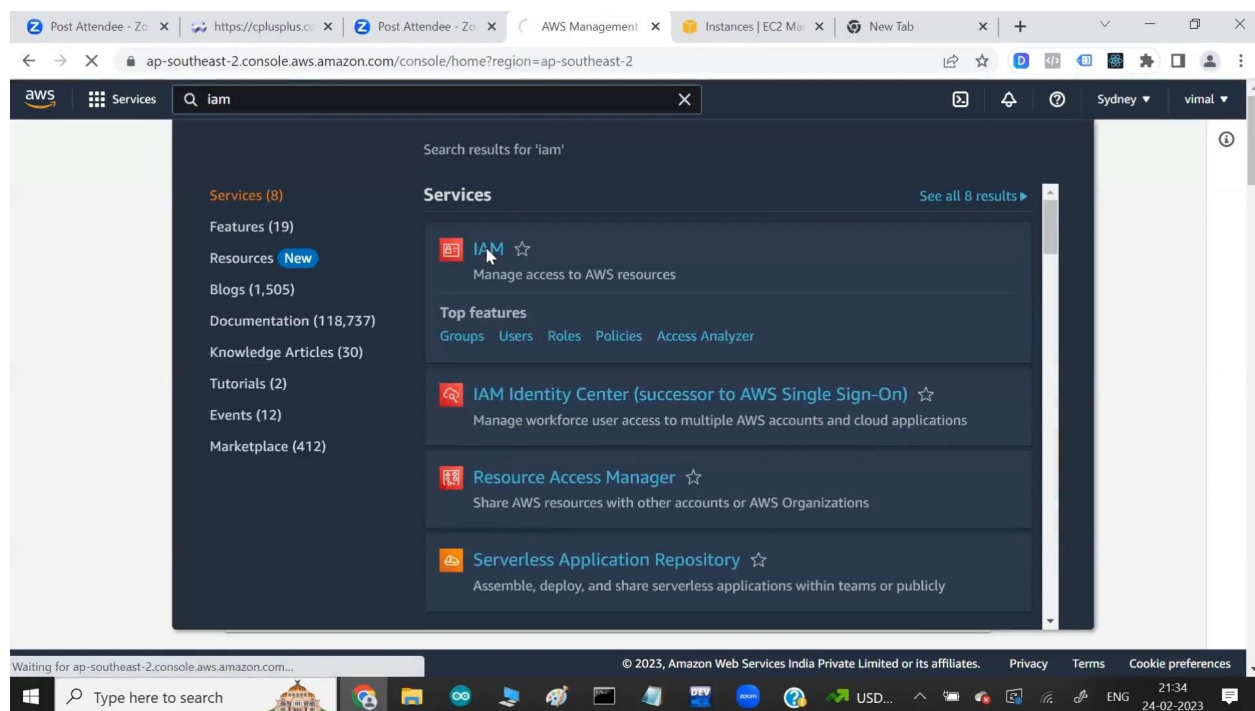


AWS Session 6

Summary – 24-02-2023



- If we want to keep monitoring your physical resources then we have service available in AWS called **Cloud Watch**.
 - How much memory is utilize?, How much CPU is used?, How much Network Bandwidth is used?, How much data is transferred from internet to instance? All of this terms are known as **Metrics**. Cloud watch give you way to monitor multiple Metrics.
 - IAM stands for Identity Access Management.
 - IAM allows you to manage users and their level of access to the aws console.
 - With the help of IAM if you want to give limited power to user you can use this service.
-
- Search IAM in the search option:



- Click on the users:

The screenshot shows the AWS IAM dashboard in the us-east-1 region. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Analyzers. The 'Users' link under Access management is highlighted. The main content area displays the 'IAM dashboard' with 'Security recommendations' for the root user, including 'Add MFA for root user' and 'Update your access permissions for AWS Billing, Cost Management, and Account consoles'. The right sidebar shows 'AWS Account' details like Account ID, Alias, and Sign-in URL, along with 'Quick Links' for security credentials.

- Give the user details which you want to create:

The screenshot shows the 'Specify user details' page in the AWS IAM console. The breadcrumb trail indicates the path: IAM > Users > Create user. The page is divided into three steps: 'Specify user details' (current), 'Set permissions', and 'Review and create'. The 'User details' section contains a 'User name' field with the value 'tom' and a checkbox for 'Provide user access to the AWS Management Console - optional'. A blue information box at the bottom provides guidance on creating programmatic access. The 'Next' button is highlighted in orange.

- Click on the provide access to the AWS Management Console , this will give user access to access the AWS console:

us-east-1.console.aws.amazon.com/iamv2/home?region=ap-southeast-2#/users/create

Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

User details

User name
tom

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

☒ 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.

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](#)

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

- Click on i want tot create IAM user:

us-east-1.console.aws.amazon.com/iamv2/home?region=ap-southeast-2#/users/create

Specify user details

Step 3
Review and create

Step 4
Retrieve password

User details

User name
tom

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Are you providing console access to a person?

☐ 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

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

- Type the password:

us-east-1.console.aws.amazon.com/iamv2/home?region=ap-southeast-2#/users/create

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

- Click on user must create a new password at next sign-in , after login in the user will get the option on the screen to reset the password.

us-east-1.console.aws.amazon.com/iamv2/home?region=ap-southeast-2#/users/create

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

- Click on next:

us-east-1.console.aws.amazon.com/iamv2/home?region=ap-southeast-2#/users/create

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: ! @ # \$ % ^ & * () _ + - [] { } | ' "

☐ 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

- Set the permissions on the user , What user can access, what should the user read etc.

us-east-1.console.aws.amazon.com/iamv2/home?region=ap-southeast-2#/users/create

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.

