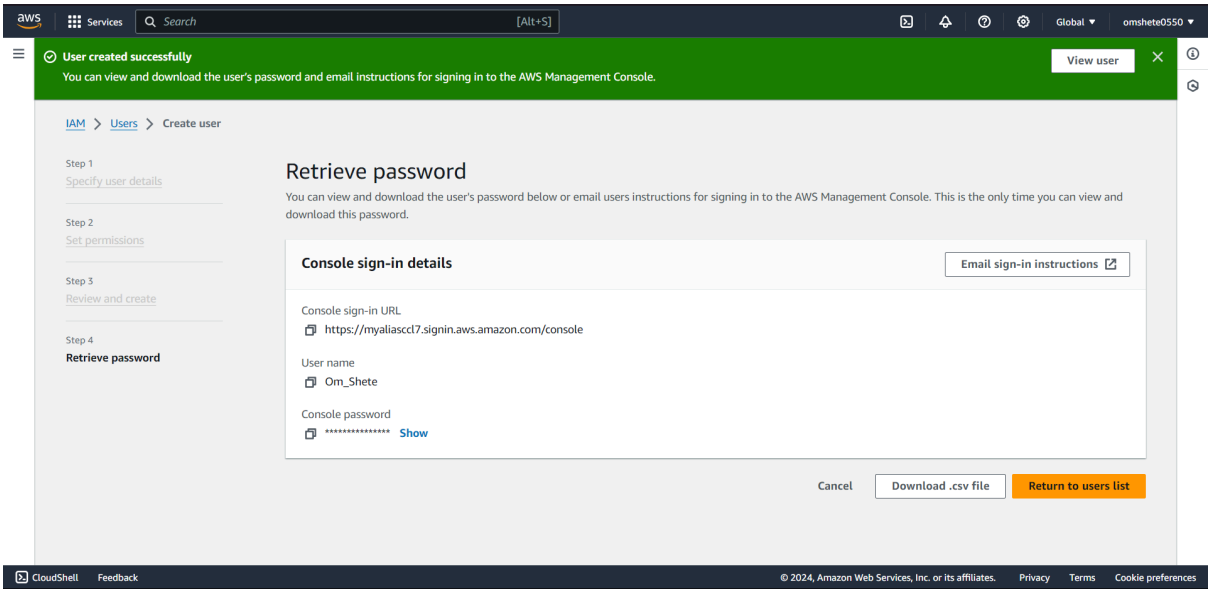


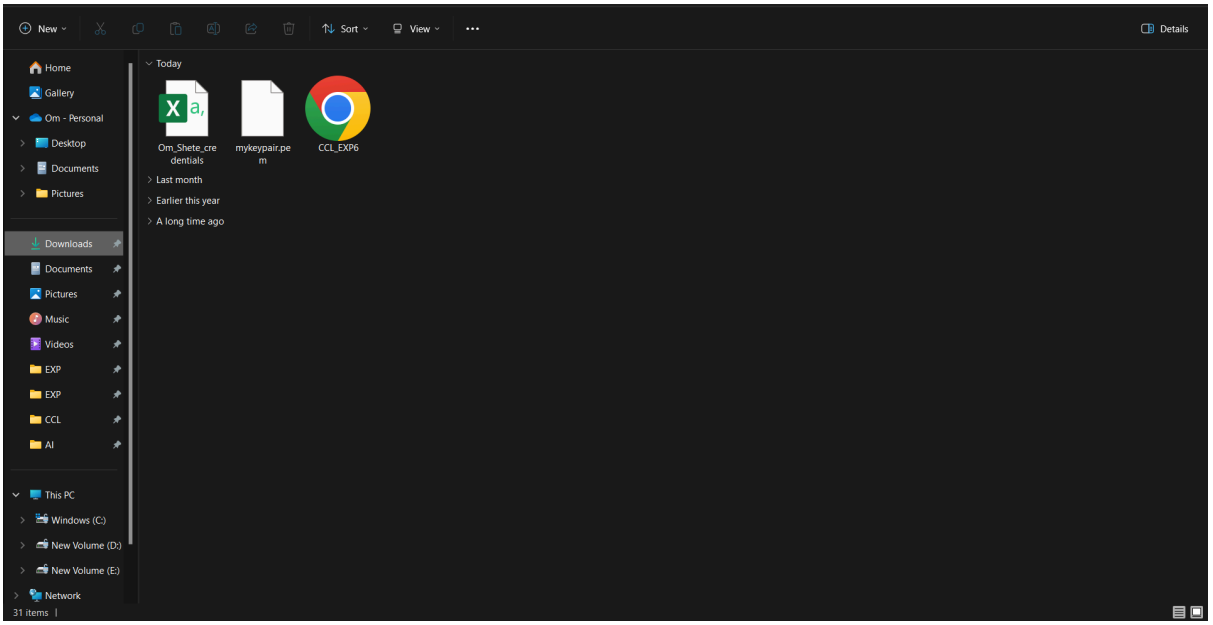

Services
Search
[Alt+S]
Global
omshete0550
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
Console password
Autogenerated password
You can view the password after you create the user.
Custom password
Enter a custom password for the user.
Must be at least 8 characters long
Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '
Show password
Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
Global
omshete0550
IAM
Users
Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
Create group
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

