

NAME: KSHITIJ GUPTA

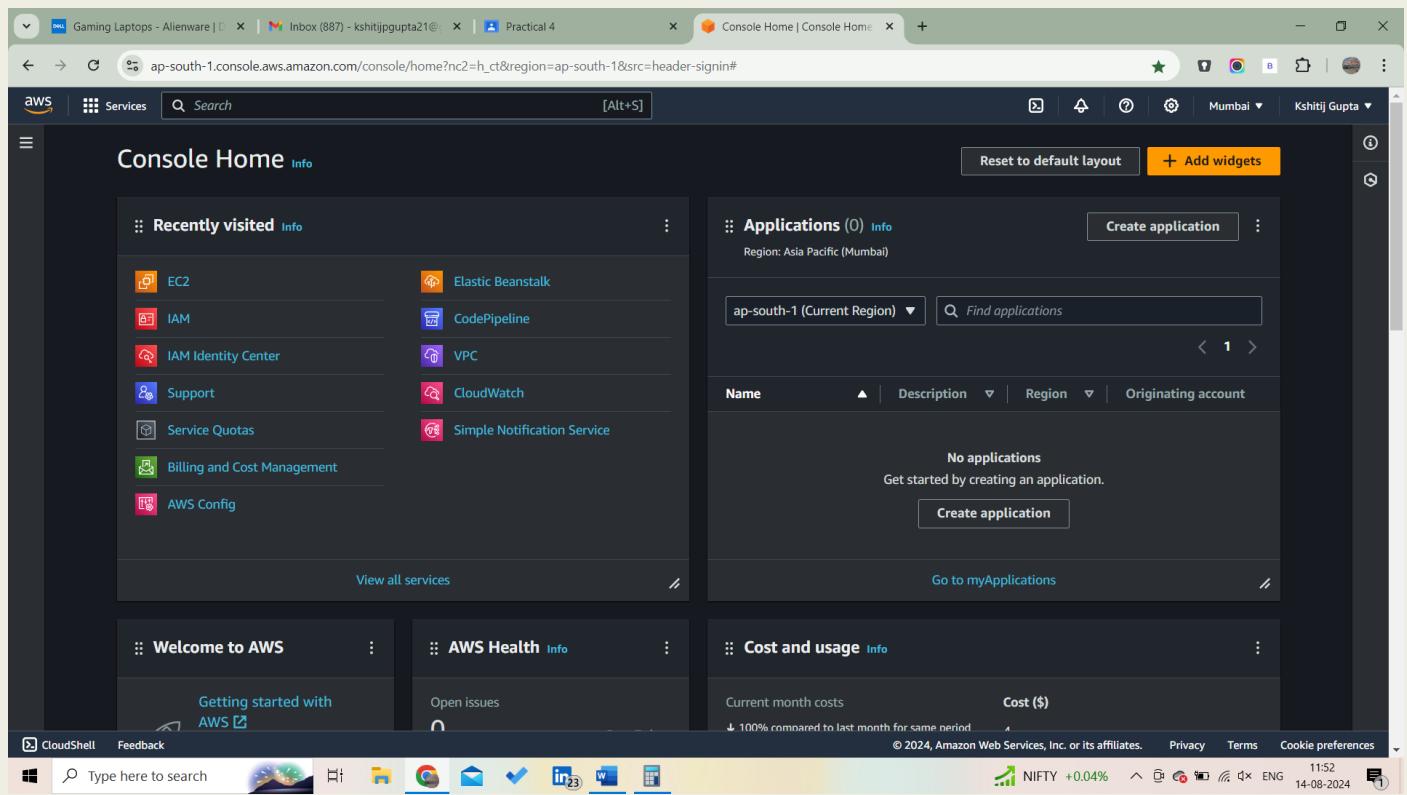
Enrolment Number: 21162101007

Sub: CCE

Practical – 4[Batch-71]

- Create an IAM users like DevOps, Solution Architect.
- Manage User roles and policies using Identity and Access Management (IAM).

Step-1: Go to console



Step-2: Click on EC2

The screenshot shows the AWS EC2 Dashboard. On the left, a sidebar lists various EC2-related services like Instances, Images, and Network & Security. The main area displays a summary of resources: 0 running instances, 0 Auto Scaling Groups, 0 Capacity Reservations, 0 Dedicated Hosts, 0 Elastic IPs, 0 Instances, 1 Key pair, 0 Load balancers, 0 Placement groups, 2 Security groups, 0 Snapshots, and 0 Volumes. Below this is a 'Launch instance' section with a 'Launch instance' button and a note about launching in the Asia Pacific (Mumbai) Region. To the right, there's a 'Service health' section showing the AWS Health Dashboard and a status of 'This service is operating normally'. A large 'EC2 Free Tier Info' box indicates 0 offers in use, with a note about exceeding the free tier limit. At the bottom, account attributes like the Default VPC (vpc-014c092f63f88be84) and settings for Data protection and security and Zones are listed.