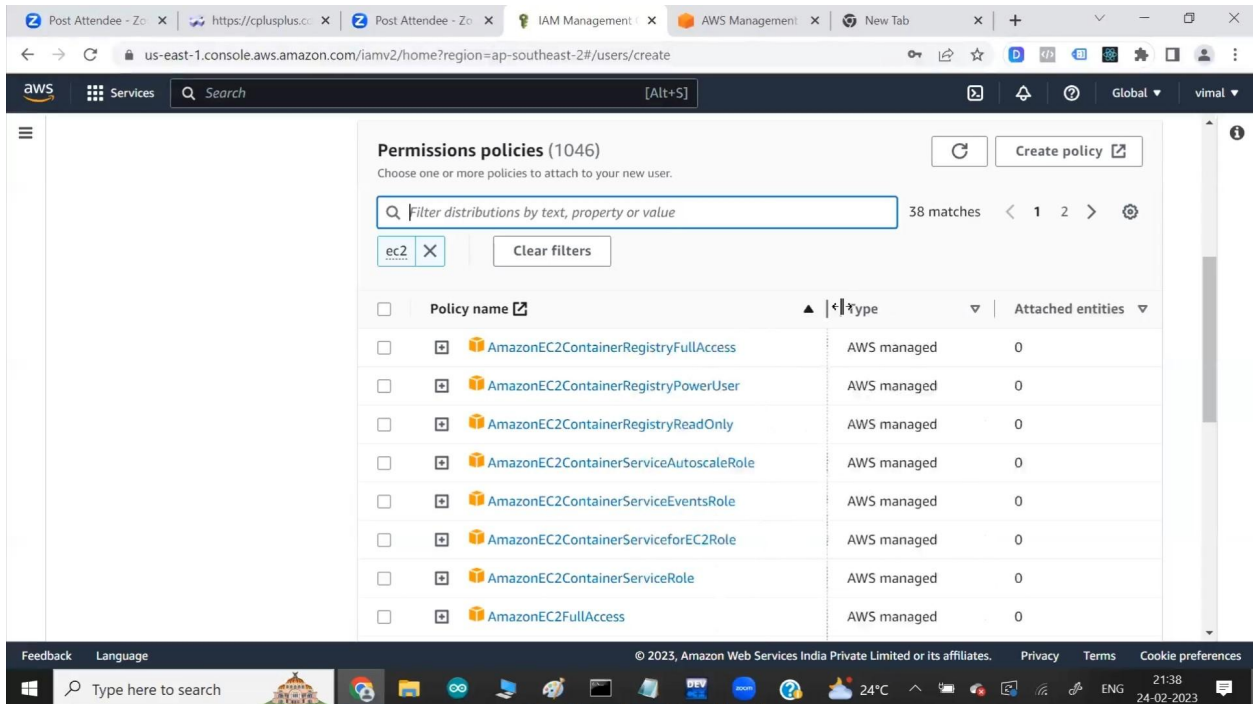
Permissions policies (1046)
Choose one or more policies to attach to your new user.