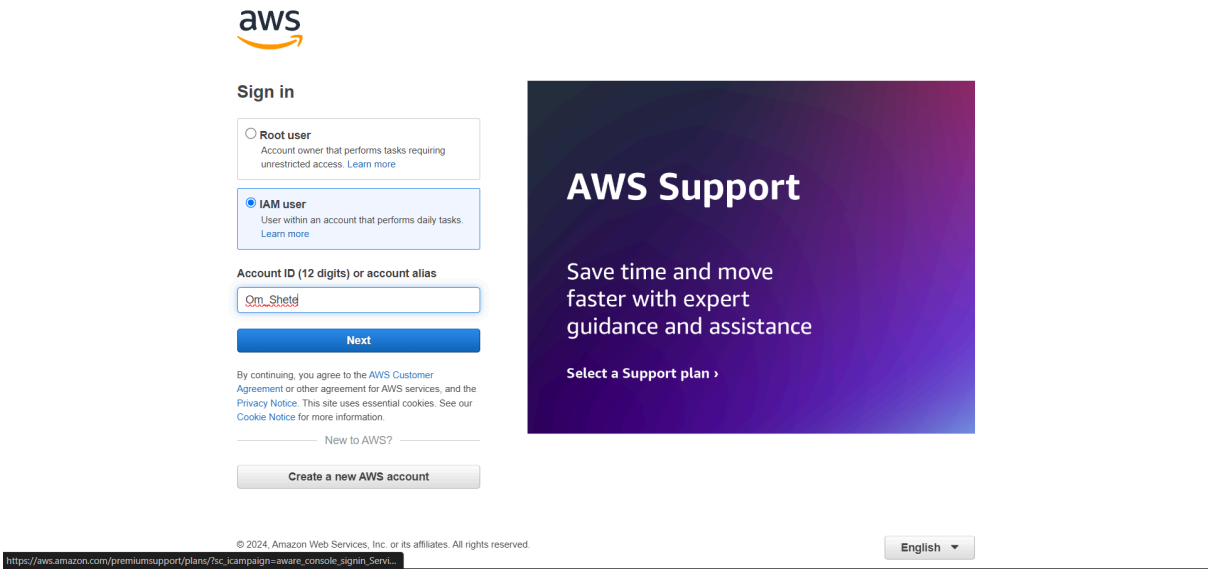

Services
Search
[Alt+S]
Global
omshete0550
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
User details
User name
Om_Shete
Console password type
Custom password
Require password reset
Yes
Permissions summary
Name
Type
Used as
IAMUserChangePassword
AWS managed
Permissions policy
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
Key
NewUser
Value - optional
Om_Shete
Remove
Add new tag
You can add up to 49 more tags.
Cancel
Previous
Create user
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

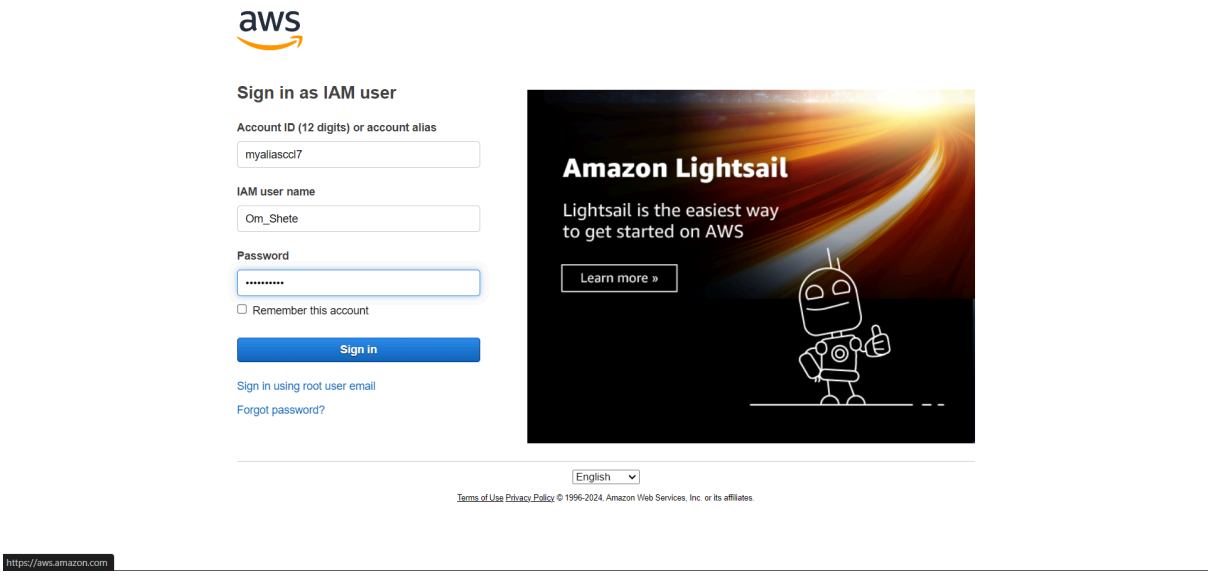
Om Shete - C3 - 2103163

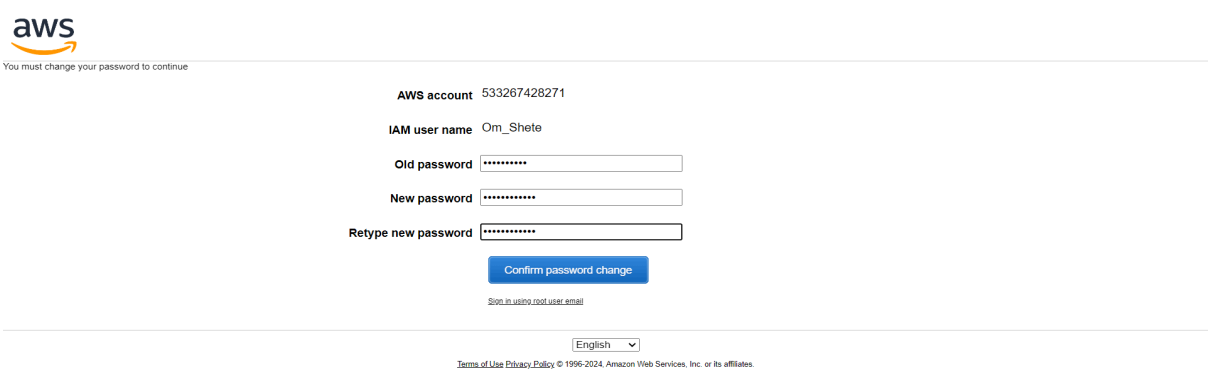




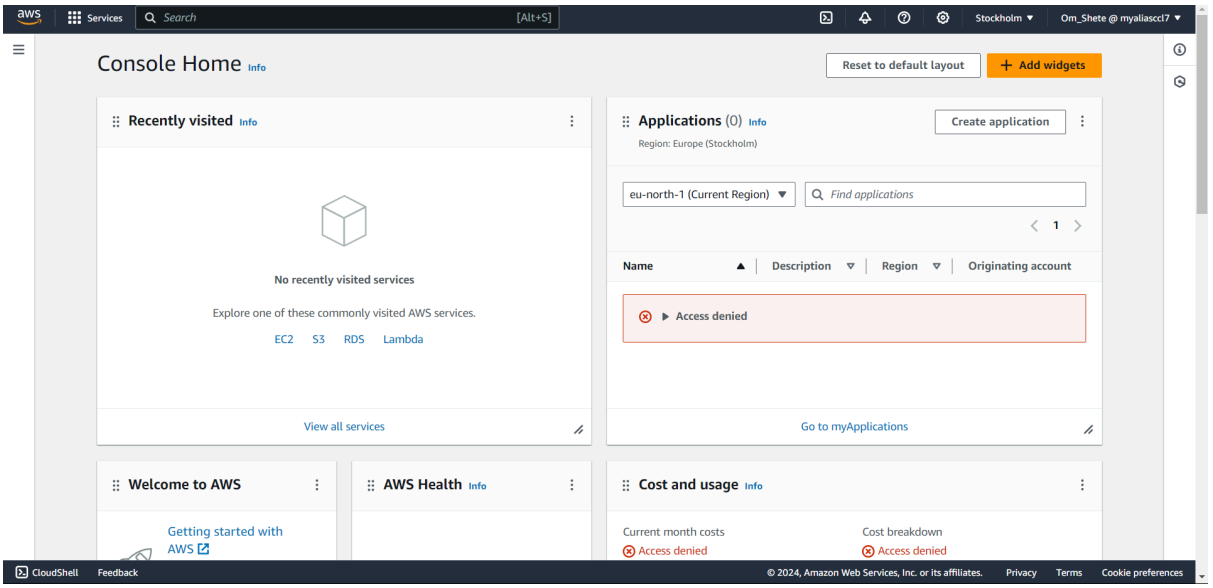
Logging in as the new User & Checking their permissions
Enter the new user's name and psw saved earlier

