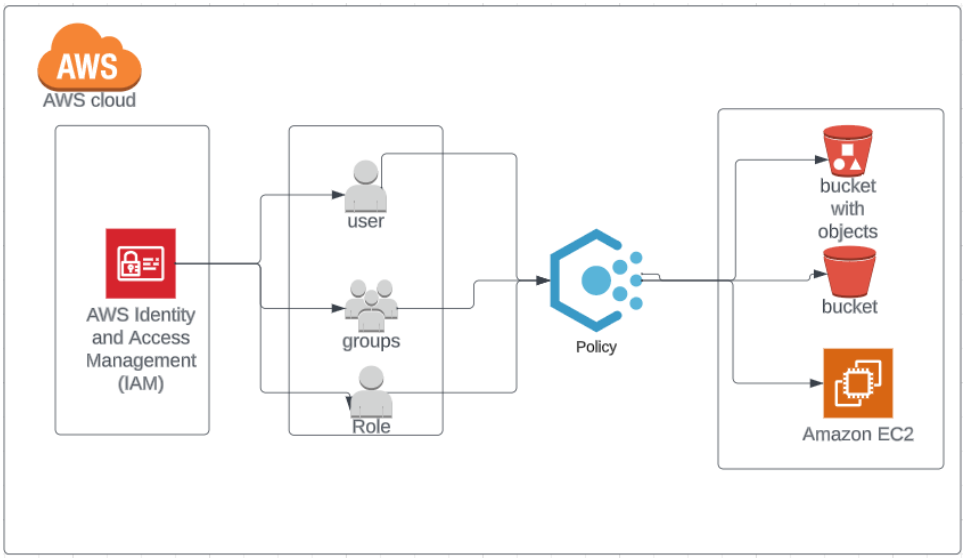
Description:

In this lab we are focusing on Amazon IAM services which is Identity Access Management. With this service we can create users, roles, groups, policies and limit the access to the users in AWS. The difference between user and role is a user can login to the AWS, but a role cannot login. We can attach a role to a user or group. We can attach policies to the users/roles in IAM.

Topology:

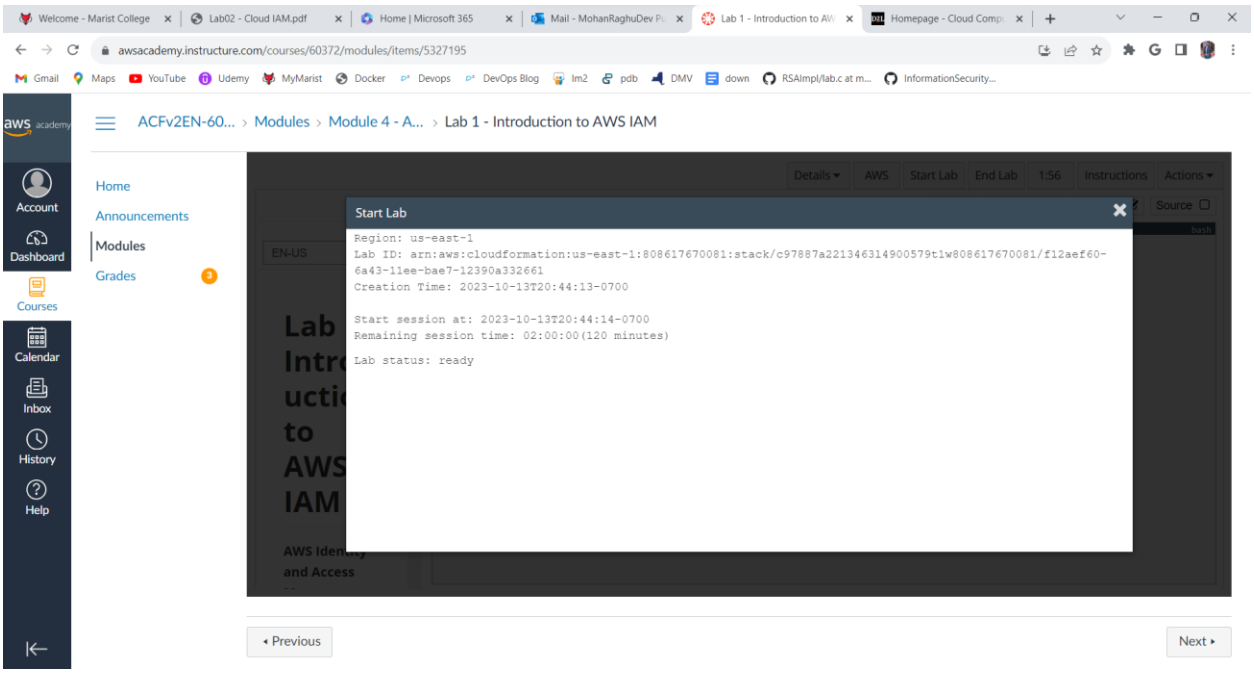


Verification:

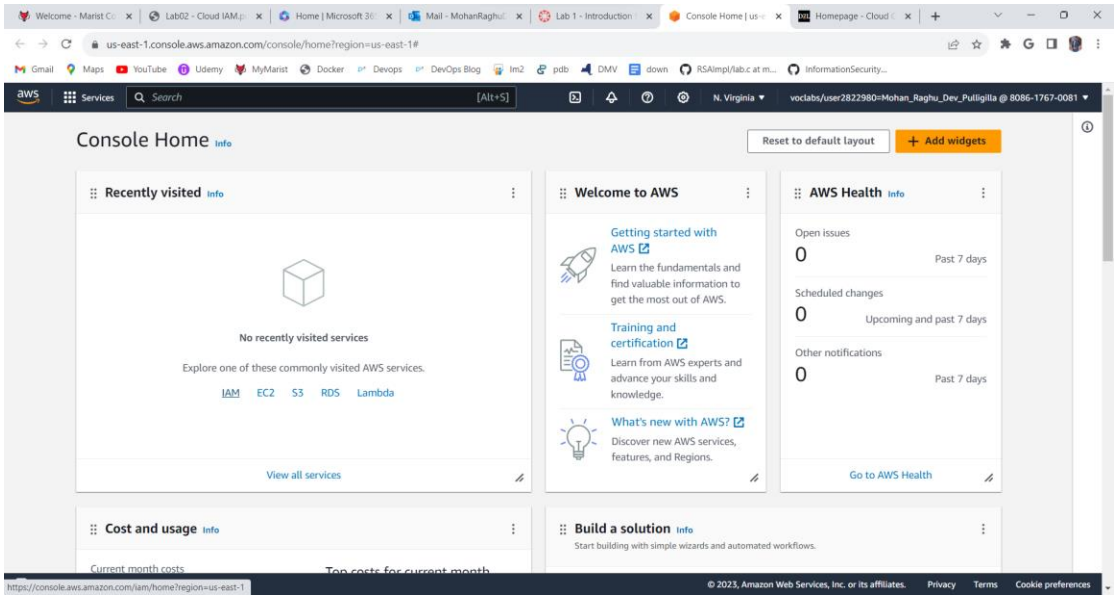
Below are the screenshots of task 1 and 2 exploring the pre created users using AWS CLI and AWS Management Console. Assigned the users with some groups and roles. They worked fine for EC2 and S3. S3 has only read access.

Task I:

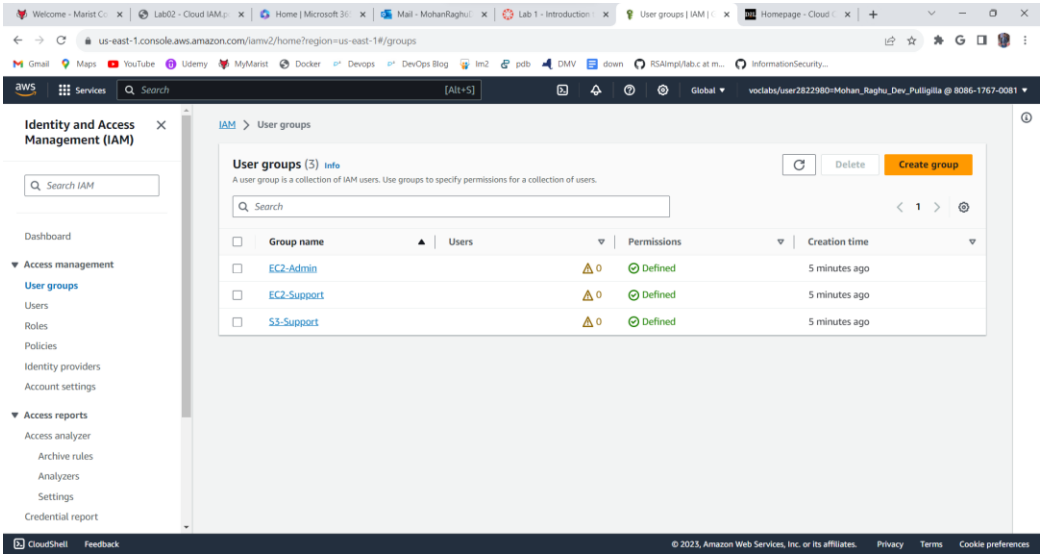
- Once login to the AWS academy you need to click on start lab. After successfully starting the lab, it states that the lab is ready to use.



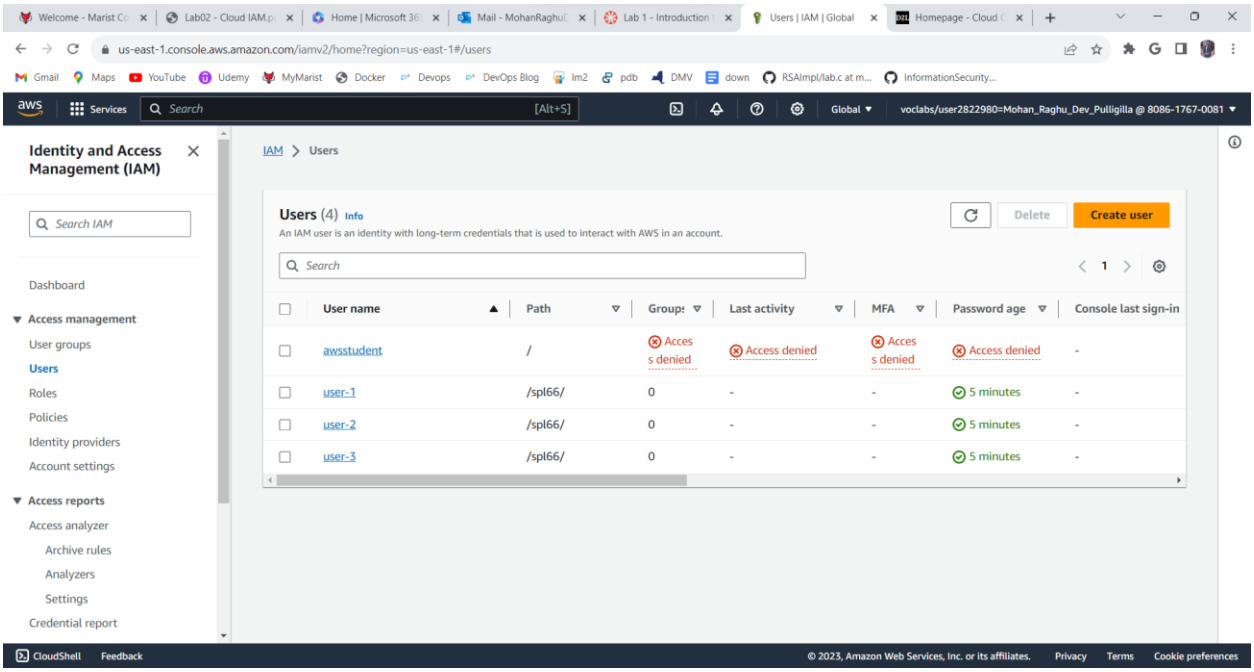
- After the lab is ready to use, we need to click on AWS so that it will redirect to AWS management console.



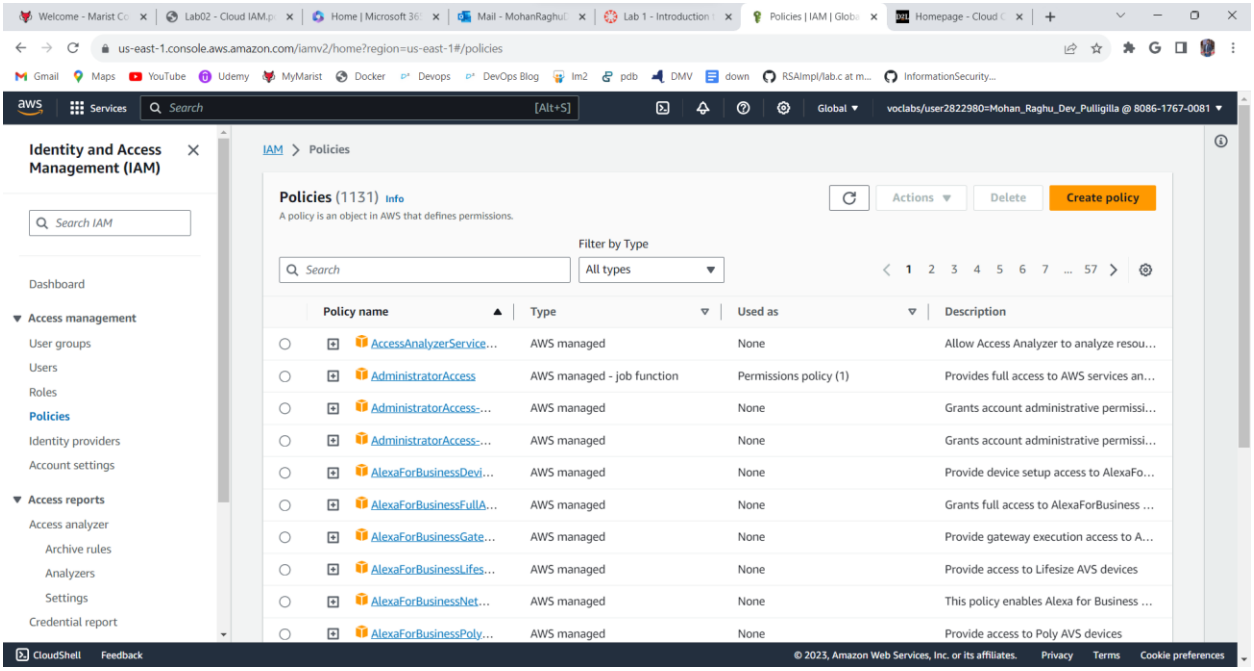
- We need to search for AWS IAM service for that we need to click on shortcut, or we can type in search bar for the required services.
- I have selected user groups which are pre created, only three groups EC2 Admin, Ec2 Support, S3 Support. The support group has read access to specific services. Admin group has full access to that service.