Filter distributions by text, property or value

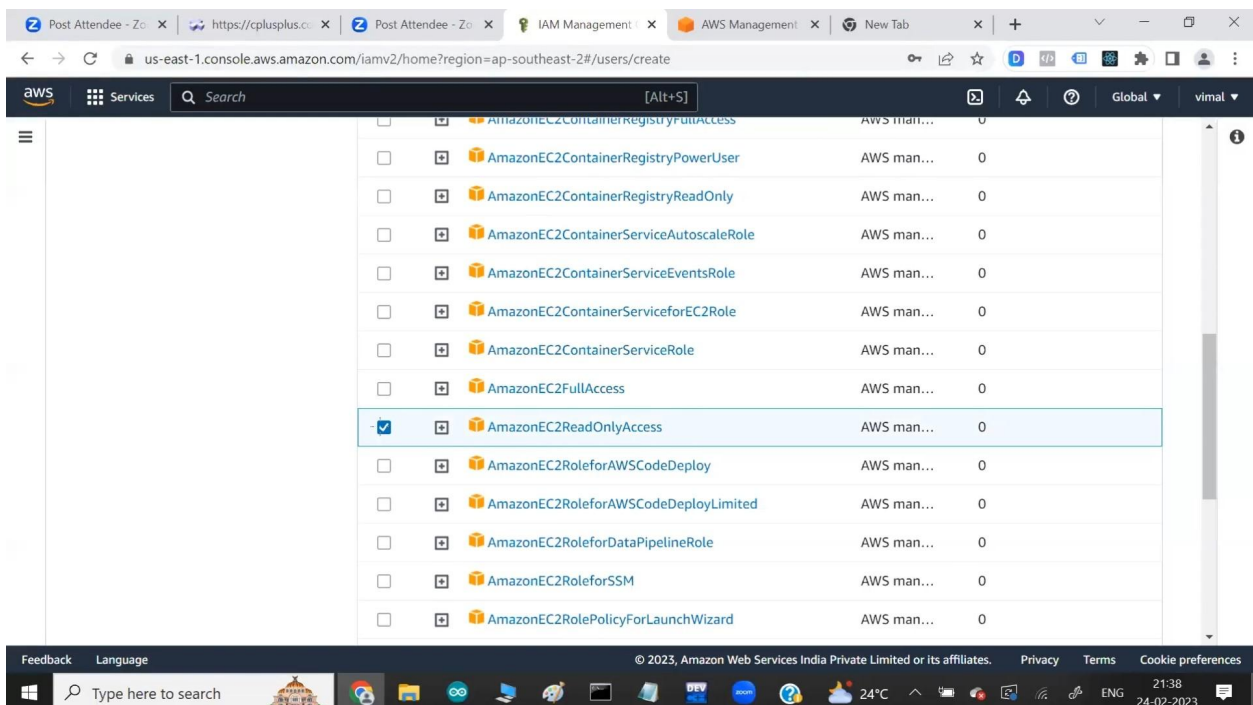
1 2 3 4 5 6 7 ... 53

Policy name	Type	Attached entities
-------------	------	-------------------

- Search the service which you want to give access to the user , here in this case we are search for EC2 service.



- Here we have selected readonly access in which user cannot create the files or update the files . User will only be able to read the files.



- After clicking on next , you will get the summary of the user and the permissions given.

The screenshot shows the AWS IAM console interface. The breadcrumb navigation is IAM > Users > Create user. The left sidebar shows the progress: Step 1 Specify user details, Step 2 Set permissions, Step 3 Review and create (active), and Step 4 Retrieve password. The main content area is titled 'Review and create' with a subtitle 'Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.'

User details

User name tom	Console password type Custom password	Require password reset Yes
------------------	--	-------------------------------

Permissions summary

Name	Type	Used as
AmazonEC2ReadOnlyAccess	AWS managed	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

- Click on Create user and the user will be created:

This screenshot shows the same 'Review and create' step as the previous one, but with additional sections visible at the bottom. The 'Permissions summary' table remains the same.

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.

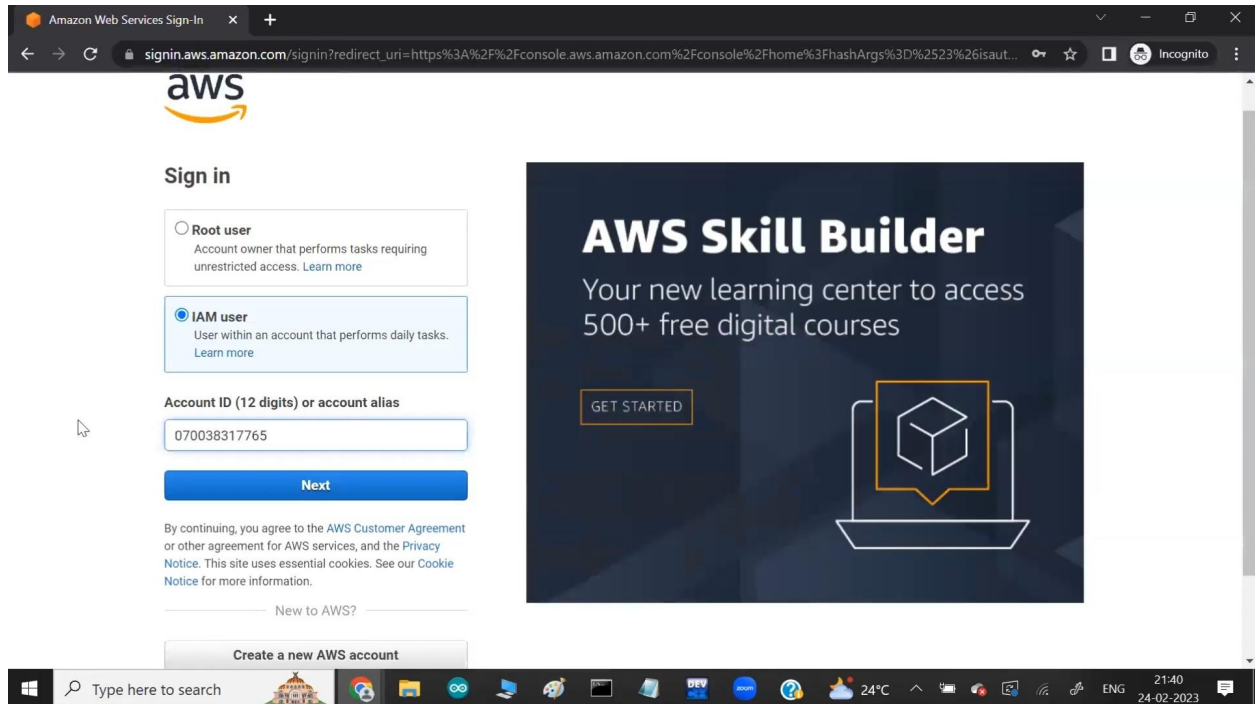
No tags associated with the resource.