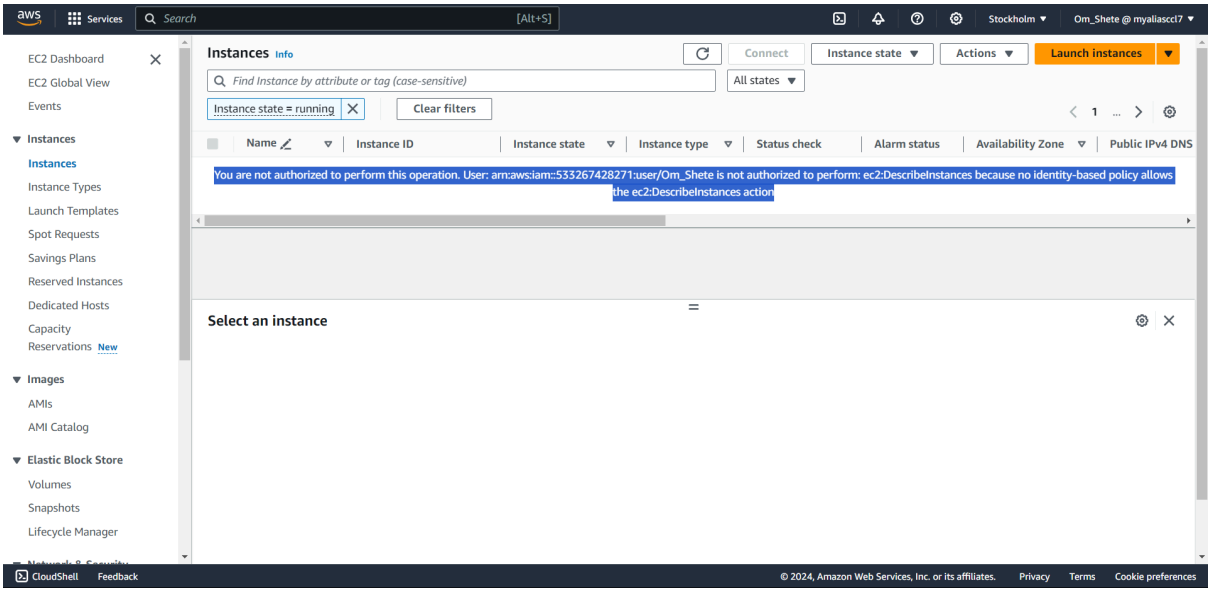


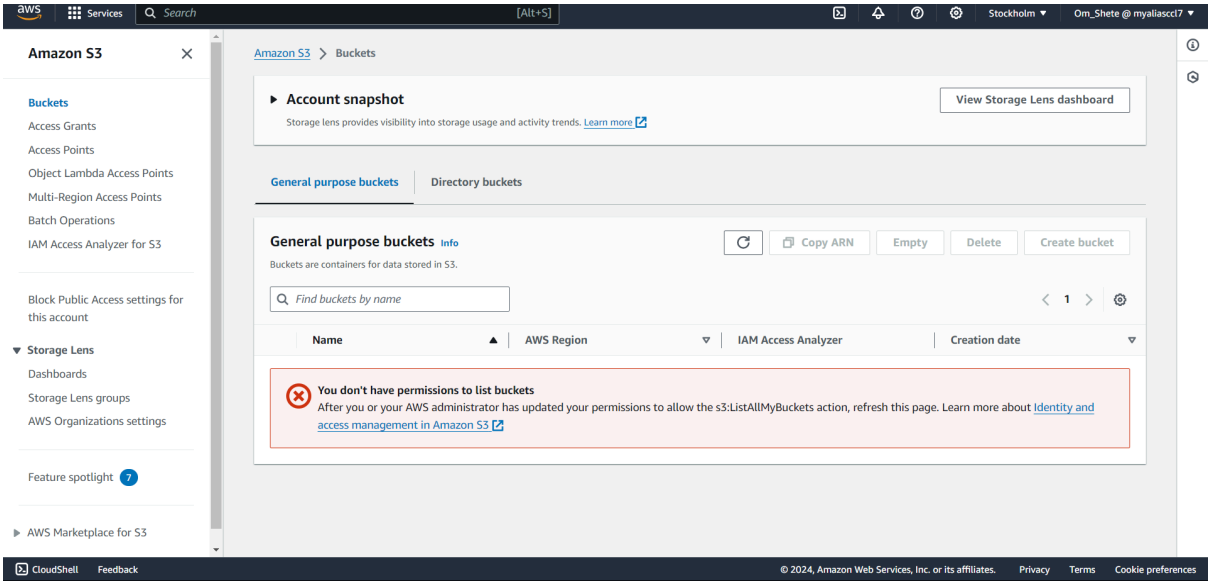


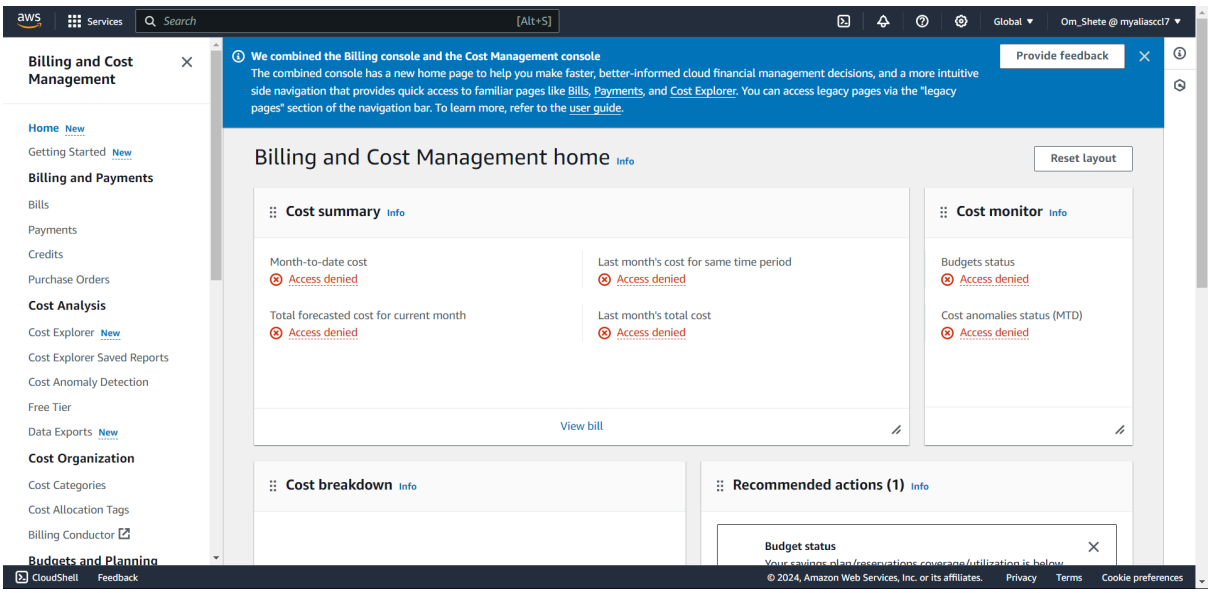


After logging in, you will notice that you don't have permission to do anything yet