Step-3: Create and Launch Instance

The screenshot shows the 'Launch an instance' wizard. The first step, 'Summary', is displayed. It asks for the number of instances (set to 1), software image (Amazon Linux 2023.5.2...), virtual server type (t2.micro), firewall (New security group), and storage (1 volume(s) - 8 GiB). A tooltip for the 'Free tier' is shown, stating: 'In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on Free tier AMI per month'. At the bottom, there are 'Cancel', 'Launch instance', and 'Review commands' buttons.

Step-4:

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The 'Name and tags' section has 'Name' set to 'IAM-kshitij'. The 'Application and OS Images (Amazon Machine Image)' section shows 'Amazon Linux 2023 AMI 2023.5.2...' selected. The 'Virtual server type (instance type)' is set to 't2.micro'. A tooltip for 'Free tier' is visible, stating: 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on a fraction of AMIs per year.' The 'Launch instance' button is highlighted.

Step-5:

The screenshot shows the 'Launch an instance' wizard completed successfully. A green banner at the top states: 'Success Successfully initiated launch of instance (i-031013af1a4d377f4)'. Below this, the 'Next Steps' section provides links to 'Create billing and free tier usage alerts', 'Connect to your instance', 'Connect an RDS database', and 'Create EBS snapshot policy'.

The screenshot shows the AWS EC2 Instances page. The left sidebar is collapsed. The main area displays a table titled "Instances (1) Info" with one row. The row contains the following columns: Name (IAM-kshtij), Instance ID (i-031013af1a4d377f4), Instance state (Pending), Instance type (t2.micro), Status check (-), Alarm status (...), Availability Zone (ap-south-1b), and Public IPv4 DNS (ec2-52-66-250-2). Below the table, a modal window titled "Select an instance" is open. The bottom right corner of the screen shows the AWS navigation bar with "CloudShell" and "Feedback" buttons, along with system status icons.

Step-6: Now go to IAM

The screenshot shows the AWS IAM Users page. The left sidebar is collapsed. The main area displays a table titled "Users Info" with one row. The row contains the following columns: User name (IAM-kshtij). The bottom right corner of the screen shows the AWS navigation bar with "CloudShell" and "Feedback" buttons, along with system status icons.

Step-7: Give a User name

The screenshot shows the 'Create user' wizard in the AWS IAM console. The current step is 'Specify user details'. The 'User name' field contains 'IAM-KSHITIJ'. A note below it specifies character limits and valid characters (A-Z, a-z, 0-9, + = . @ _ - (hyphen)). An optional checkbox for 'Provide user access to the AWS Management Console' is unchecked. A callout box provides instructions for generating programmatic access keys. Navigation links for 'Step 1: Specify user details', 'Step 2: Set permissions', and 'Step 3: Review and create' are visible on the left. Buttons for 'Cancel' and 'Next' are at the bottom right.

Step-8: before Set a permission

The screenshot shows the 'Set permissions' step of the 'Create user' wizard. It offers three methods: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. A note encourages using groups for managing permissions by job function. A 'Create group' button is available. A 'Set permissions boundary - optional' section is shown below. Navigation links for 'Step 1: Specify user details', 'Step 2: Set permissions', and 'Step 3: Review and create' are on the left. Buttons for 'Cancel', 'Previous', and 'Next' are at the bottom right.

Step-9: Create a user group

The screenshot shows the 'Create user group' wizard at Step 2: Set permissions. In the 'Permissions policies' section, a search bar filters results by 'EC2F'. A table lists two policies: 'AmazonEC2FullAccess' (selected) and 'EC2FastLaunchFullAccess'. The table includes columns for Policy name, Type, Usage, and Description. Buttons for 'Cancel' and 'Create user group' are at the bottom.

Step-10: Now set a permission

The screenshot shows the 'Set permissions' step of the wizard. The 'Permissions options' section has 'Add user to group' selected. Other options include 'Copy permissions' and 'Attach policies directly'. Below is a 'User groups' table showing one group named 'DEV-OPS' attached to the 'AmazonEC2FullAccess' policy. A note about setting a permissions boundary is at the bottom.

Step-11:in the permission option set a select the USER_GROUP

The screenshot shows the 'Permissions options' step of the IAM user creation wizard. The 'Add user to group' option is selected. A table below lists one user group, 'DEV-OPS', which has 0 attached policies and was created on 2024-08-14 (Now). The table includes columns for Group name, Users, Attached policies, and Created.