[Add new tag](#)

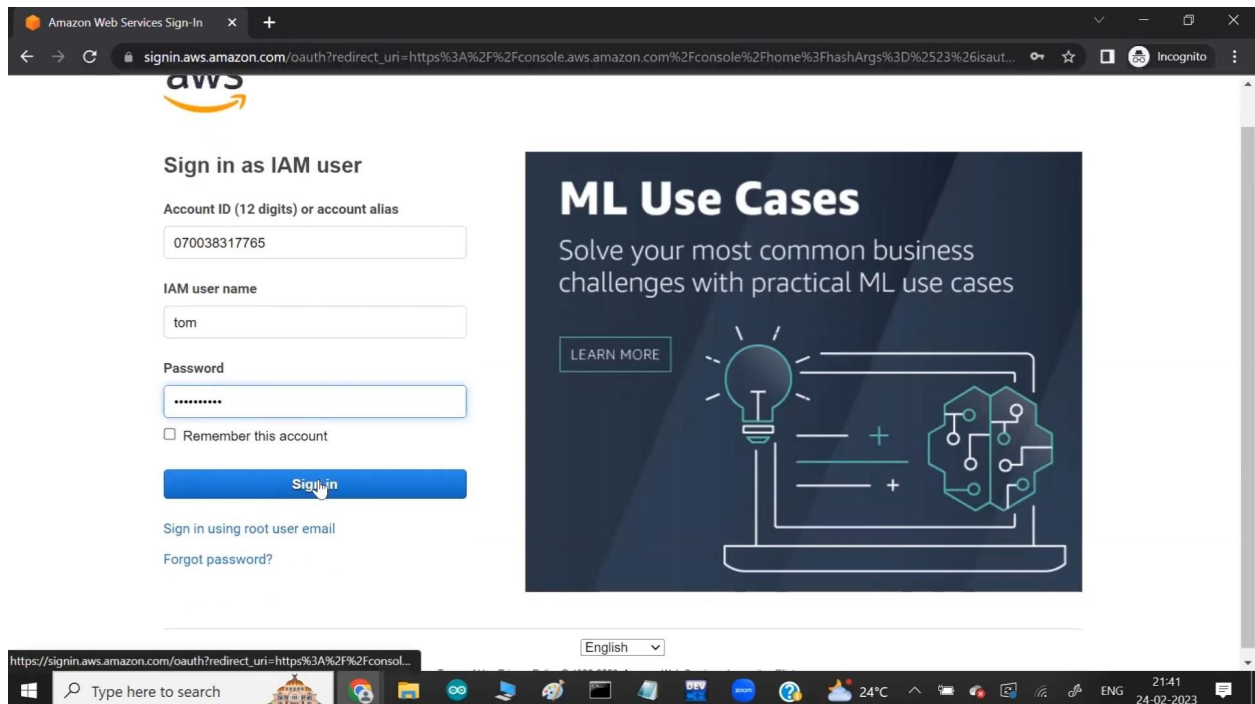
You can add up to 50 more tags.

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create user' (which is highlighted in orange and has a mouse cursor over it).

- Click on the IAM user and provide the id of the ROOT account because IAM user is the sub account of the root user.



- Provide the details and click on sign in:



- Reset the password and click on confirm:

The screenshot shows the AWS Sign-In page in a web browser. The URL is `signin.aws.amazon.com/clm?action=changepassword&userType=iam&redirect_uri=https%3A%2F%2Fconsole.aws.amazon.com%2Fconsole%2F...`. The page displays the AWS logo and a message: "You must change your password to continue". Below this, the following information is shown:

- AWS account:** 070038317765
- IAM user name:** tom
- Old password:** [input field]
- New password:** [input field]
- Retype new password:** [input field]

A blue button labeled "Confirm password change" is located below the password fields. Below the button is a link: "Sign in using root user email". At the bottom of the page, there is a language dropdown menu set to "English" and a footer with "Terms of Use" and "Privacy Policy" links, along with copyright information: "© 1996-2023, Amazon Web Services, Inc. or its affiliates.".

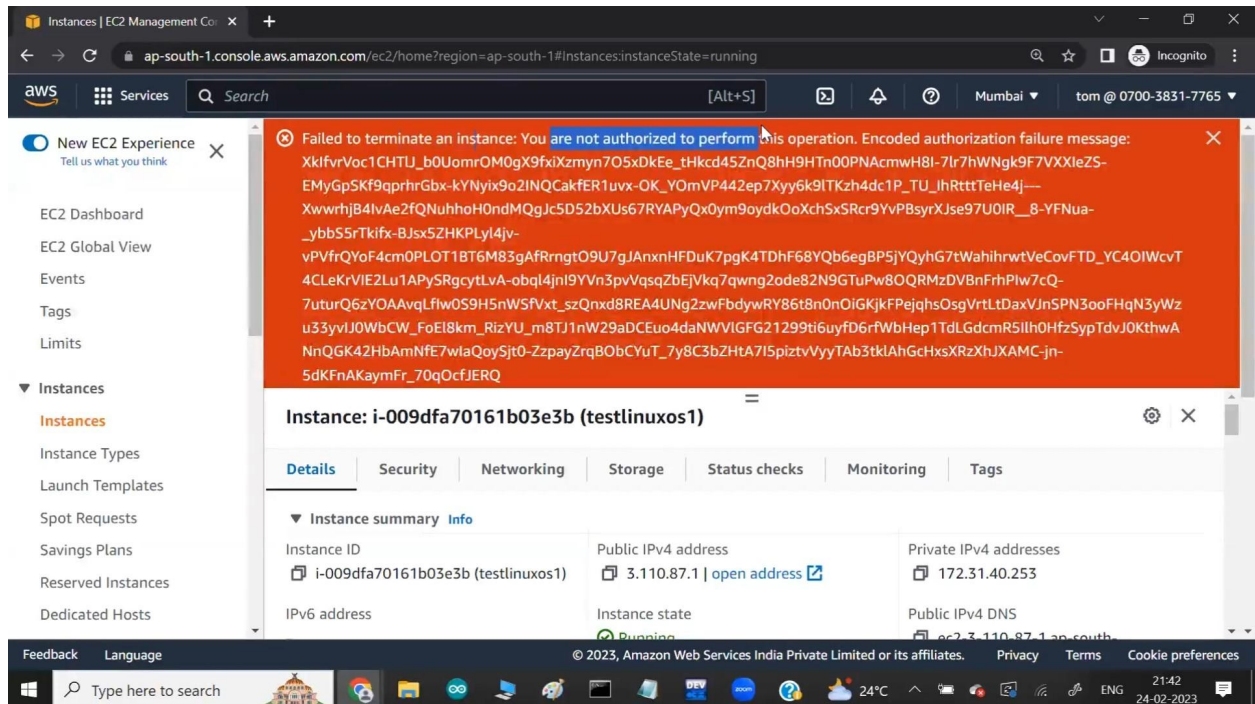
- You can the the IAM user created in the top right corner:

The screenshot shows the AWS Management Console in a web browser. The URL is `ap-northeast-1.console.aws.amazon.com/console/home?region=ap-northeast-1#`. The page displays the "Console Home" section with a "Reset to default layout" button and an "Add widget" button. Below this, there is a "Recently visited" section with a message: "No recently visited services". Below this, there is a section titled "Explore one of these commonly visited AWS services." with links to IAM, EC2, S3, RDS, and Lambda. At the bottom of the page, there is a footer with "Feedback", "Language", and copyright information: "© 2023, Amazon Web Services India Private Limited or its affiliates.".

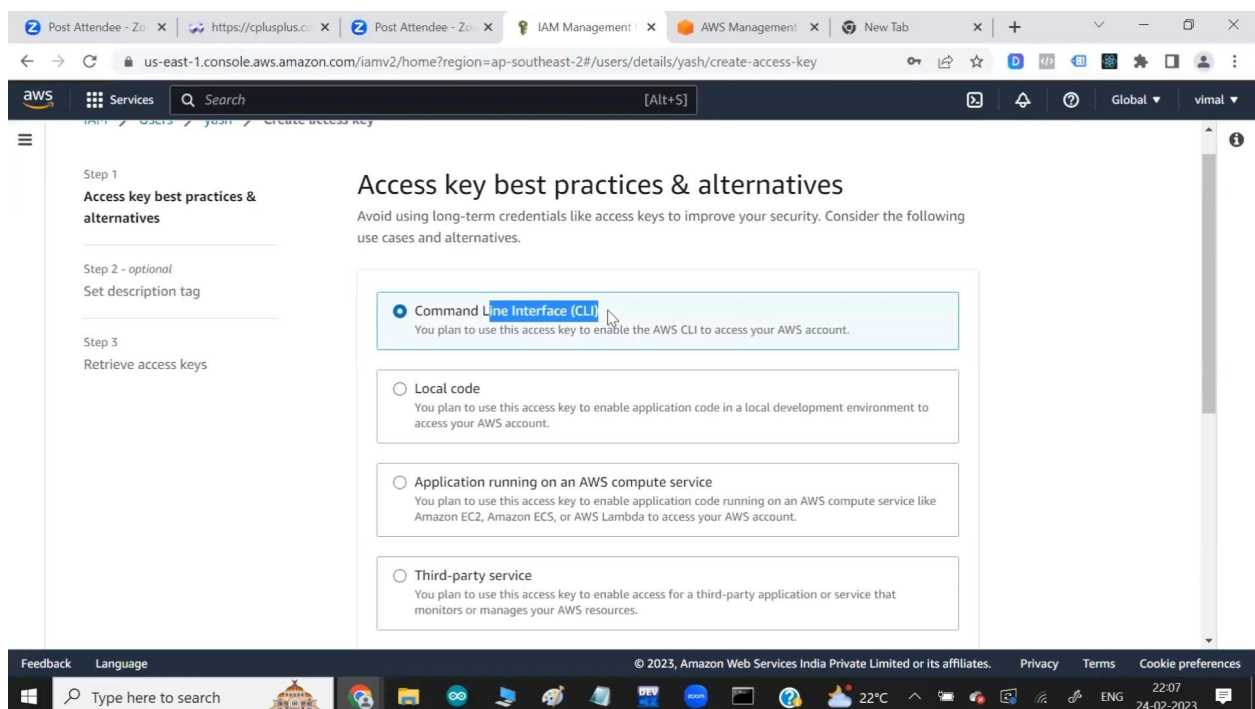
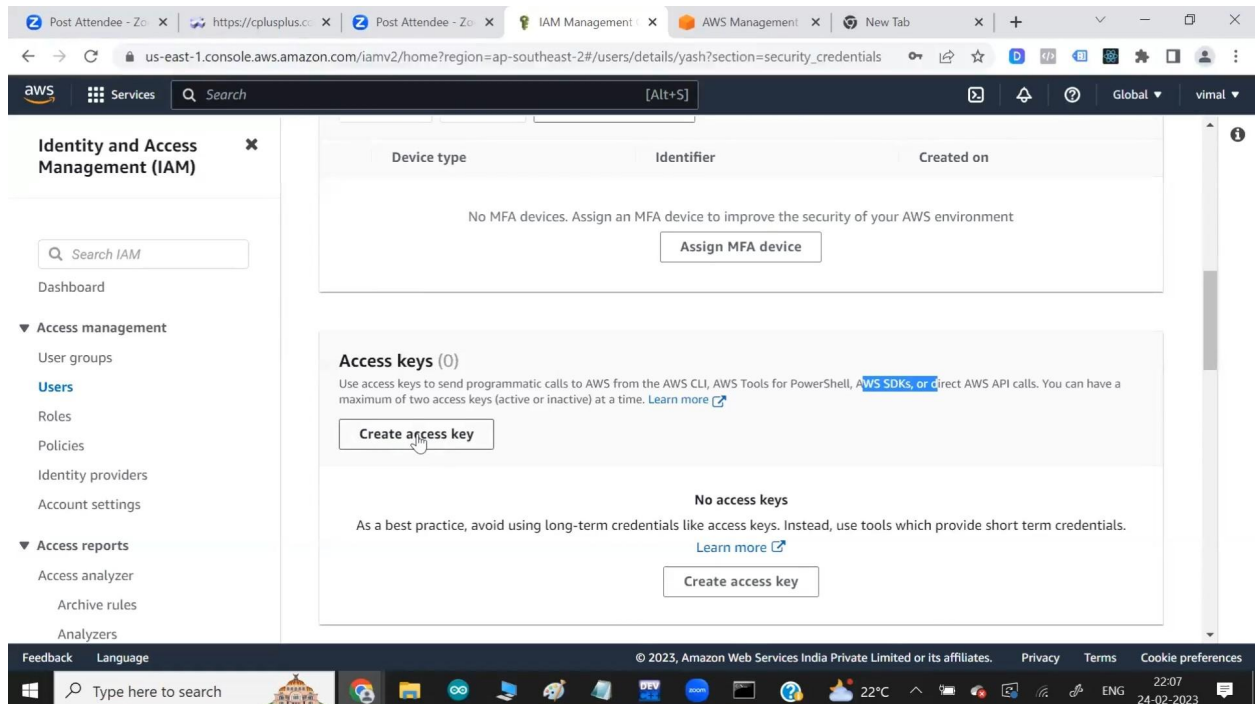
In the top right corner, a dropdown menu is open, showing the following options:

- Account ID: 0700-3831-7765
- IAM user: tom
- Account
- Organization
- Service Quotas
- Billing Dashboard
- Security credentials
- Settings
- Switch role
- Sign out

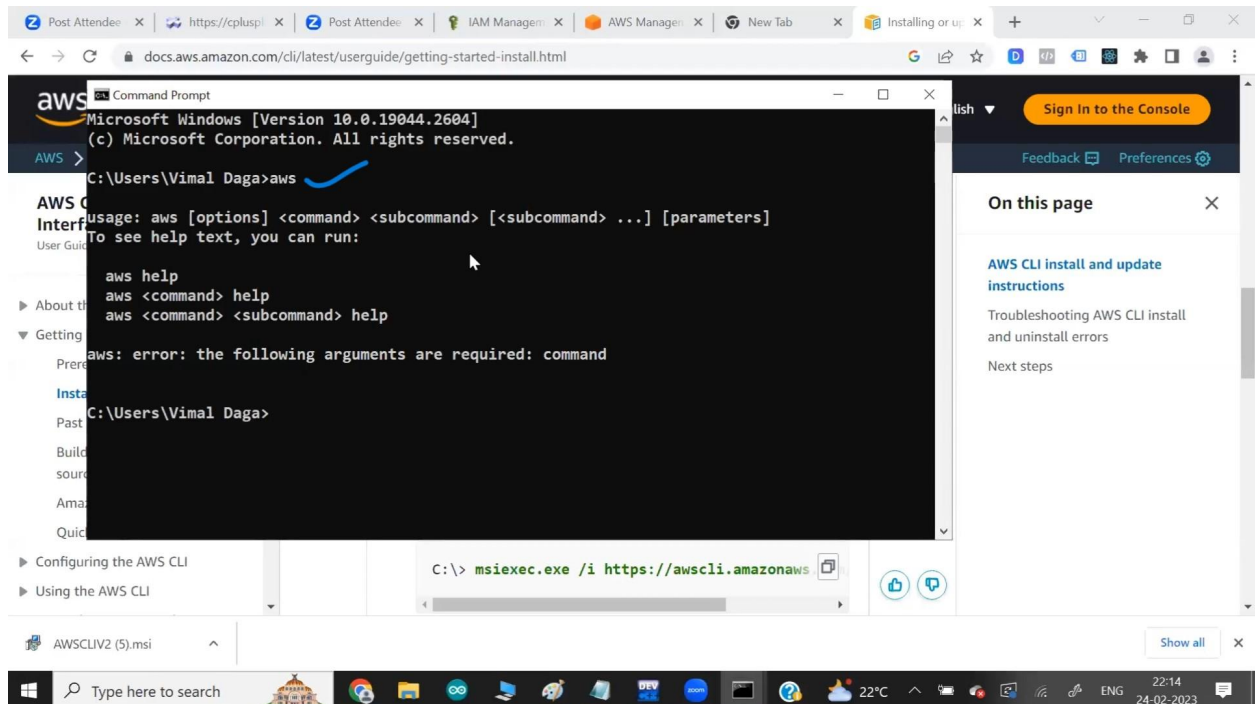
- As this user has only read power in ec2 service other than this if the user tries to do anything, for example:- user tries to terminated the created instance it will prompt on the screen access denied.