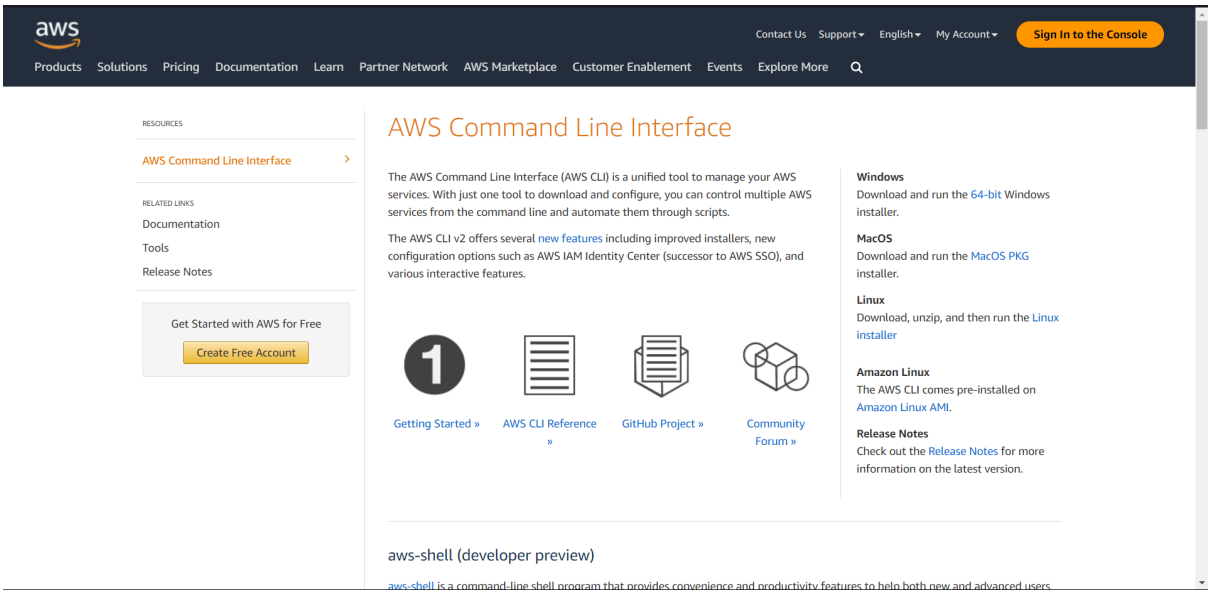


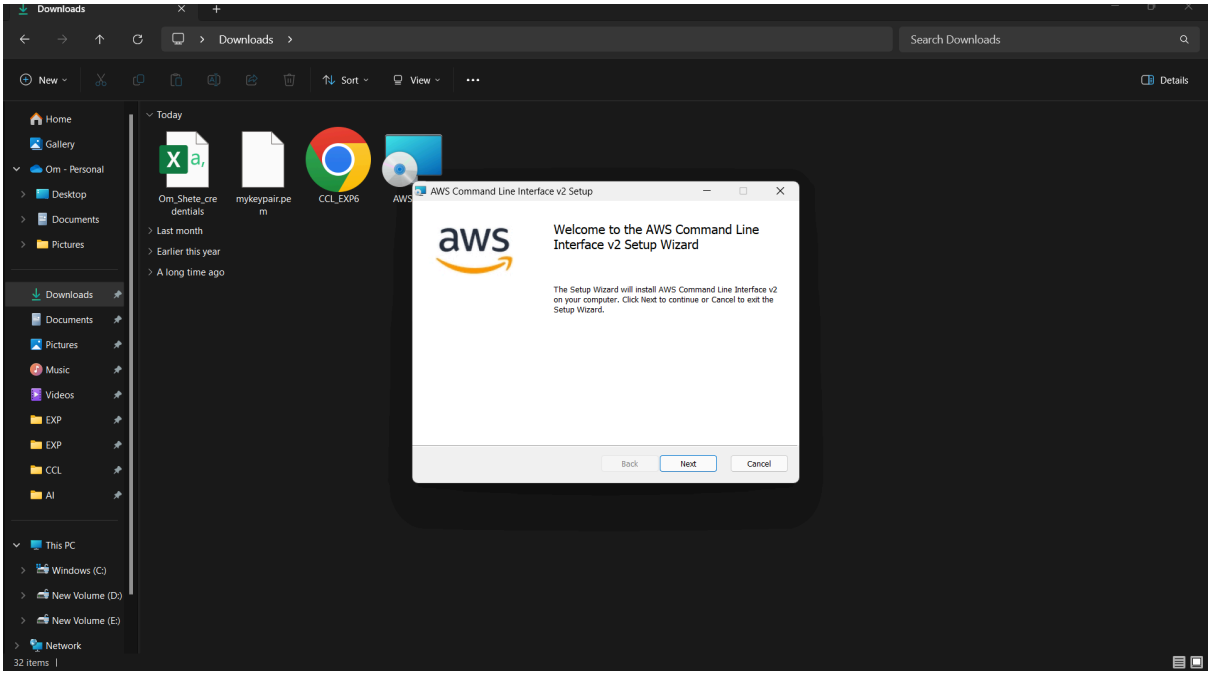


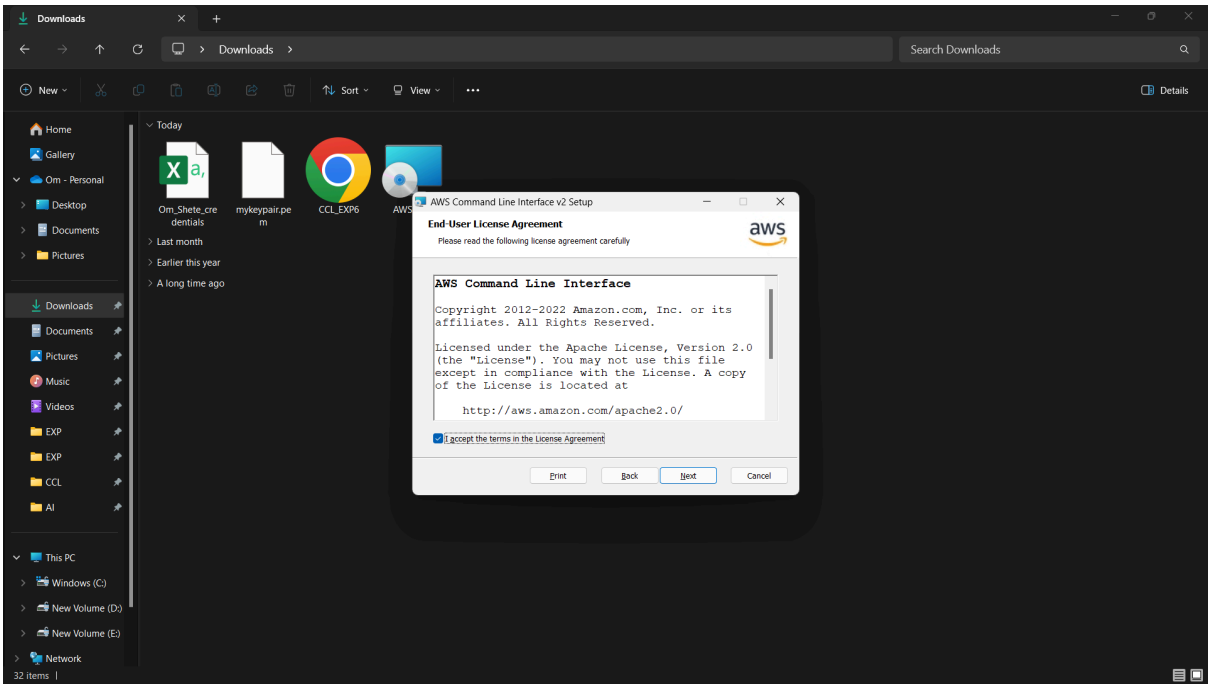


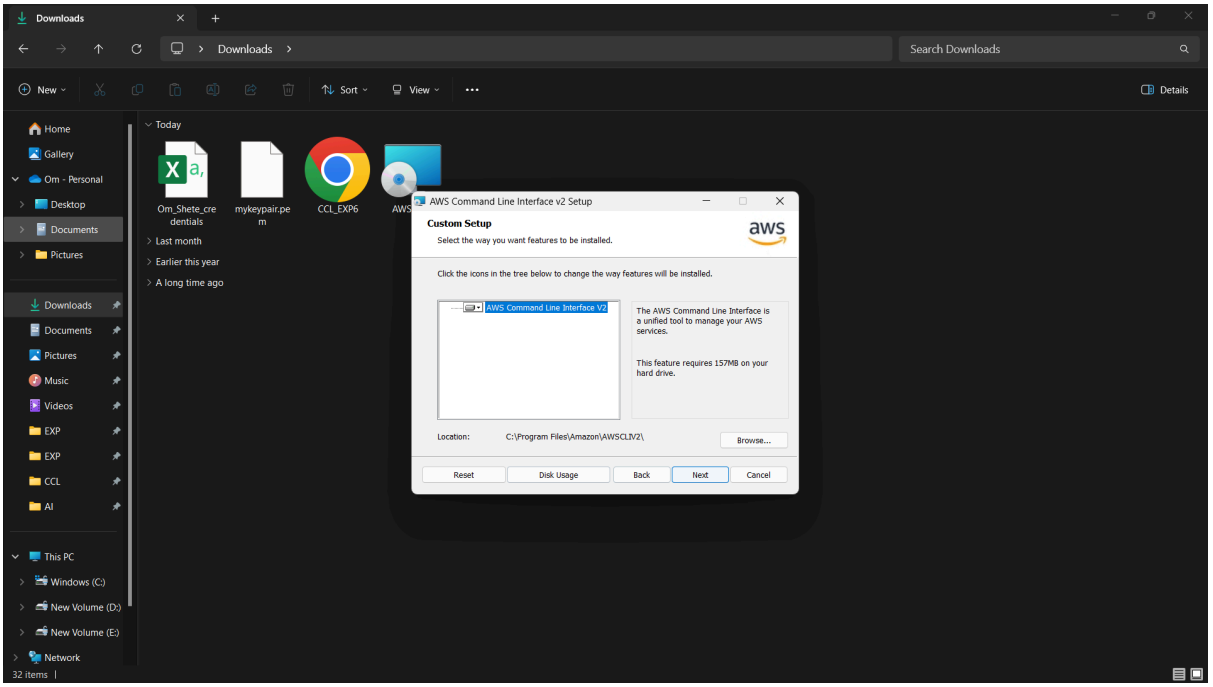


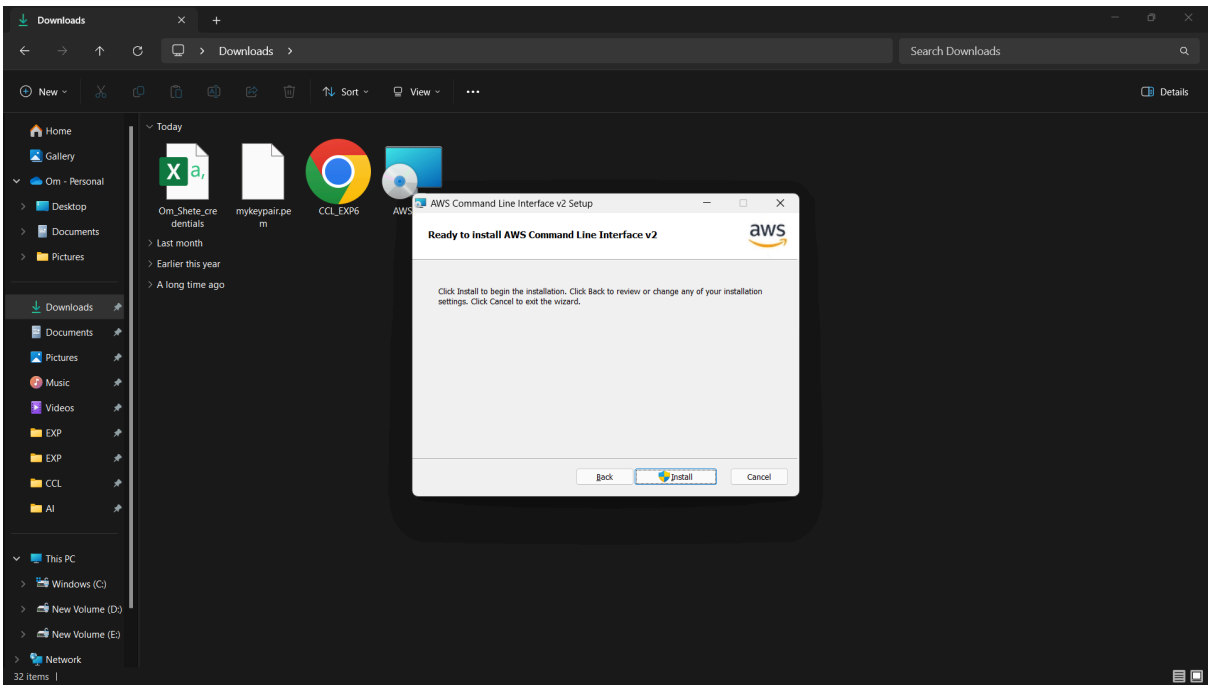
Type “AWS CLI” in a new window of any browser and go to it’s the main page of AWS regarding the same Click on 64-bit hyperlink in the RHS column under the Windows section and download, install the AWS CLI