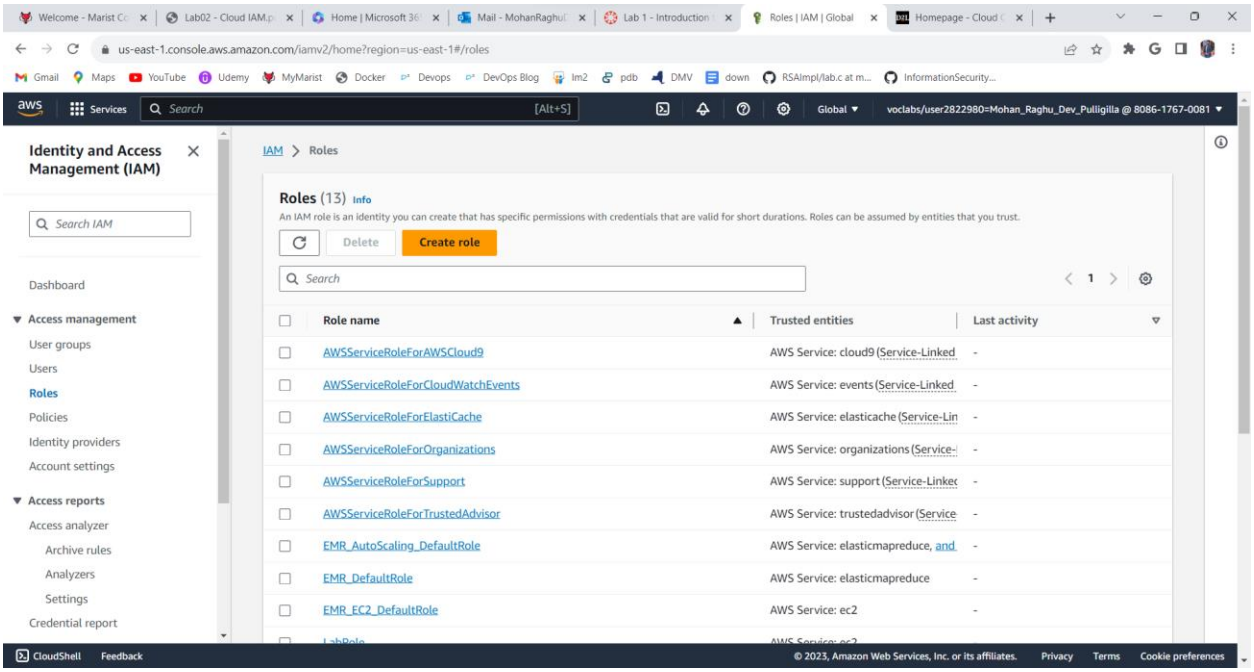
- I have selected the users to display the list of pre created users.
- There are Four users. AWS Student, User-1, User-2, User-3.



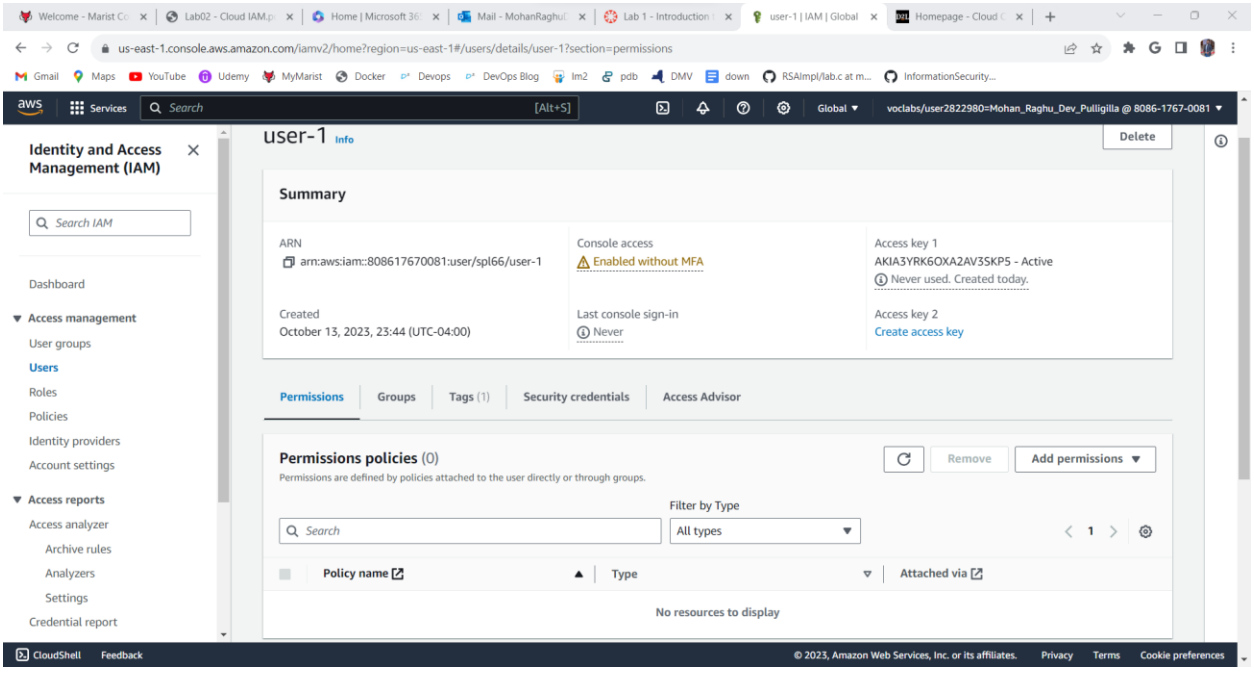
- I have selected policies to see the list of policies, there are 1131 policies which are created by AWS, we can Identify user created as well as AWS created policies by seeing the AWS logo Infront of the policies, whereas user created policies does not have any logo Infront of policy.



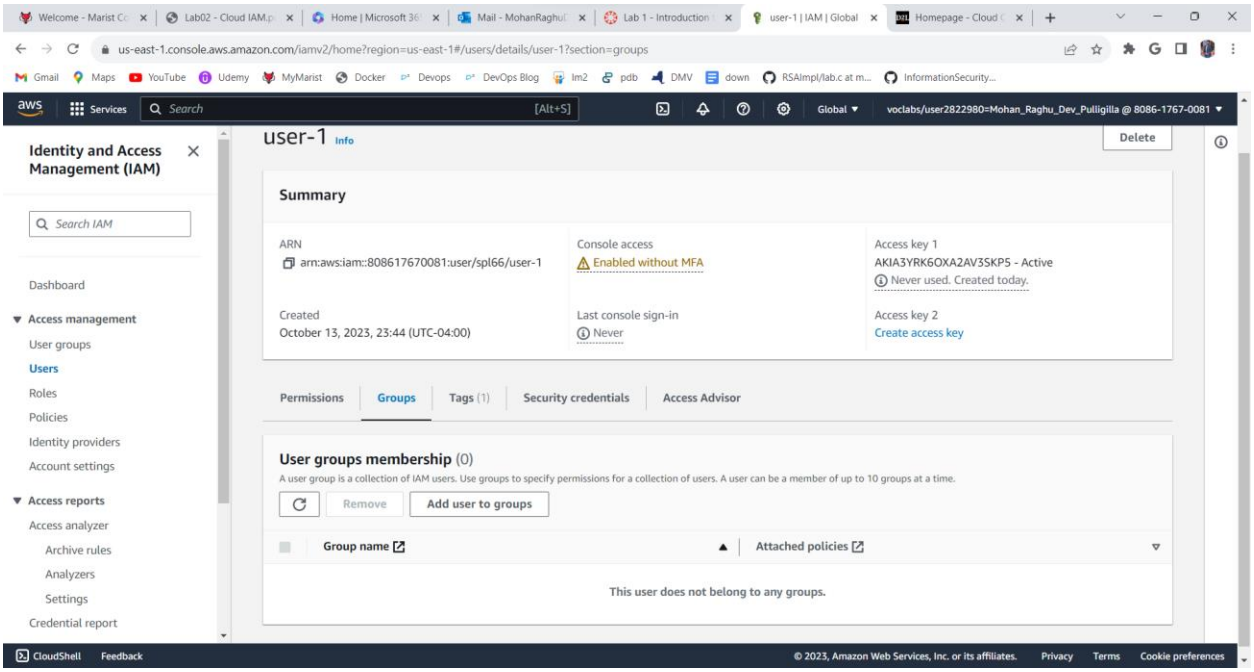
- I have selected roles to see the pre created roles in AWS, we can attach these roles to the users as well as the machines we created. Example EC2_S3role is used to link EC2 and the S3 bucket to read and write to the bucket.



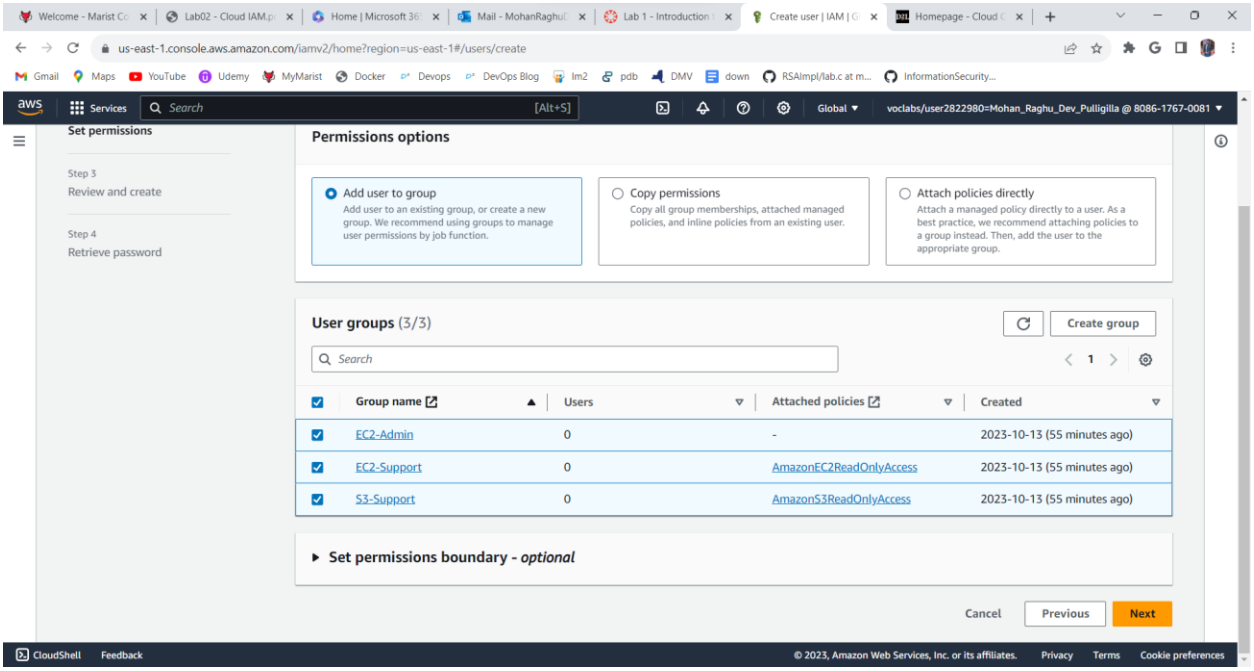
- I have selected user-1 and checked permissions, but there are no permissions attached to it.



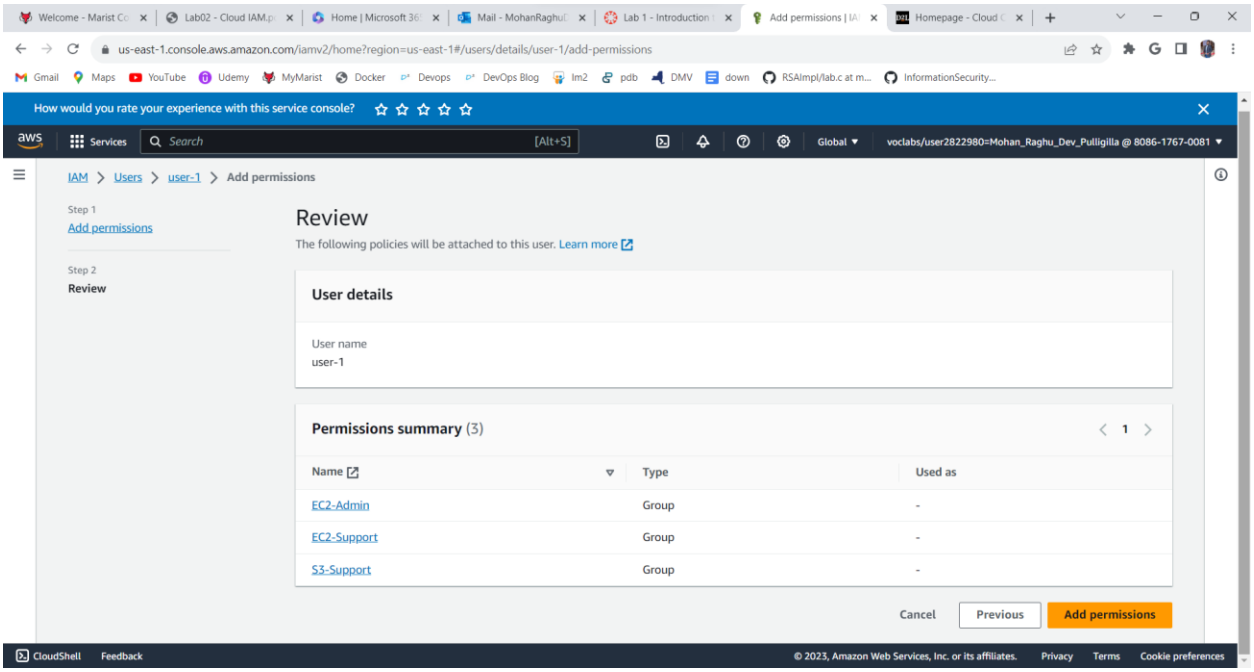
- User-1 doesn't have any groups attached to it.



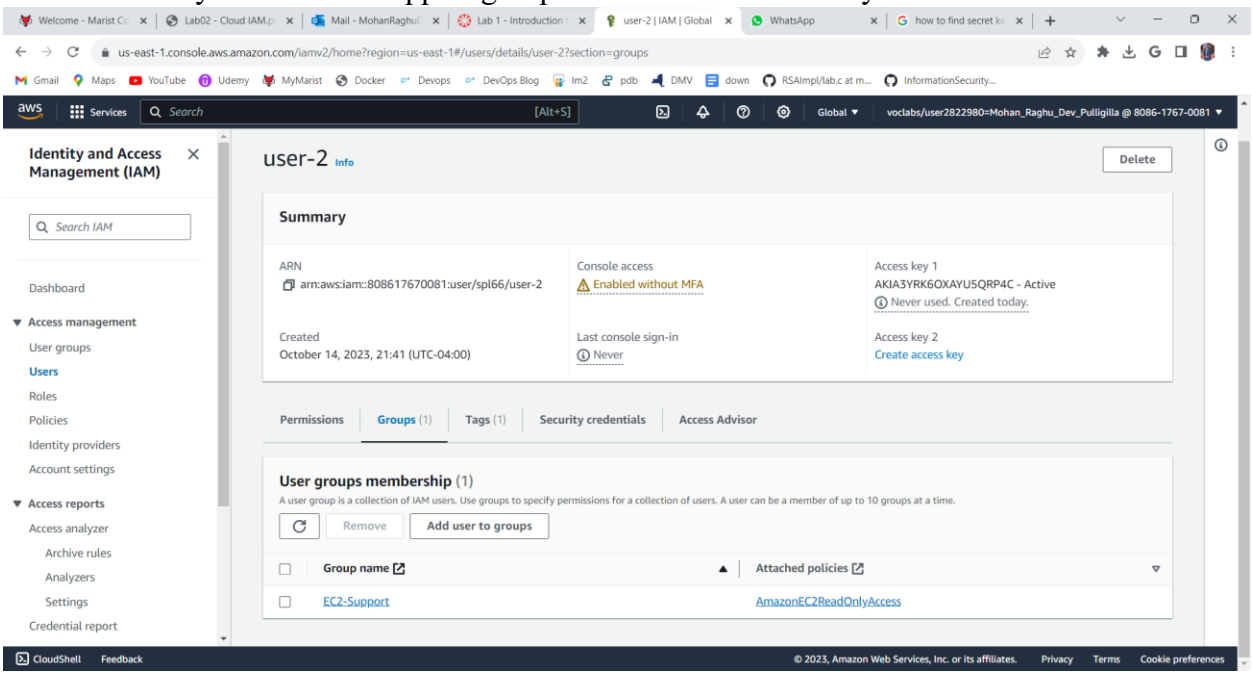
- Click on add user to group and add the groups to user, for user-1 I have added the default 3 pre created groups.