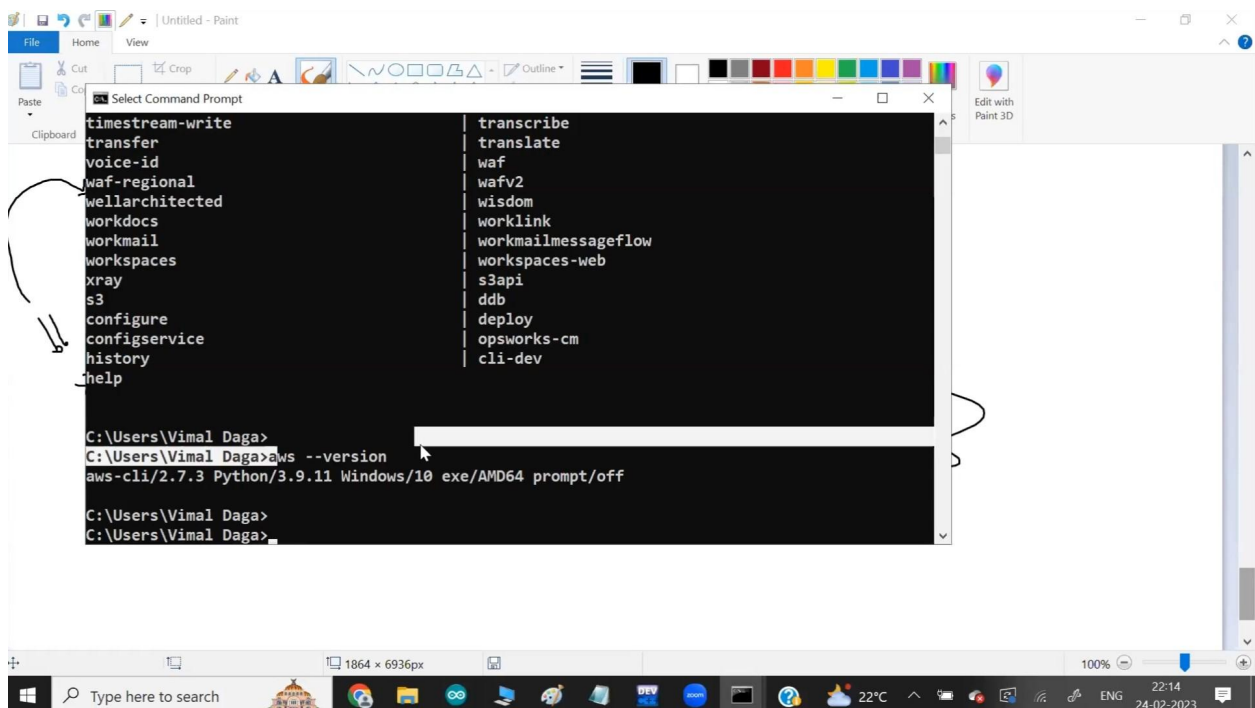
- You can also create the user and give the full access.
- You can use all the AWS services with the
 - Console (WebUI)
 - Command line Interface(CLI).
 - API
- When user wants to login as human beign user logs in with the help of username and password.
- When user wants to login programmatically, user need access key and secret key to login.



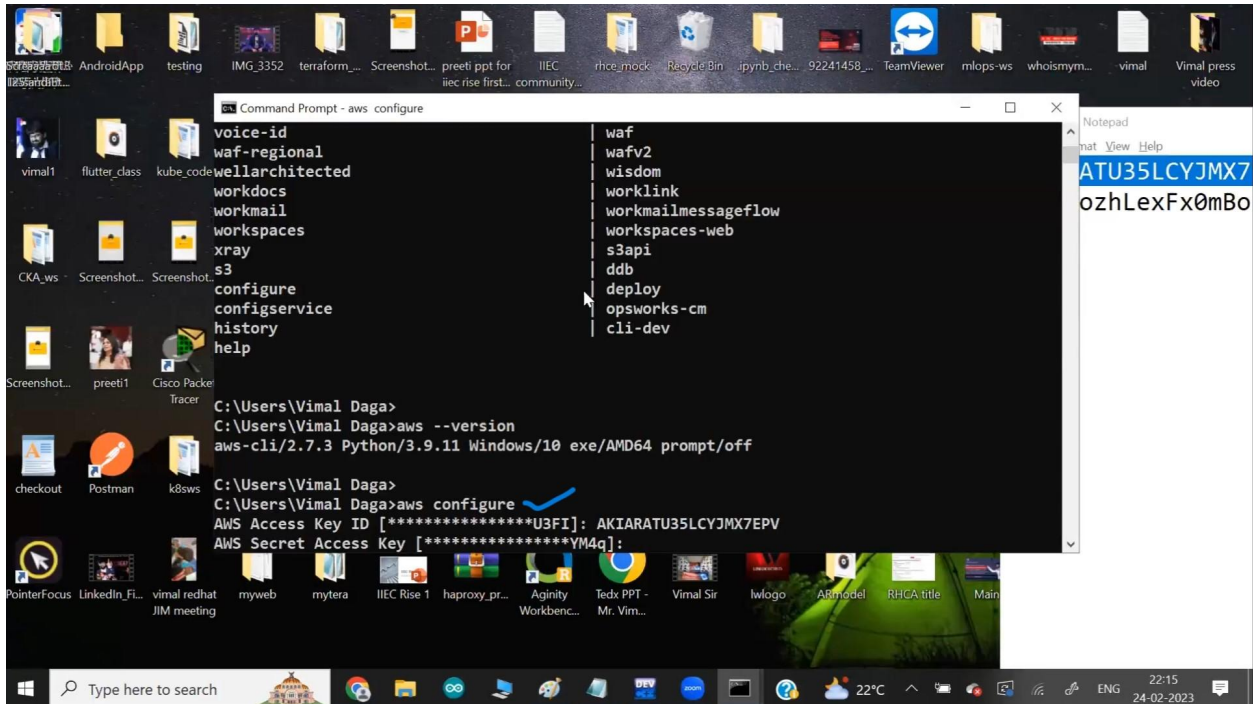
- To login via CLI you need to download AWS CLI.
- Link to Download AWS CLI :- <https://awscli.amazonaws.com/AWSCLIV2.msi>
- Install the software.
- Open your command prompt and type **aws** you will see the aws cli has downloaded and installed.