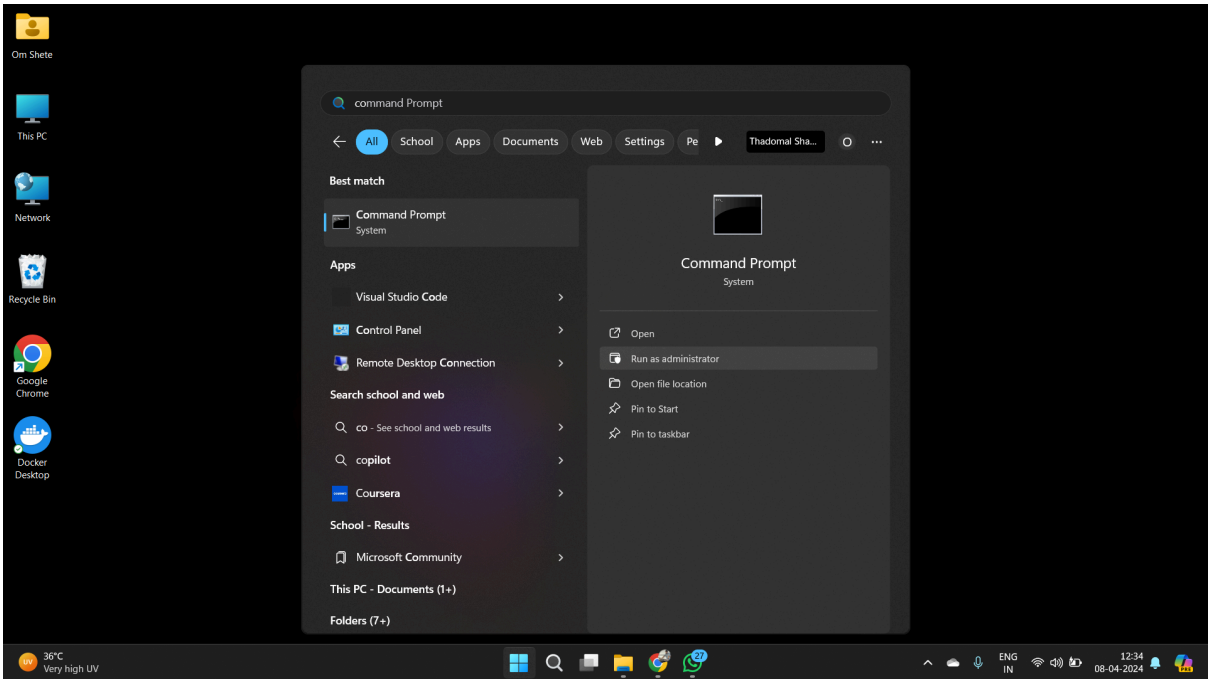



Downloads
Search Downloads
New
Sort
View
Details
Home
Gallery
Om - Personal
Desktop
Documents
Pictures
Downloads
Documents
Pictures
Music
Videos
EXP
EXP
CCL
AI
This PC
Windows (C:)
New Volume (D:)
New Volume (E:)
Network
32 items
Today
Om_Shete_credentials
mykeypair.pem
CCL_EXP6
Last month
Earlier this year
A long time ago
AWS Command Line Interface v2 Setup
Welcome to the AWS Command Line Interface v2 Setup Wizard
The Setup Wizard will install AWS Command Line Interface v2 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel

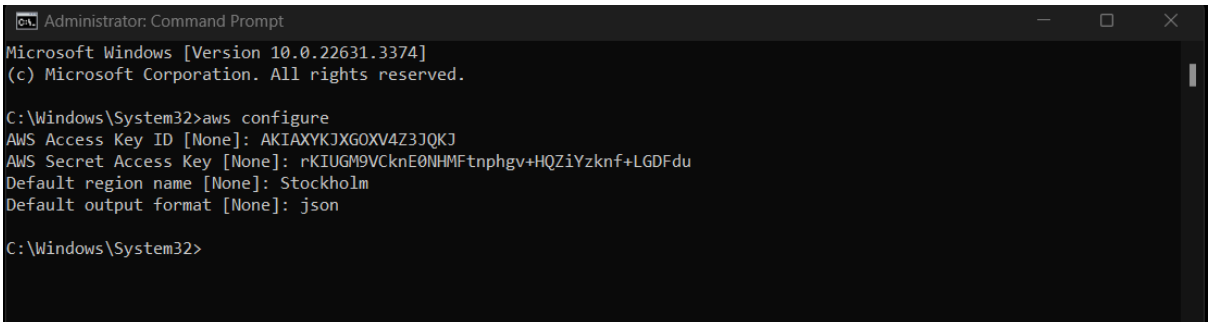

Downloads
Search Downloads
New
Sort
View
Details
Home
Gallery
Om - Personal
Desktop
Documents
Pictures
Downloads
Documents
Pictures
Music
Videos
EXP
EXP
CCL
AI
This PC
Windows (C:)
New Volume (D:)
New Volume (E:)
Network
32 items
Today
Om_Shete_credentials
mykeypair.pem
CCL_EXP6
Last month
Earlier this year
A long time ago
AWS Command Line Interface v2 Setup
End-User License Agreement
Please read the following license agreement carefully
AWS Command Line Interface
Copyright 2012-2022 Amazon.com, Inc. or its affiliates. All Rights Reserved.
Licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at
http://aws.amazon.com/apache2.0/
I accept the terms in the License Agreement
Print
Back
Next
Cancel