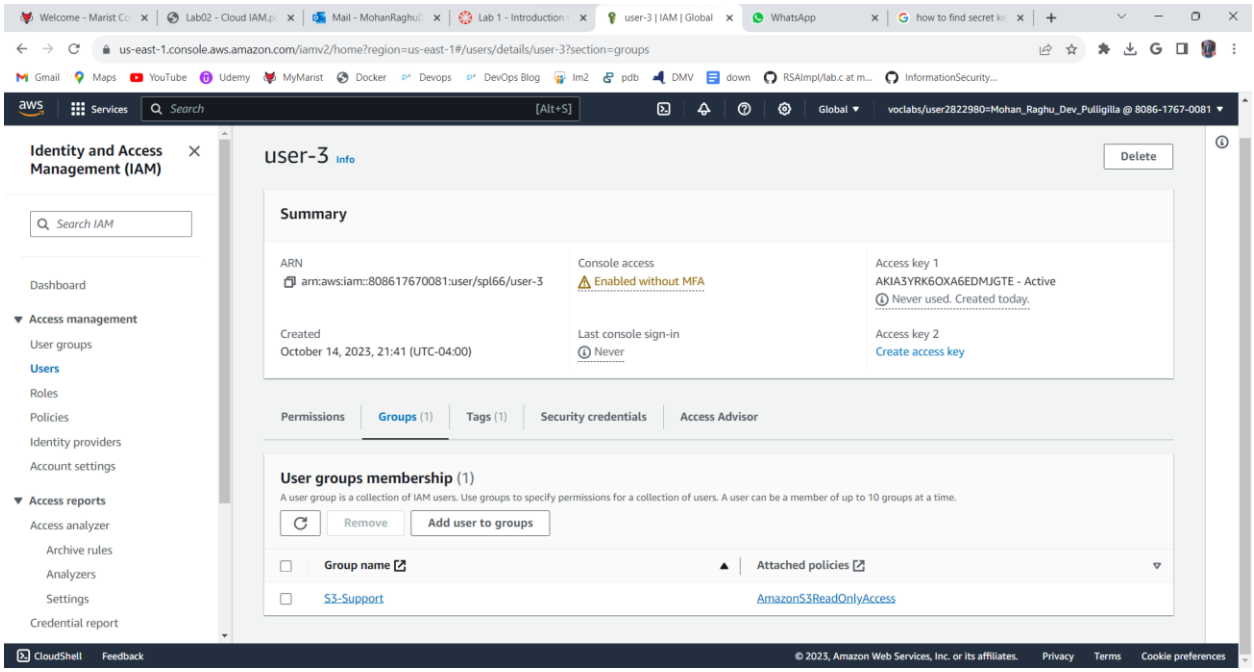
- Once select the groups then click on next and add permissions.



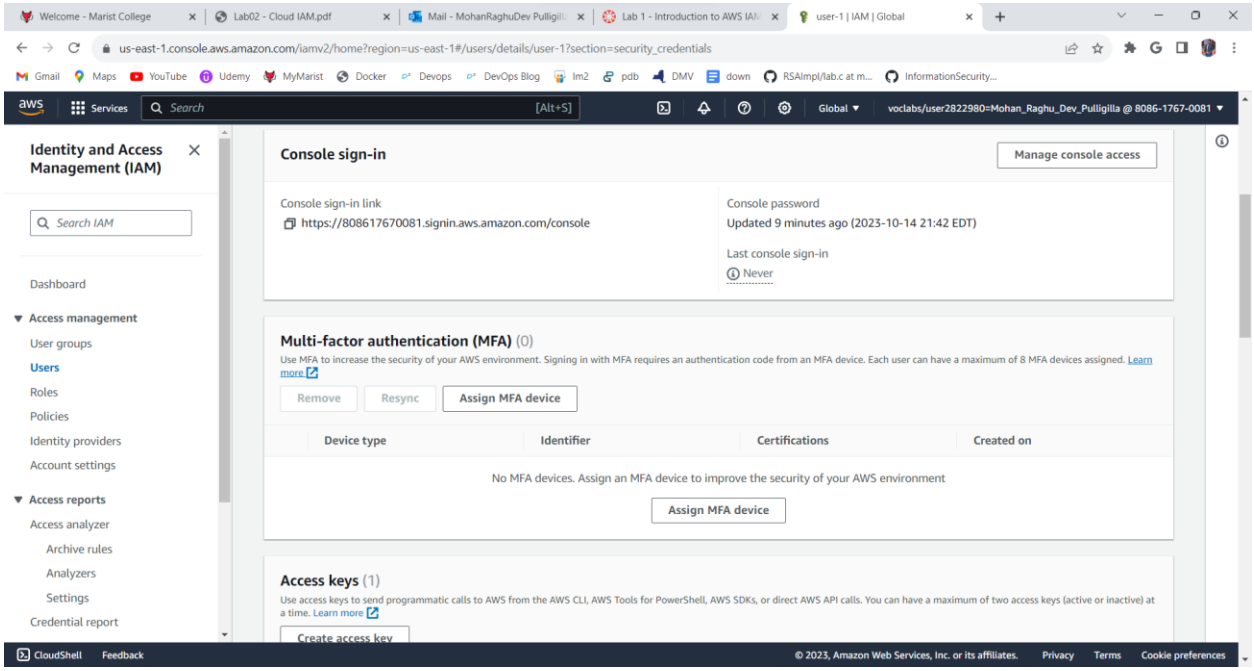
- In the same way added EC2-Support group to user-2.which has only read access to EC2.



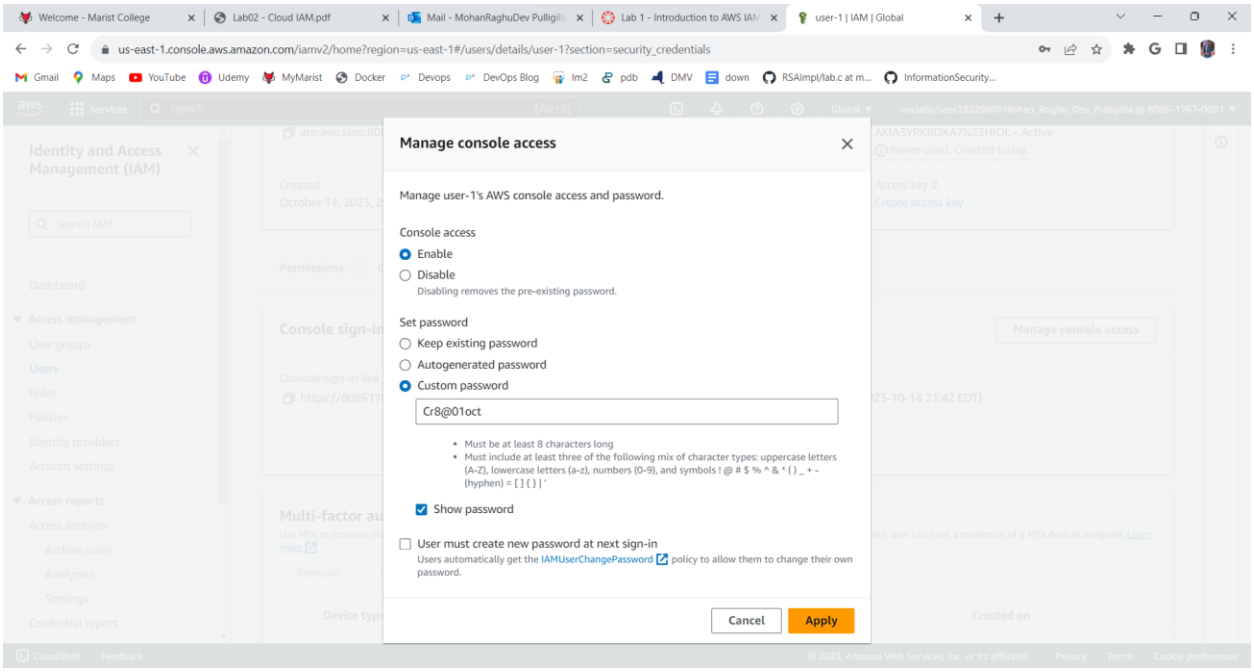
- Added S3-Support group to user-3 , which has only read access to S3 bucket.



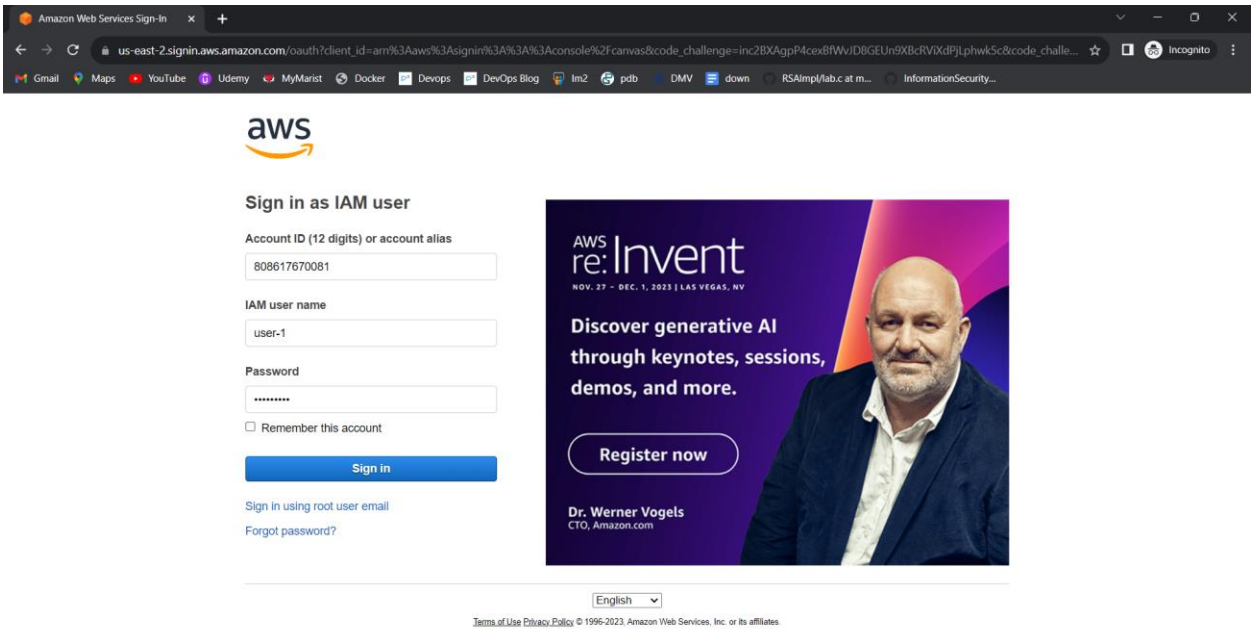
- Once the users are assigned with groups , worked on logging into AWS management console using user-1. For that select user-1 we will see console sign-in link, with that we can login to AWS management console.



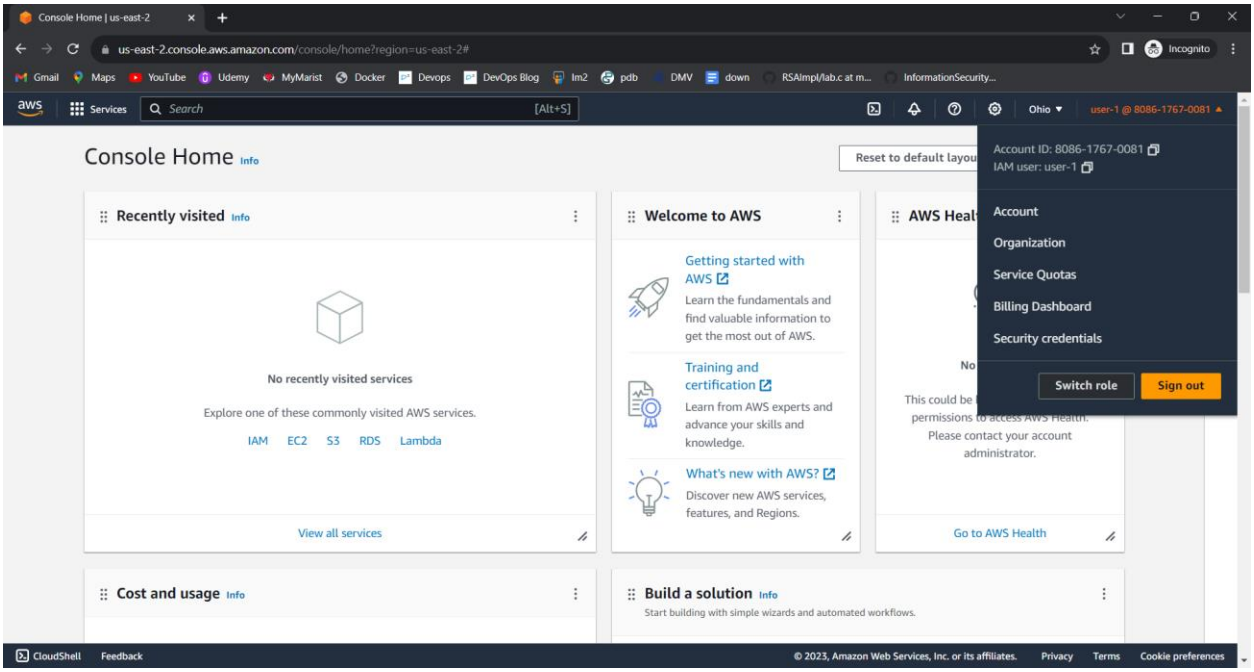
- And then we need to add password for user-1 to login to the AWS management console and the click on apply.