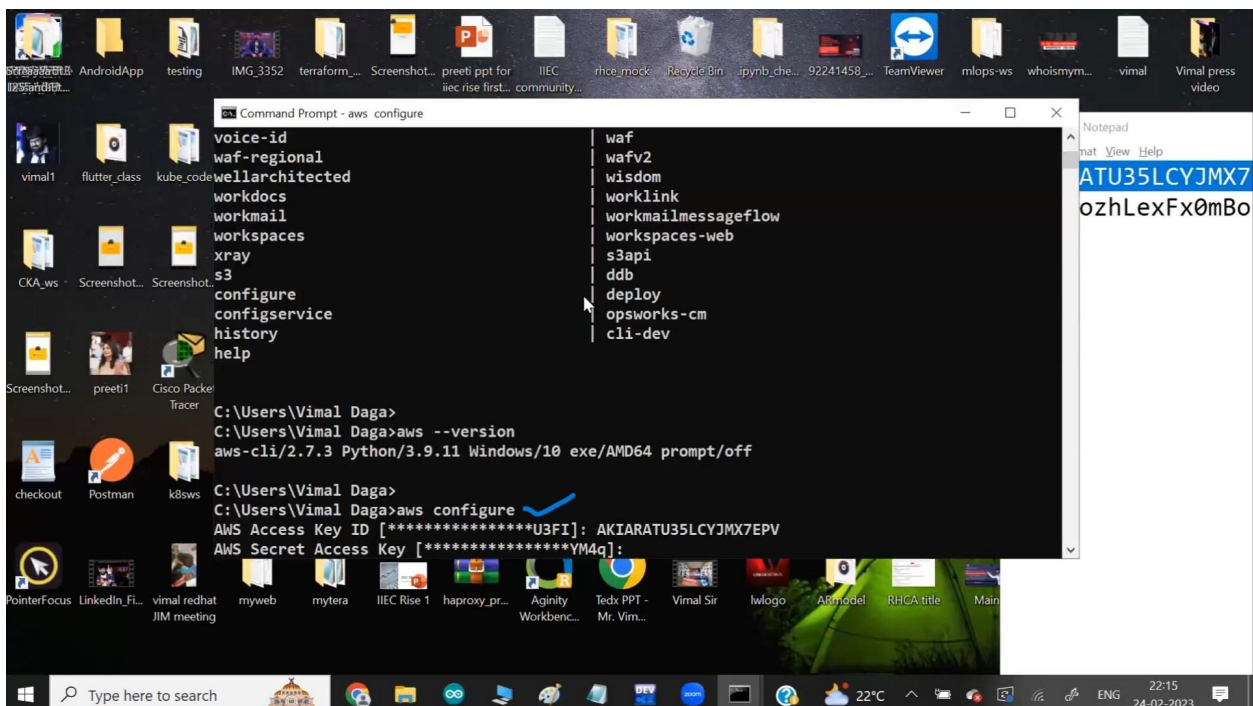
- `aws --version` will show you which version you have installed.



- `aws configure` this command will help you to login via CLI into AWS, you need to provide access key and secret key.



- Enter your access key and secret key.
- You need to provide region in which you want to login.



- You can list the commands by simply typing `aws <subservice name>` :

- `Aws ec2 stop-instances --instance-ids <id of your instance> :`
- This command will stop the running instance with the id provided.

The screenshot shows a Windows Command Prompt window with the following text:

```
* terminate-instances
* unassign-ipv6-addresses
* unassign-private-ip-addresses
C:\Users\Vimal Daga>aws ec2 stop-instances
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:
    aws help
    aws <command> help
    aws <command> <subcommand> help
aws: error: the following arguments are required: --instance-ids
C:\Users\Vimal Daga>aws ec2 stop-instances --instance-ids i-009dfa70161b03e3b
```

In the background, a portion of the AWS Management Console is visible, showing a list of EC2 instances. The table below represents the visible data:

Instance summary Info			
Instance ID	Public IPv4 address	Private IPv4 address	

- Similarly you can start the instance also you can launch the instance using CLI and do many more things.