Downloads
Search Downloads
New
Sort
View
Details
Home
Gallery
Om - Personal
Desktop
Documents
Pictures
Downloads
Documents
Pictures
Music
Videos
EXP
EXP
CCL
AI
This PC
Windows (C:)
New Volume (D:)
New Volume (E:)
Network
32 items
Today
Om_Shete_credentials
mykeypair.pem
CCL_EXP6
Last month
Earlier this year
A long time ago
AWS Command Line Interface v2 Setup
Custom Setup
Select the way you want features to be installed.
Click the icons in the tree below to change the way features will be installed.
AWS Command Line Interface V2
The AWS Command Line Interface is a unified tool to manage your AWS services.
This feature requires 157MB on your hard drive.
Location:
C:\Program Files\Amazon\AWSCLIV2\
Browse...
Reset
Disk Usage
Back
Next
Cancel


Downloads
Search Downloads
New
Sort
View
Details
Home
Gallery
Om - Personal
Desktop
Documents
Pictures
Downloads
Documents
Pictures
Music
Videos
EXP
EXP
CCL
AI
This PC
Windows (C:)
New Volume (D:)
New Volume (E:)
Network
32 items
Today
Om_Shete_credentials
mykeypair.pem
CCL_EXP6
Last month
Earlier this year
A long time ago
AWS Command Line Interface v2 Setup
Ready to install AWS Command Line Interface v2
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

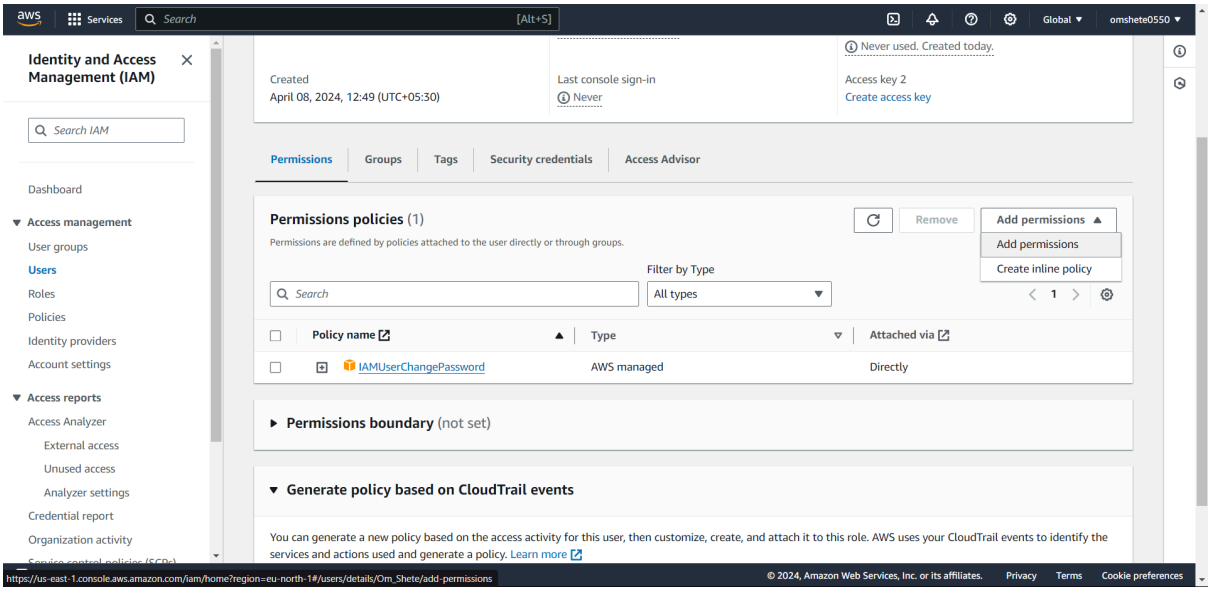


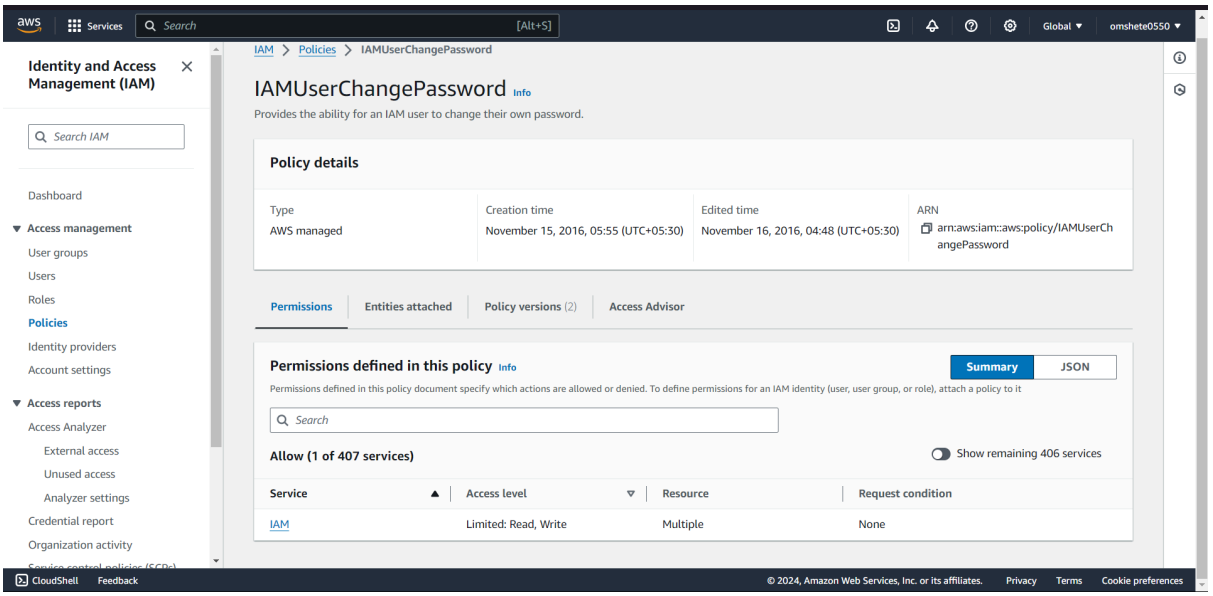
Type aws configure, it will ask for a few inputs; AWS Access Key ID and Key are the ones which we saved earlier Default region name is whichever region AWS you are using; in case of Mumbai, its: apsouth-1 The output format is json in our case