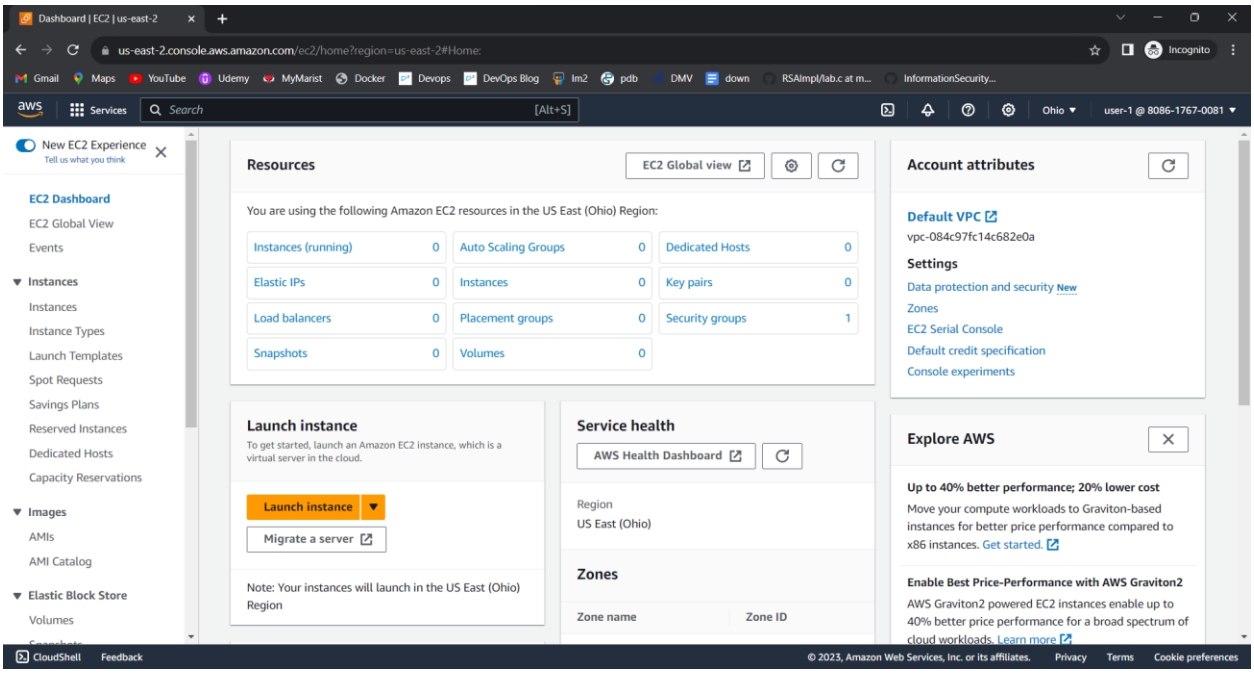
- Once password is created, using that console link login to the AWS management console.



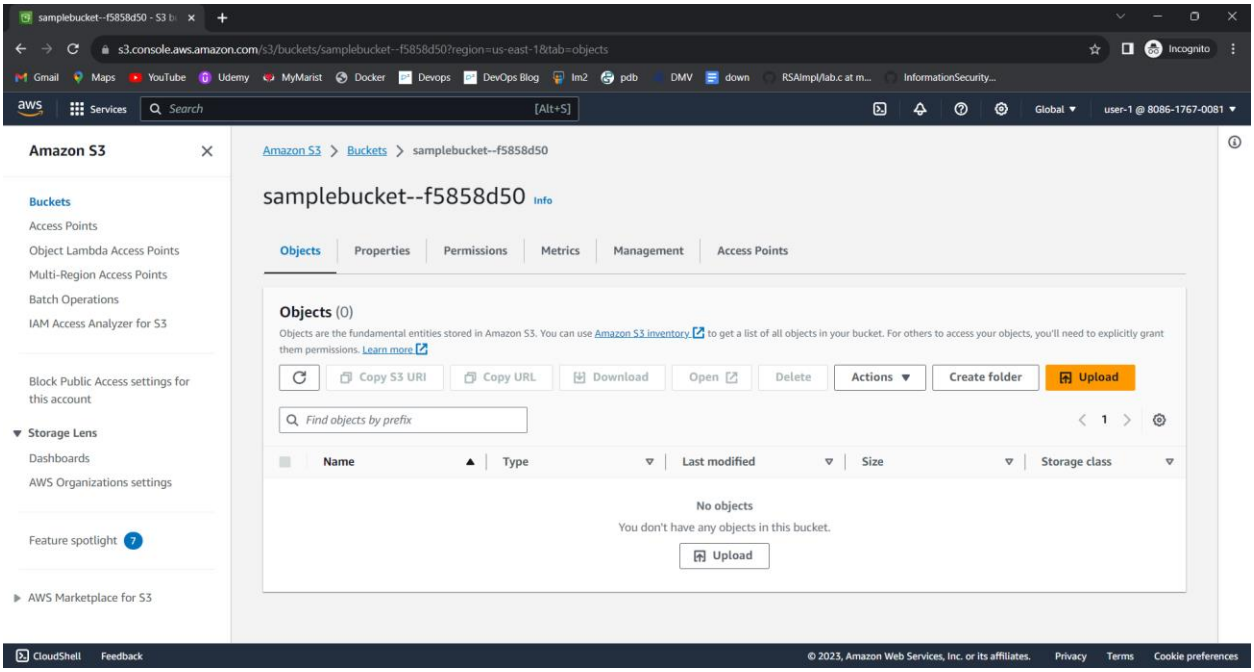
- After Successful login to AWS management console, selected few services to verify the access.



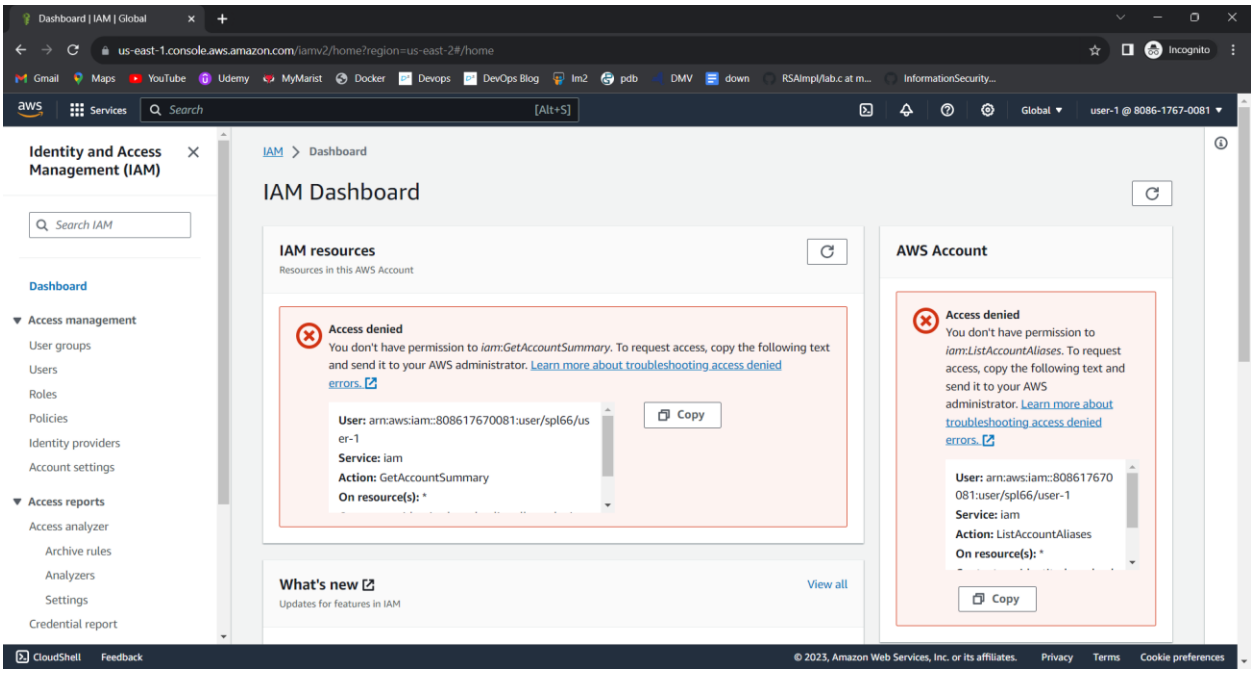
- I have selected the EC2 services and able to see the instances.



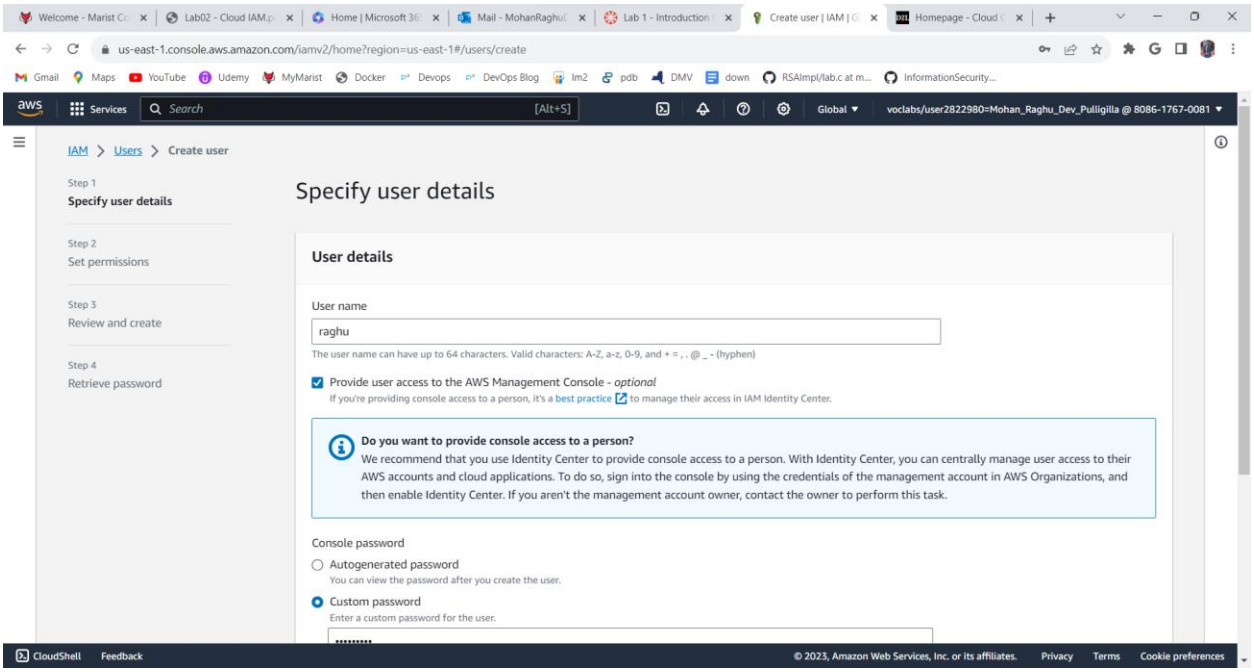
- I have selected the S3 the see the list of buckets.

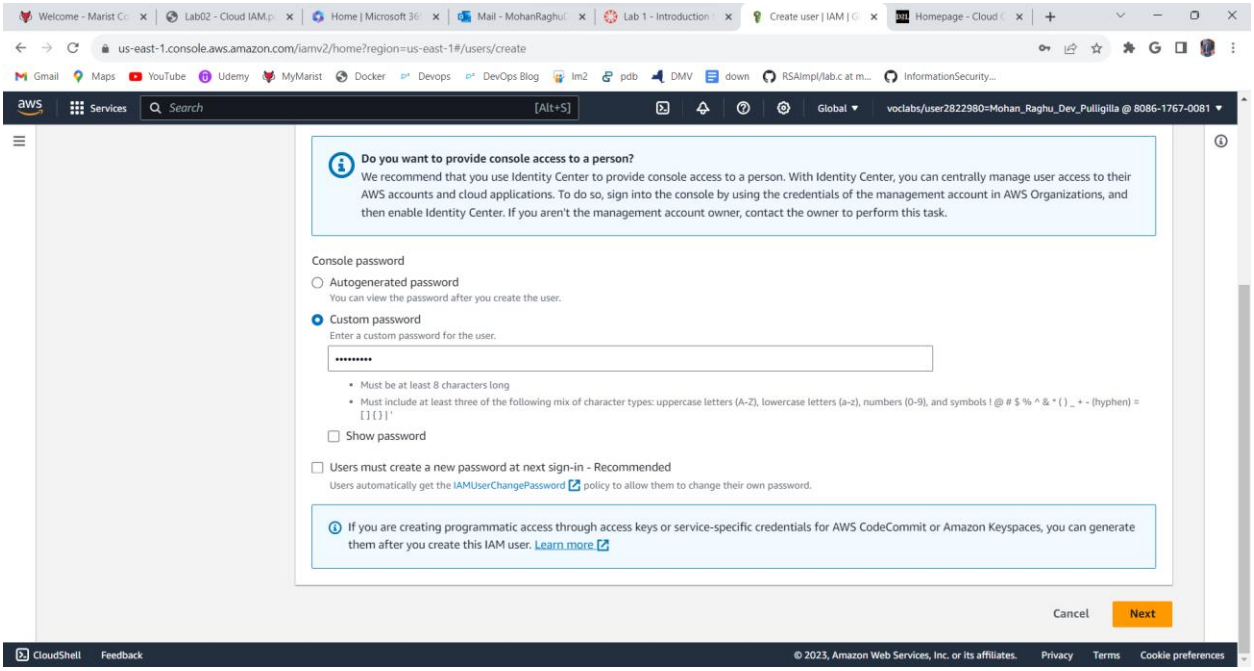


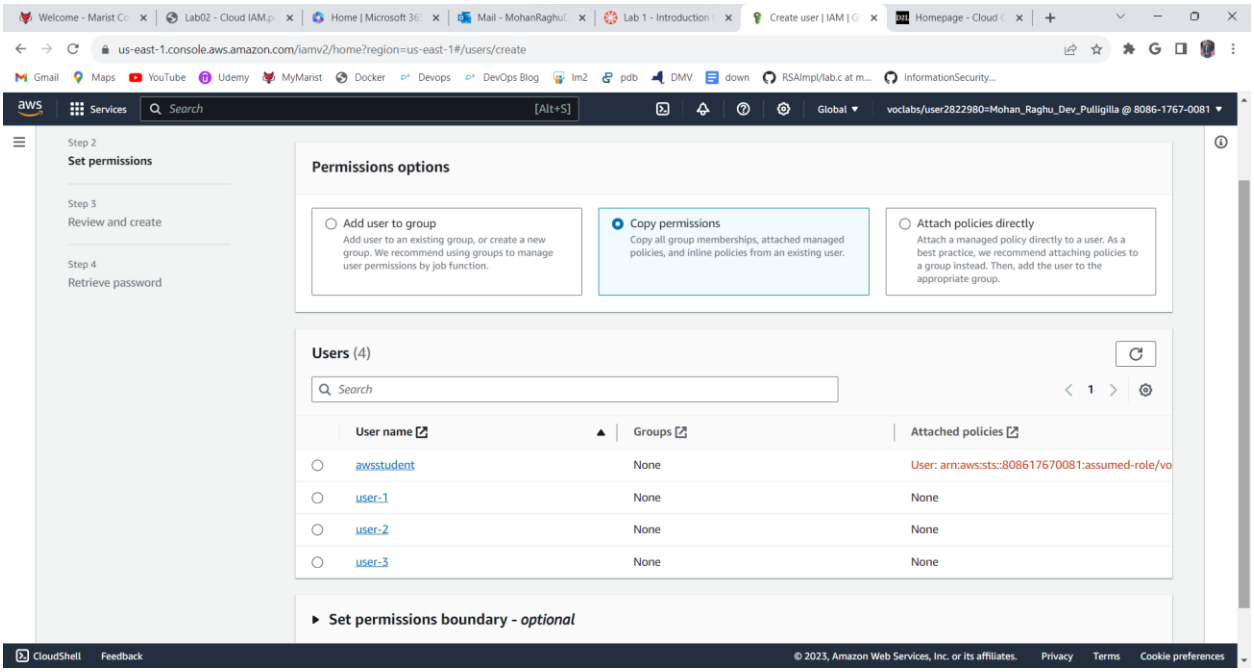
- As the User-1 has only EC2 and S3 access tried to access other services which user-1 doesn't have access to it. I have selected IAM the It showed Access denied.

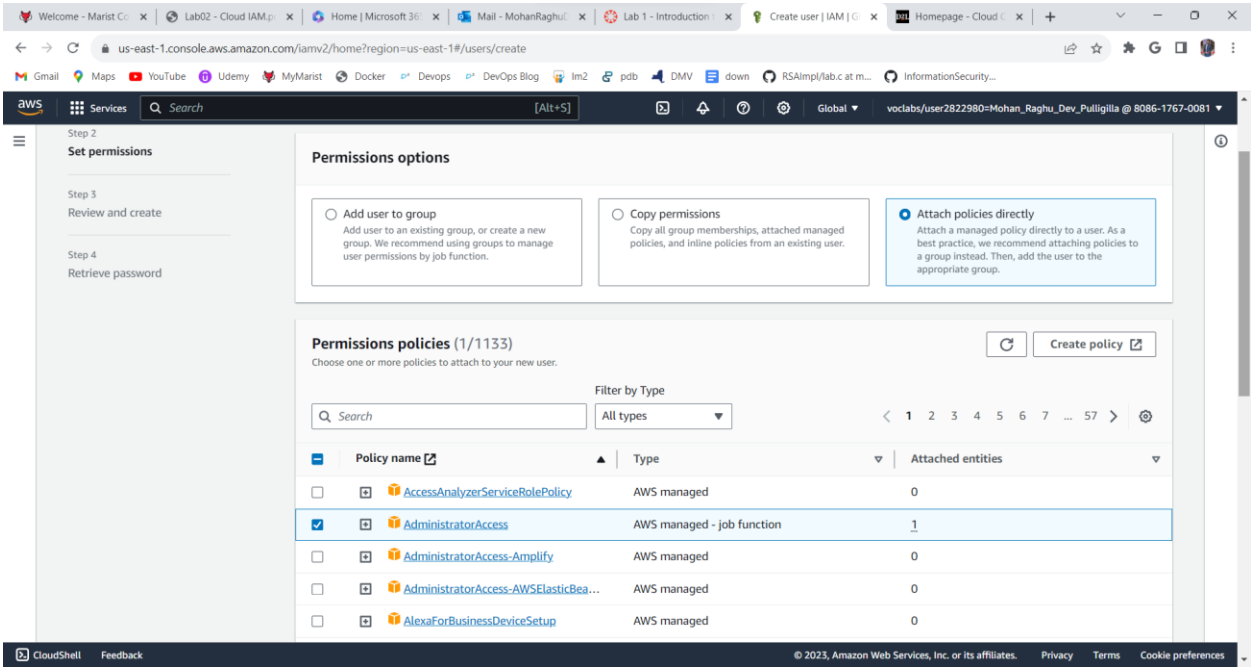


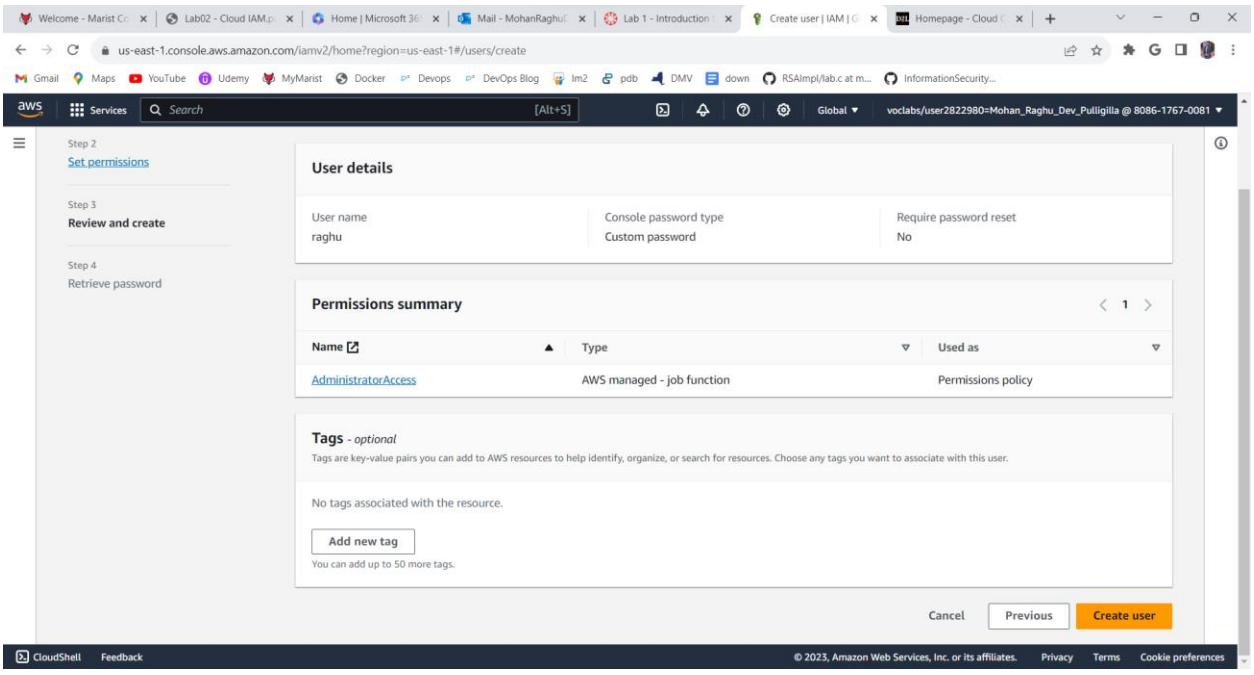
- I have tried to create the user when I have first logged into the AWS I have tried to create user with basic details . Then It showed user doesn't have access to create user.

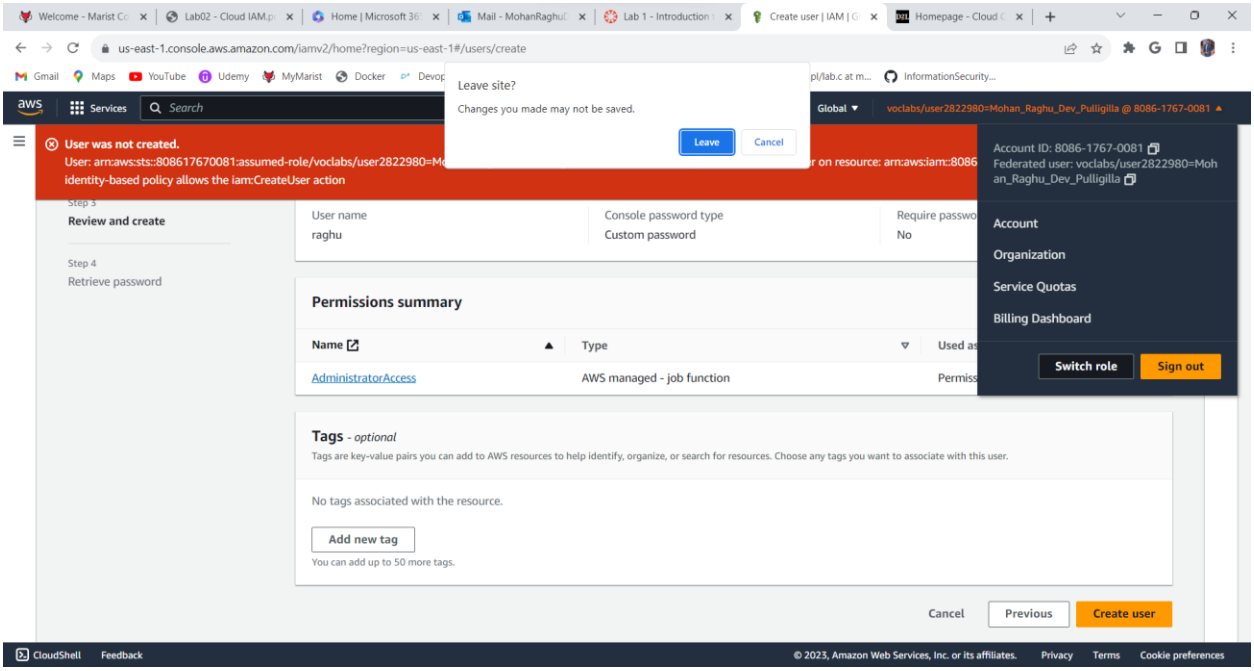


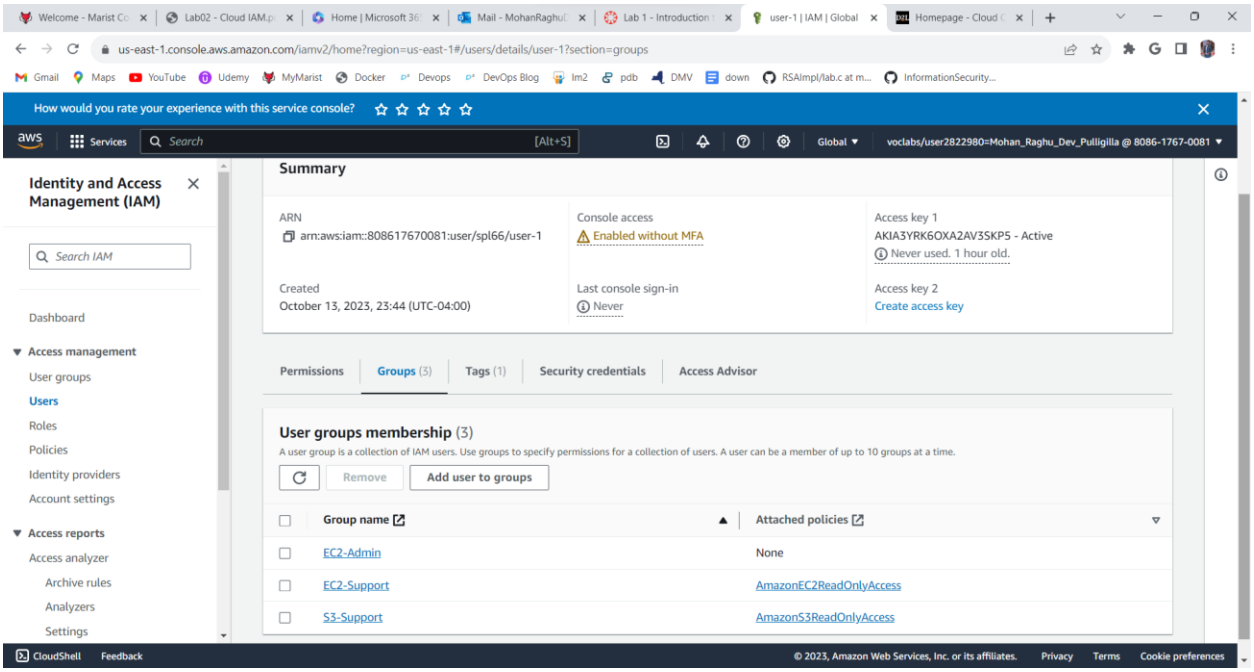

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/create
Services
Search
[Alt+S]
Global
voclabs/user2822980=Mohan_Raghu_Dev_Pulligilla @ 8086-1767-0081
Do you want to provide console access to a person?
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications. To do so, sign into the console by using the credentials of the management account in AWS Organizations, and then enable Identity Center. If you aren't the management account owner, contact the owner to perform this task.
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
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

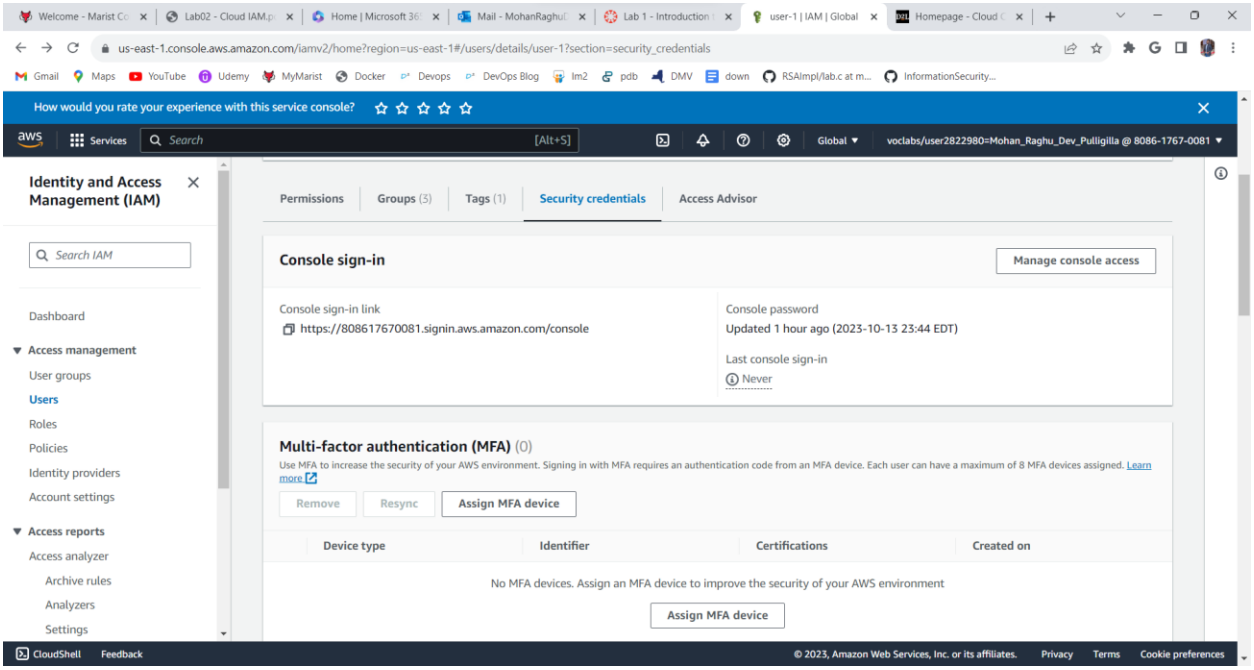

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/create
Services
Search
[Alt+S]
Global
voclabs/user2822980=Mohan_Raghu_Dev_Pulligilla @ 8086-1767-0081
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Permissions options
Add user to group
Add user to an existing 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.
Users (4)
Search
User name
Groups
Attached policies
awsstudent
None
User: arn:aws:sts::808617670081:assumed-role/vo
user-1
None
None
user-2
None
None
user-3
None
None
Set permissions boundary - optional
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