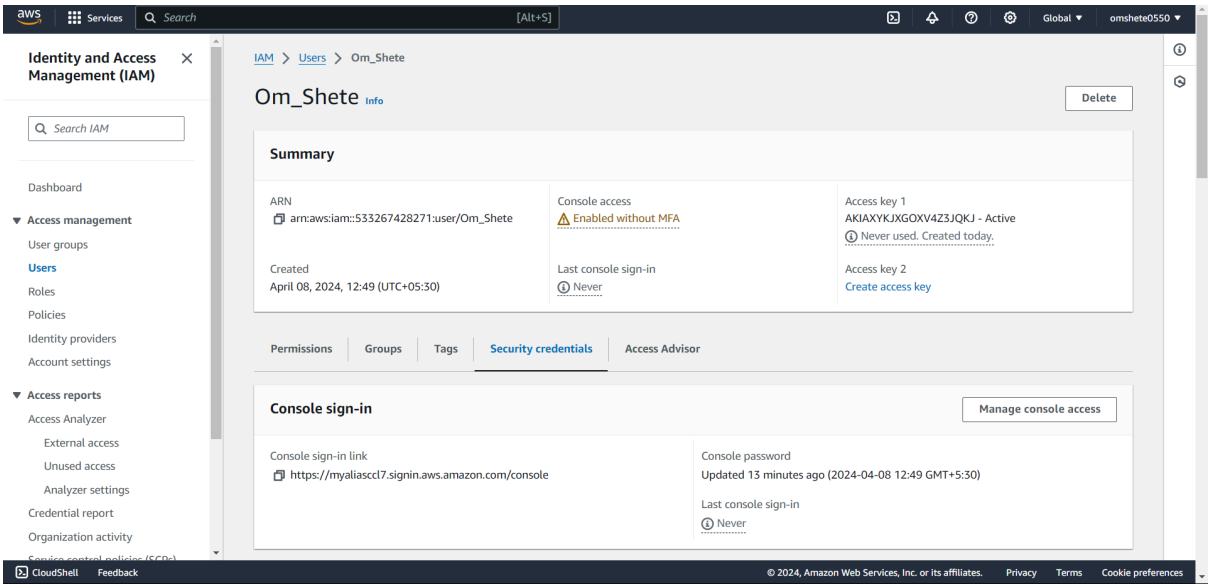
The next two steps are OPTIONAL: aws –version aws s3 ls

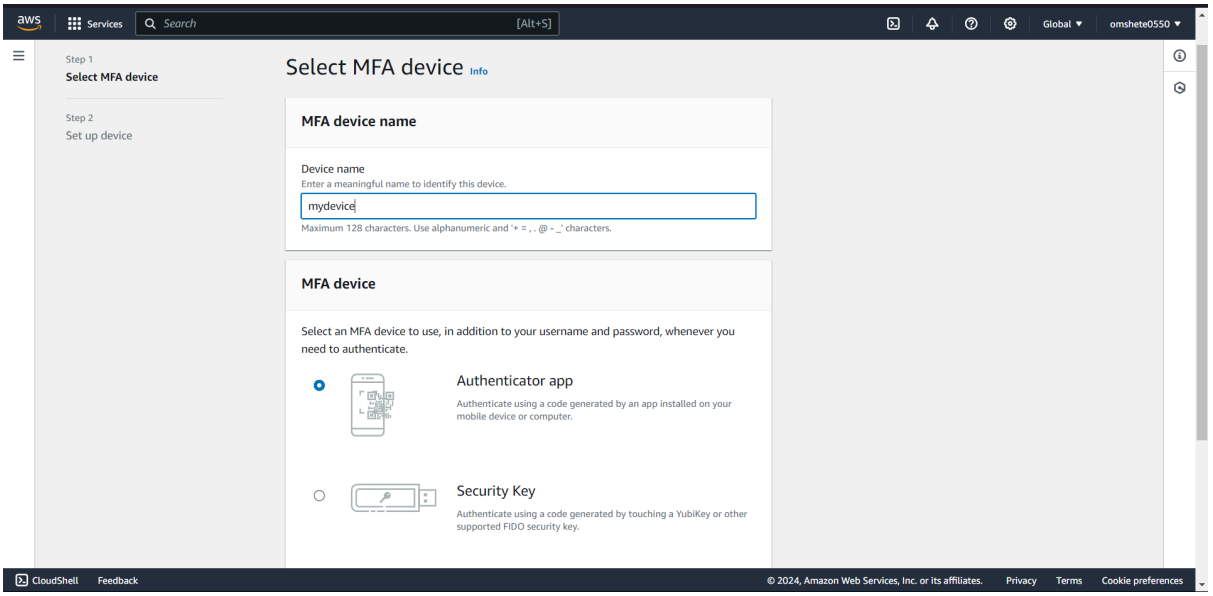
Go in the security credentials tab under Users of IAM Dashboard

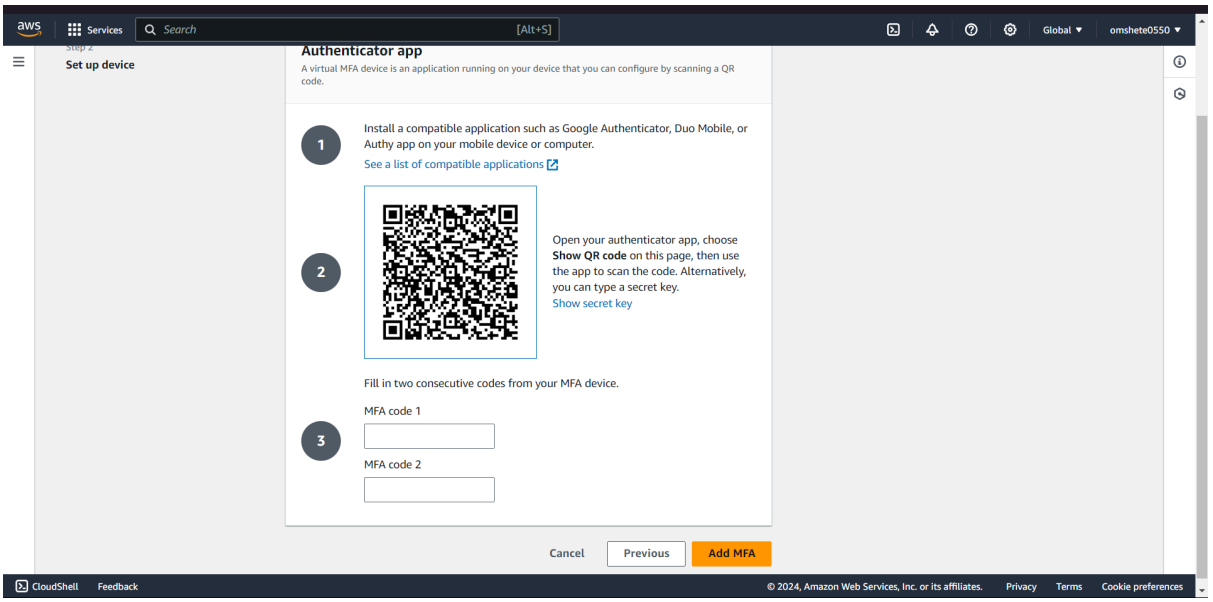




Click on the “Manage” Hyperlink







Enter two of the codes which are shown in the Google Authenticator App over a span of 30 secs each; click on Assign MFA Button