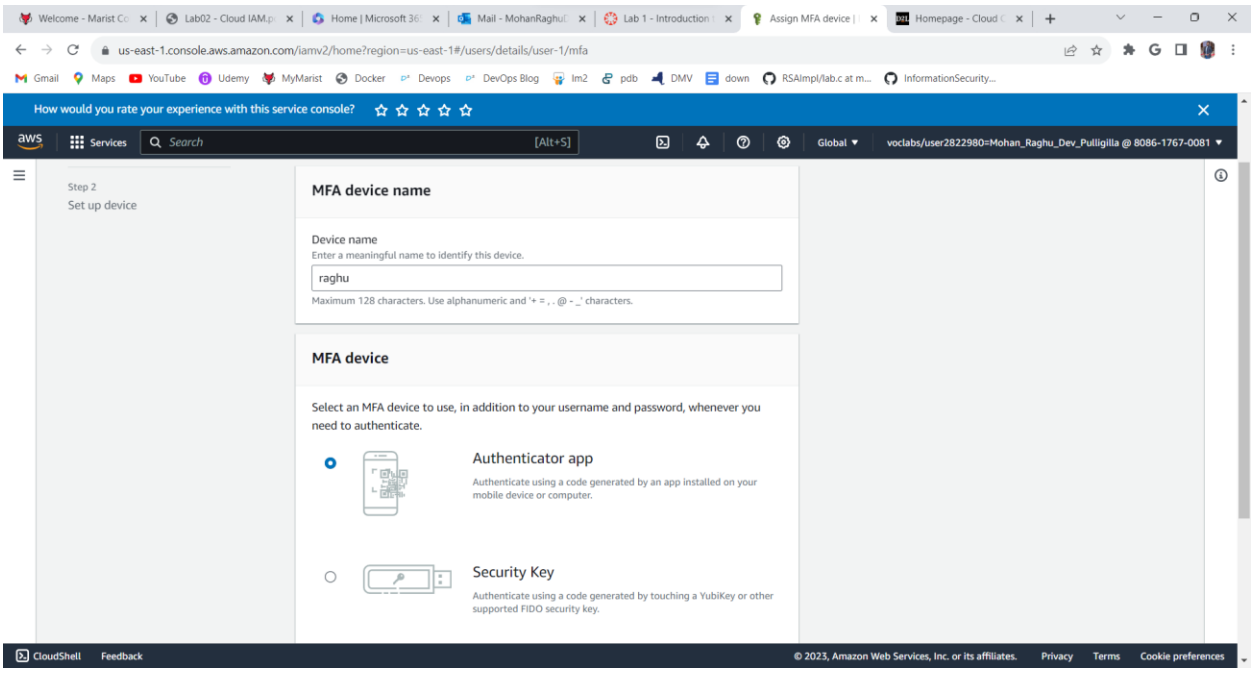

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/create
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
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.
Permissions policies (1/1133)
Choose one or more policies to attach to your new user.
Create policy
Filter by Type
Search
All types
Policy name
Type
Attached entities
AccessAnalyzerServiceRolePolicy
AWS managed
0
AdministratorAccess
AWS managed - job function
1
AdministratorAccess-Amplify
AWS managed
0
AdministratorAccess-AWSElasticBea...
AWS managed
0
AlexaForBusinessDeviceSetup
AWS managed
0
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

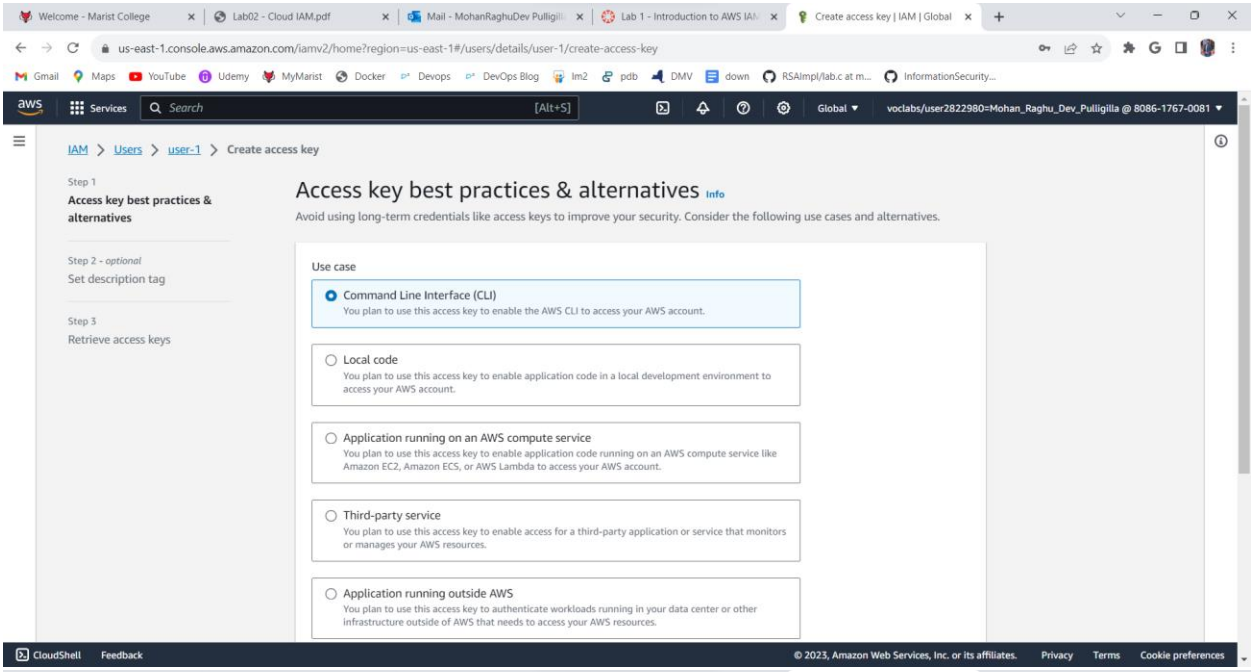

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/create
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
User details
User name
raghu
Console password type
Custom password
Require password reset
No
Permissions summary
Name
Type
Used as
AdministratorAccess
AWS managed - job function
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.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create user
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

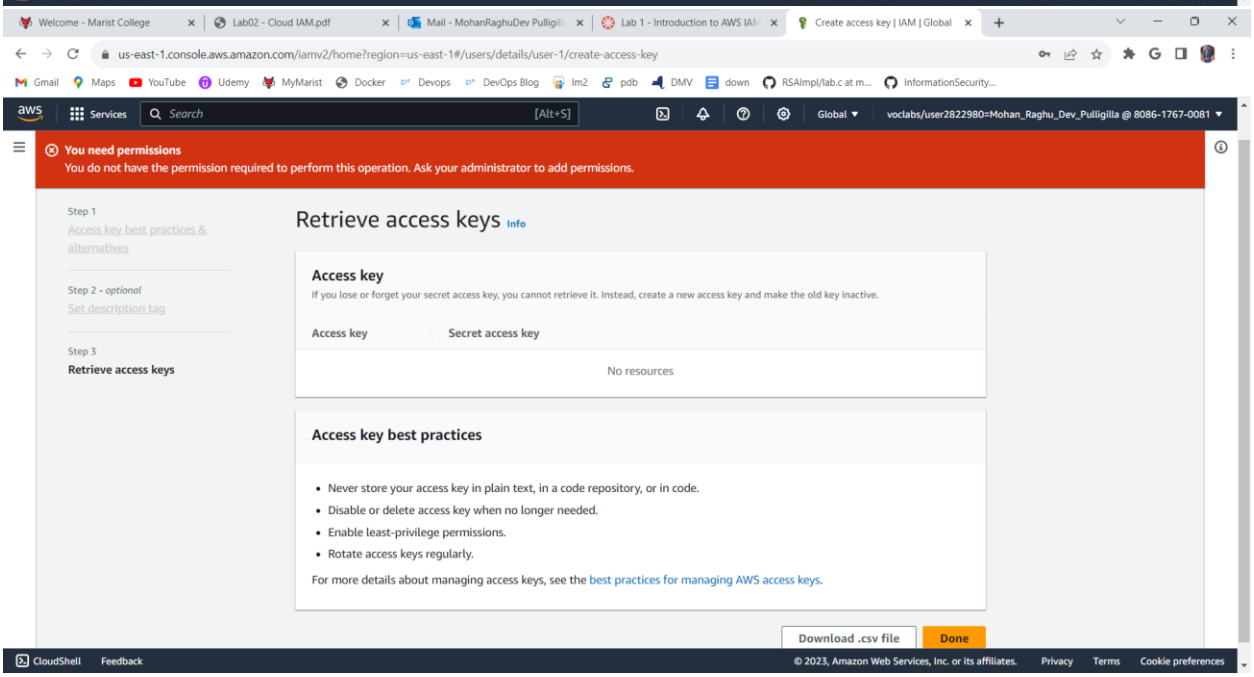

Leave site?
Changes you made may not be saved.
Leave
Cancel
User was not created.
identity-based policy allows the iam:CreateUser action
Step 3
Review and create
Step 4
Retrieve password
User name
raghu
Console password type
Custom password
Permissions summary
Name
Type
AdministratorAccess
AWS managed - job function
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.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create user
Account ID: 8086-1767-0081
Federated user: voclabs/user2822980=Mohan_Raghu_Dev_Pulligilla
Account
Organization
Service Quotas
Billing Dashboard
Switch role
Sign out
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


How would you rate your experience with this service console?
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Summary
ARN
arn:aws:iam::808617670081:user/spl66/user-1
Console access
Enabled without MFA
Access key 1
AKIA3YRK6OXA2AV3SKP5 - Active
Never used. 1 hour old.
Created
October 13, 2023, 23:44 (UTC-04:00)
Last console sign-in
Never
Access key 2
Create access key
Permissions
Groups (3)
Tags (1)
Security credentials
Access Advisor
User groups membership (3)
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.
Remove
Add user to groups
Group name
Attached policies
EC2-Admin
None
EC2-Support
AmazonEC2ReadOnlyAccess
S3-Support
AmazonS3ReadOnlyAccess
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


How would you rate your experience with this service console?
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Permissions
Groups (3)
Tags (1)
Security credentials
Access Advisor
Console sign-in
Manage console access
Console sign-in link
https://808617670081.signin.aws.amazon.com/console
Console password
Updated 1 hour ago (2023-10-13 23:44 EDT)
Last console sign-in
Never
Multi-factor authentication (MFA) (0)
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
Remove
Resync
Assign MFA device
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
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

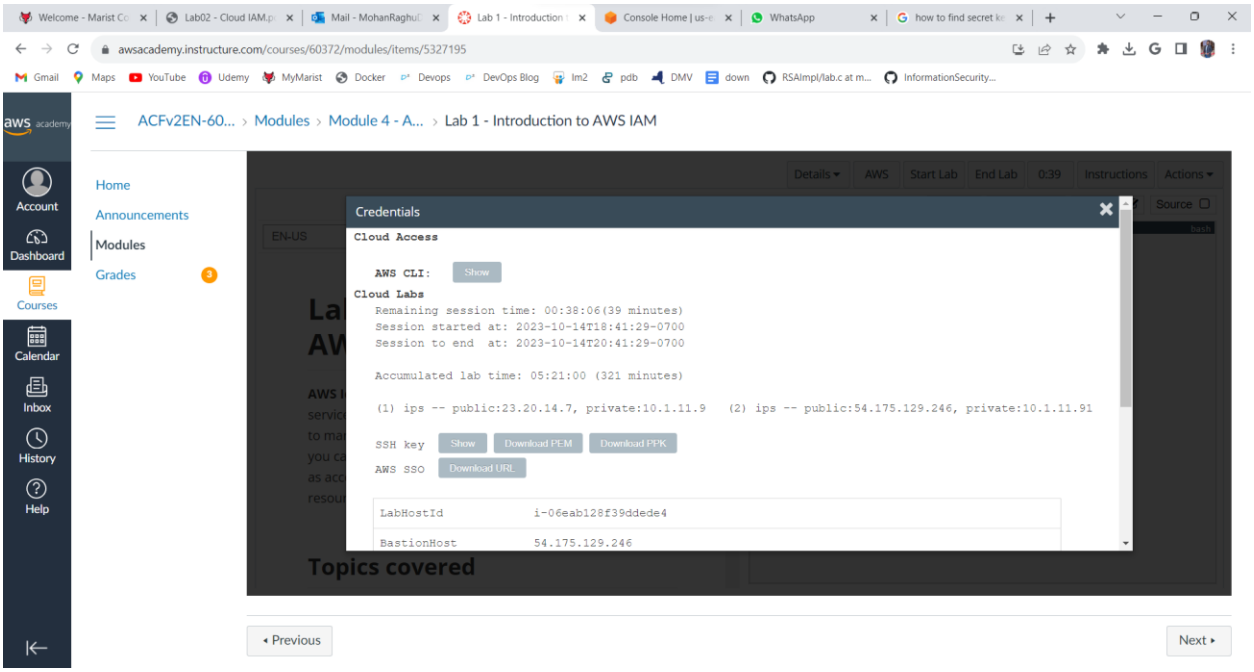

How would you rate your experience with this service console?
Step 2
Set up device
MFA device name
Device name
Enter a meaningful name to identify this device.
raghu
Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.
MFA device
Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.
Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.
Security Key
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

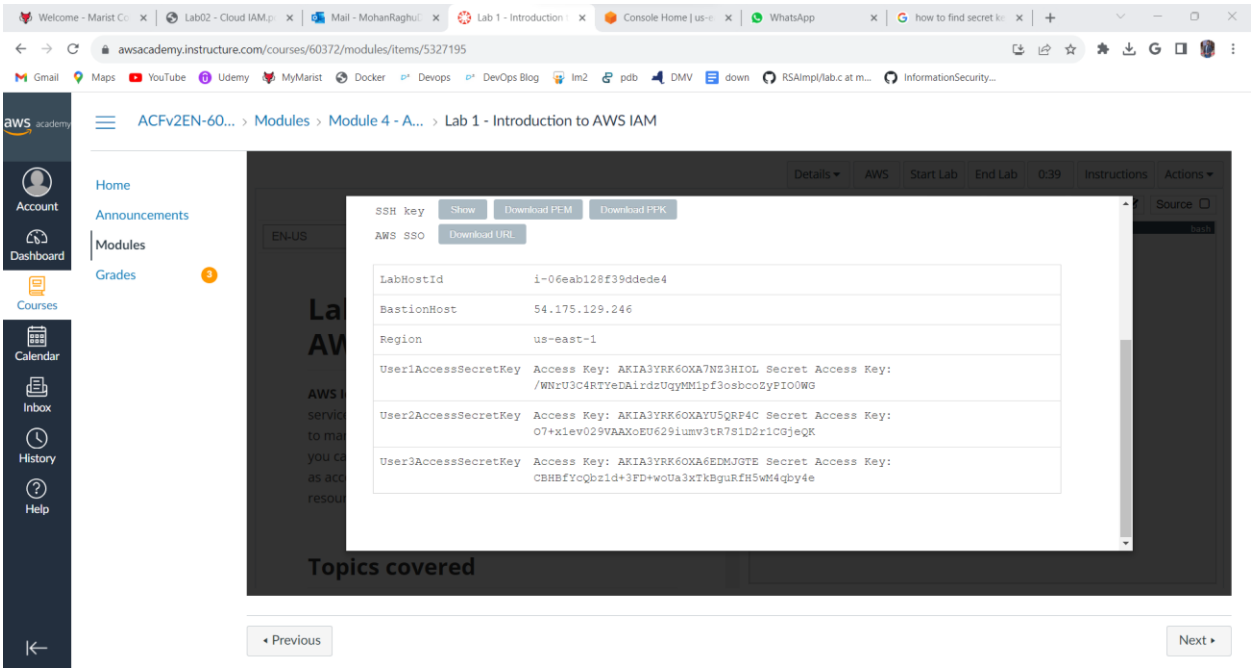

Welcome - Marist College
Lab02 - Cloud IAM.pdf
Mail - MohanRaghuDev Pulligilla
Lab 1 - Introduction to AWS IAM
Create access key | IAM | Global
us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/details/user-1/create-access-key
Gmail Maps YouTube Udemy MyMarist Docker Devops DevOps Blog Im2 pdb DMV down RSAImpl/lab.c at m... InformationSecurity...
aws Services Search [Alt+S] Global voclabs/user2822980=Mohan_Raghu_Dev_Pulligilla @ 8086-1767-0081
IAM > Users > user-1 > Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Access key best practices & alternatives Info
Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.
Use case
Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.
Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.
Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.
CloudShell Feedback
© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences


Welcome - Marist College
Lab02 - Cloud IAM.pdf
Mail - MohanRaghuDev Pulligilla
Lab 1 - Introduction to AWS IAM
Create access key | IAM | Global
us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/details/user-1/create-access-key
Gmail Maps YouTube Udemy MyMarist Docker Devops DevOps Blog Im2 pdb DMV down RSAImpl/lab.c at m... InformationSecurity...
aws Services Search [Alt+S] Global voclabs/user2822980=Mohan_Raghu_Dev_Pulligilla @ 8086-1767-0081
You need permissions
You do not have the permission required to perform this operation. Ask your administrator to add permissions.
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Retrieve access keys Info
Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.
Access key
Secret access key
No resources
Access key best practices
Never store your access key in plain text, in a code repository, or in code.
Disable or delete access key when no longer needed.
Enable least-privilege permissions.
Rotate access keys regularly.
For more details about managing access keys, see the best practices for managing AWS access keys.
Download .csv file
Done
CloudShell Feedback
© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

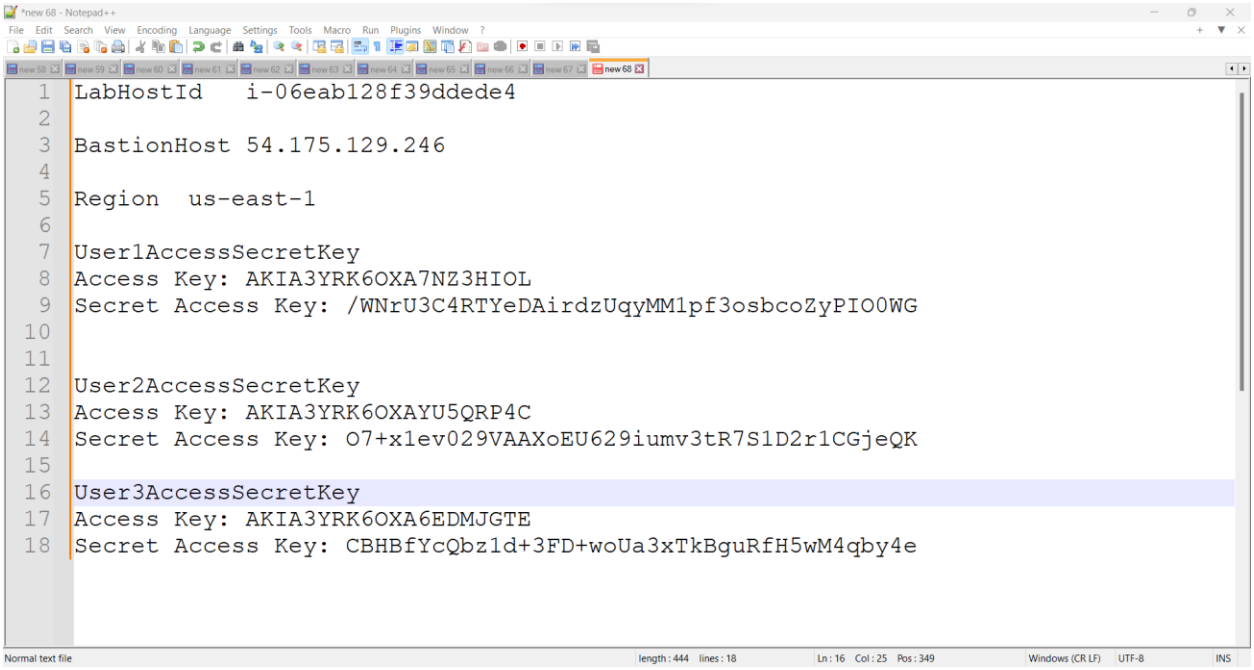
Task II:

- For Task II, check the user access key and secret key selecting details and then click on show. It will display all the details as shown in below screenshot.

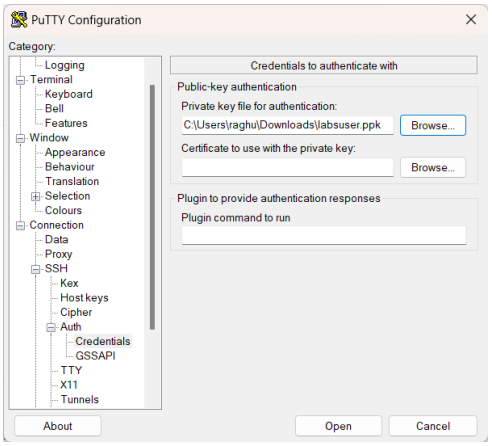




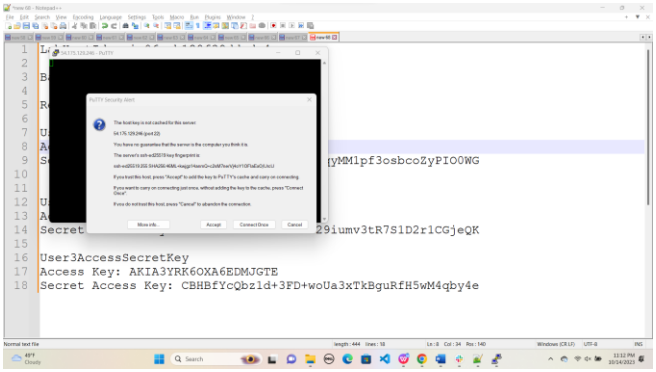
- Copied all the details into a note pad and download the ppk file to connect to the bastion node using putty.



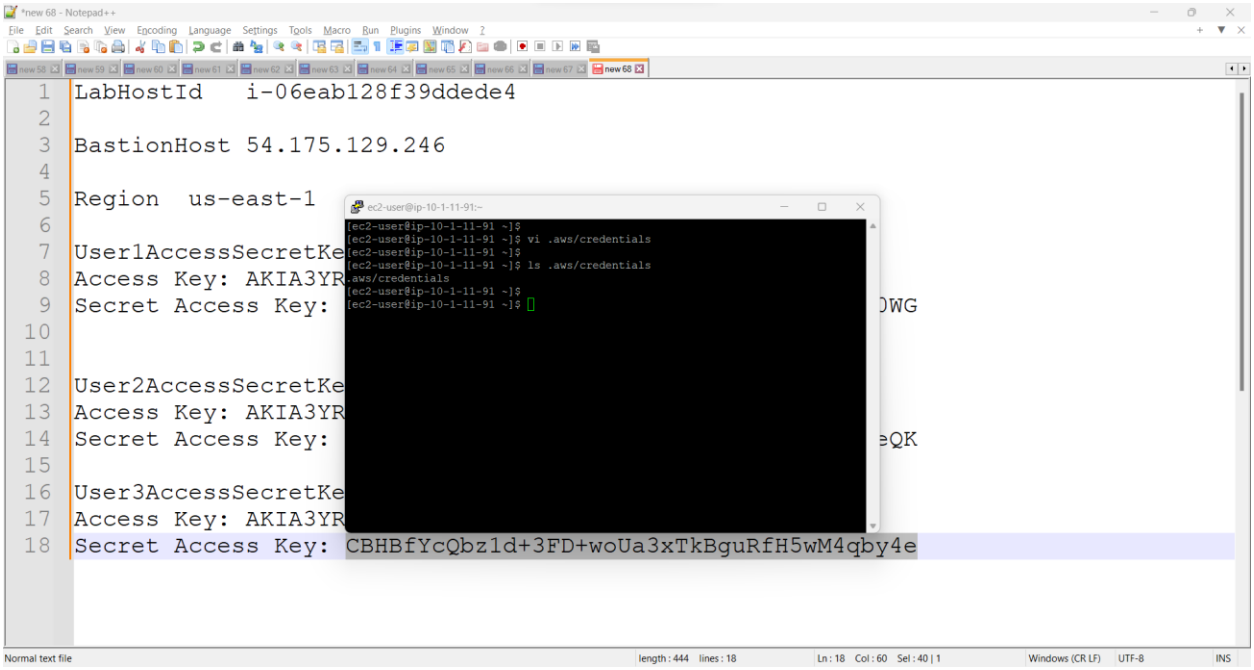
- After entering the bastion IP in connection and then select the ppk file and then click on open.



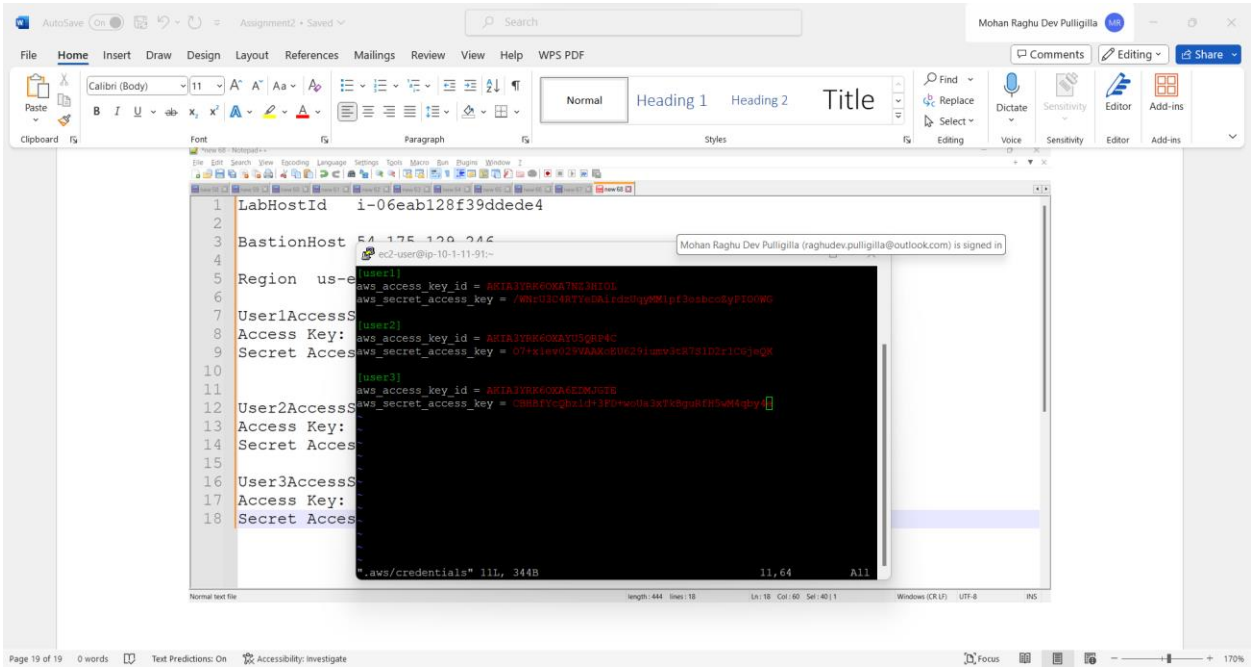
- Once we click on open then a pop will appear, then click on accept.



- Once login to the bastion configured AWS profile for user-1,user-2, user-3.

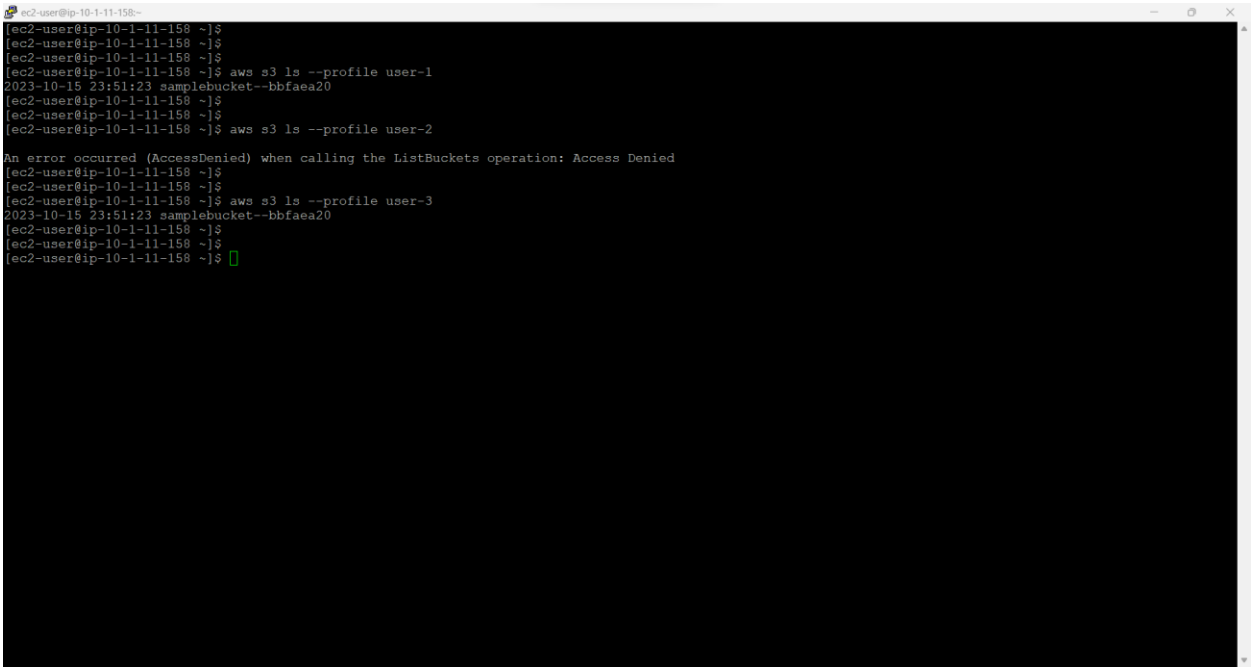


- Below screenshot shows the configuration of AWS profiles for user-1,user-2,user-3.

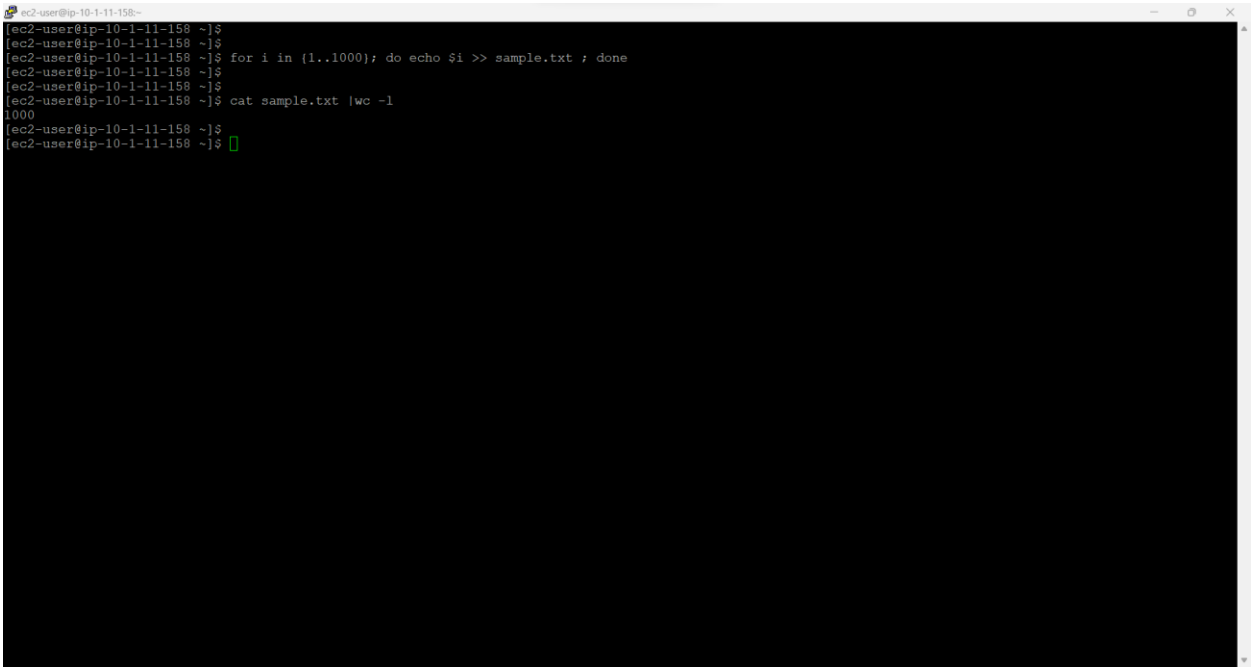


- After successful configuration of profile checking the users access on few AWS services.
- Below screenshot show that we have performed list S3 bucket with 3 users.
- User-1 and user-3 has read access to S3 buckets so that it showing list of buckets.

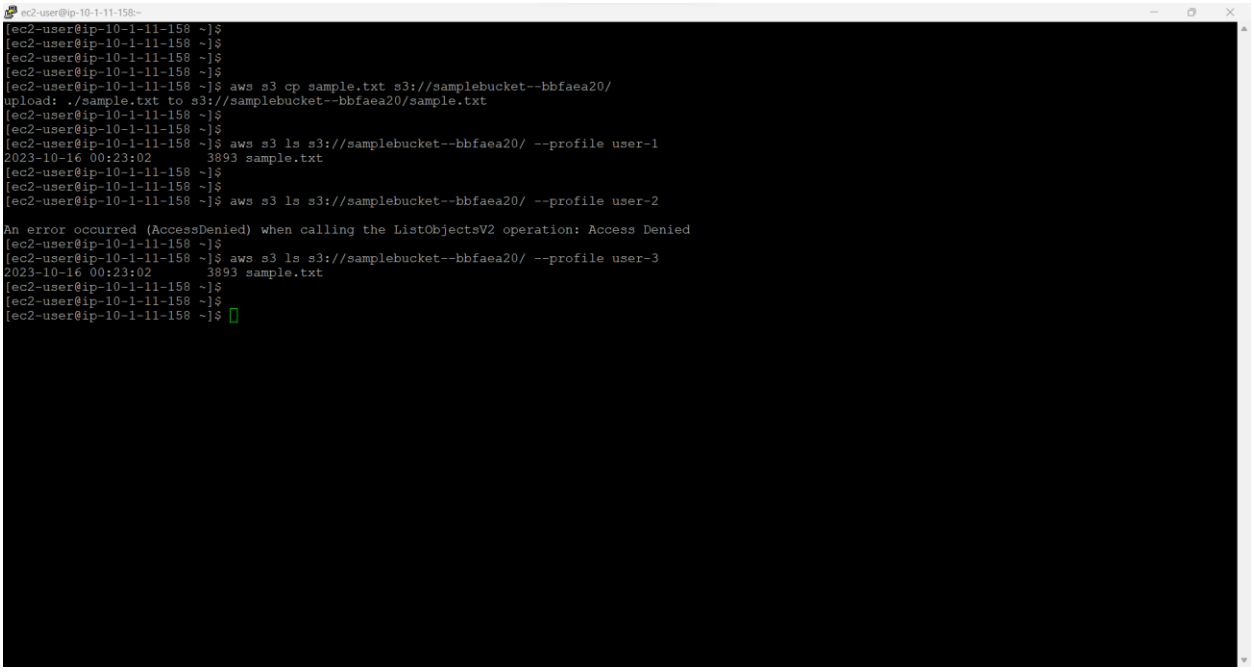
- User-2 has only read access to EC2. That why access denied for user-2.



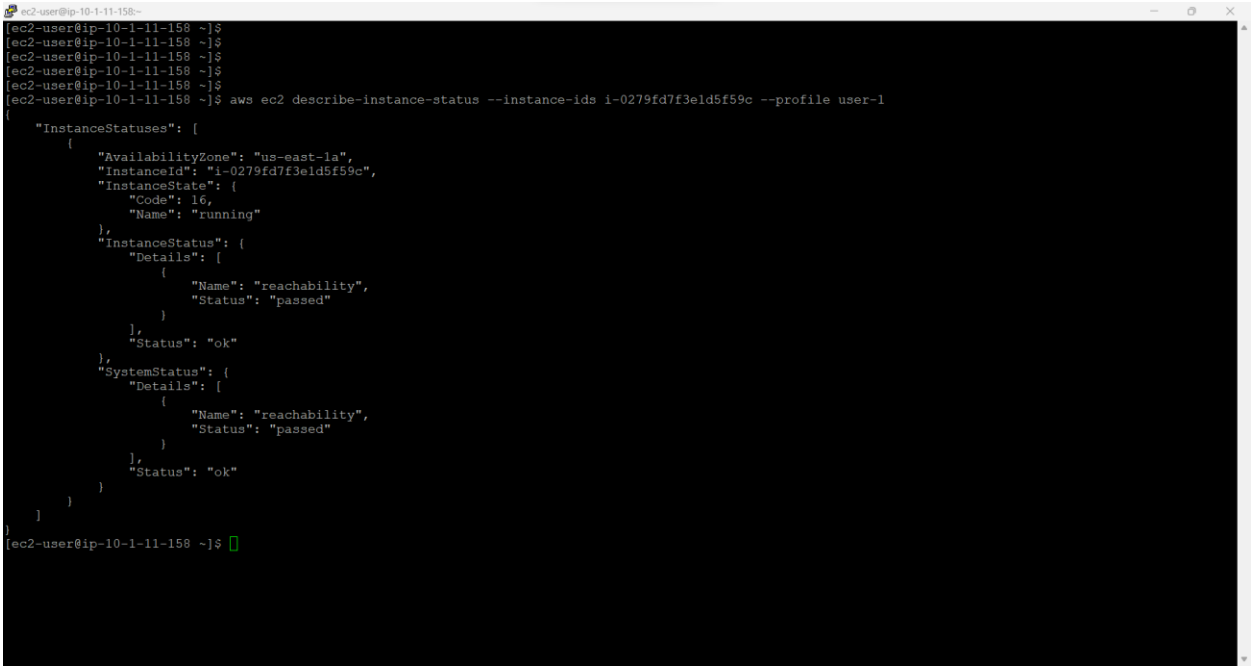
- I have created a sample.txt with 100- lines in it using for loop to insert data in it.



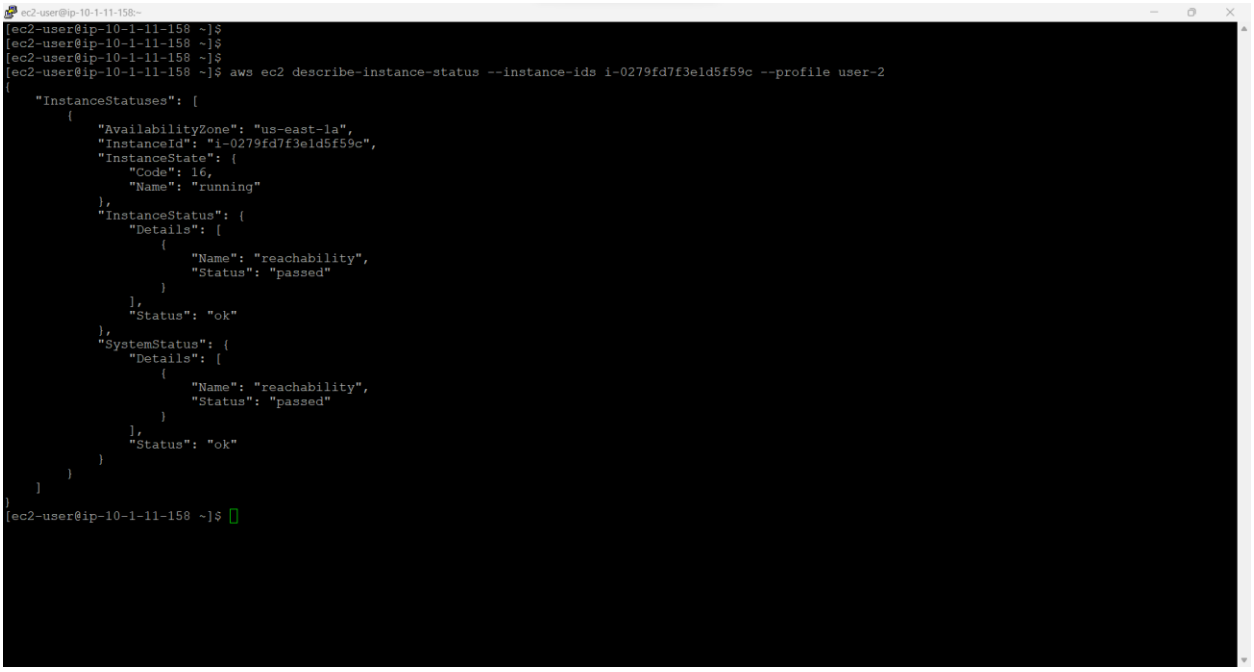
- Once the sample.txt is created tried to upload it to S3 bucket with user-1 and user-3 , it denied because both users have read only access.
- So uploaded the file to S3 bucket with default user and it was successful.
- The tries to list the objects in the bucket with user-1 and user-3 it was successful.



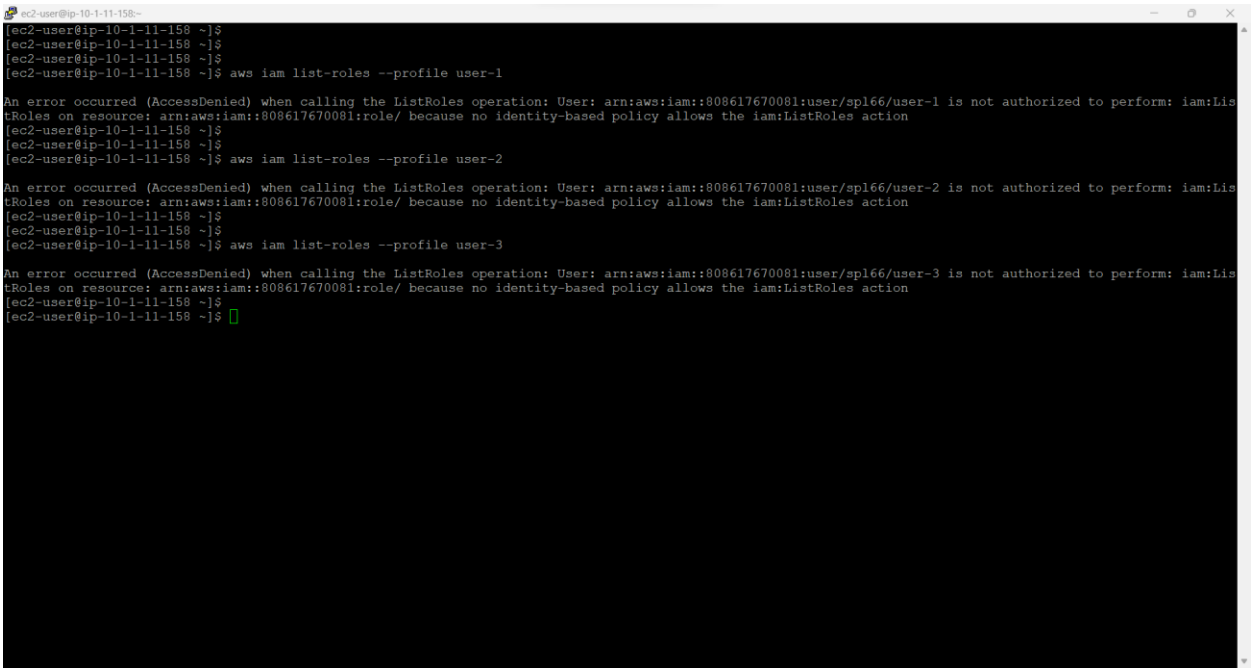
- User-1 has full access to EC2 so tried to describe an instance. Below is screenshot showing successful result of it.



- Tried to describe instance with user-2 as it has EC2 read access, below screenshot shows successful result of it.



- Tried to list IAM roles with user-1, user-2,user-3 as it doesn't have any access to IAM its access denies, below screenshot shows the result of it.



- Tried the same list roles with default user then it was successful, below screenshot shows the result of it

Conclusion:

In this Lab I have worked on AWS IAM service which is Identity Access Management. I have worked on assigning the groups to the users and verified them using the Aws management console and AWS CLI. With the pre created user tried the access to specific services it worked for the services for which user has access to it, and access was denied for the services where users doesn't have access to it. So that we can conclude that a user created in IAM has not access to every service, but they have access to the services which we have provided to them. We can limit the access to the users by adding policies, groups, or roles.