User groups (1/1)			
Group name	Users	Attached policies	Created
DEV-OPS	0	AmazonEC2FullAccess	2024-08-14 (Now)

Step-12: Review your settings

The screenshot shows the 'Review and create' step of the IAM user creation wizard. It displays the user details ('User name: IAM-KSHITIJ'), a permissions summary ('DEV-OPS' assigned to 'Permissions group'), and a tags section ('No tags associated with the resource').

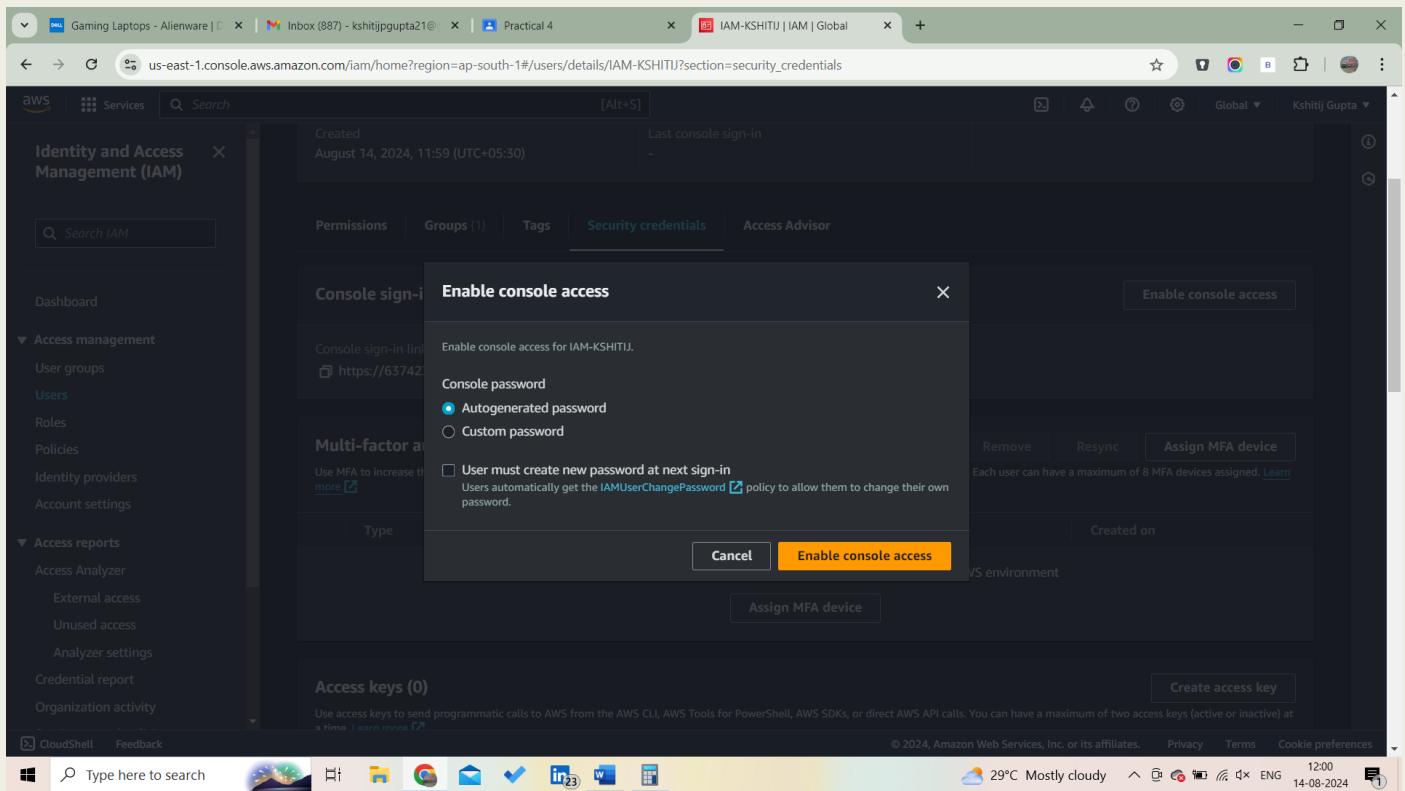
Step-13: User is created

The screenshot shows the AWS IAM Users page. A green banner at the top indicates "User created successfully". Below the banner, the page title is "Users (1) Info". A table lists one user: "IAM-KSHITIJ". The "Console access" column shows "Disabled". There is a "Create access key" button in the "Access keys" column. The left sidebar shows the navigation menu for IAM.

Step-14: click on the user and enable the console access

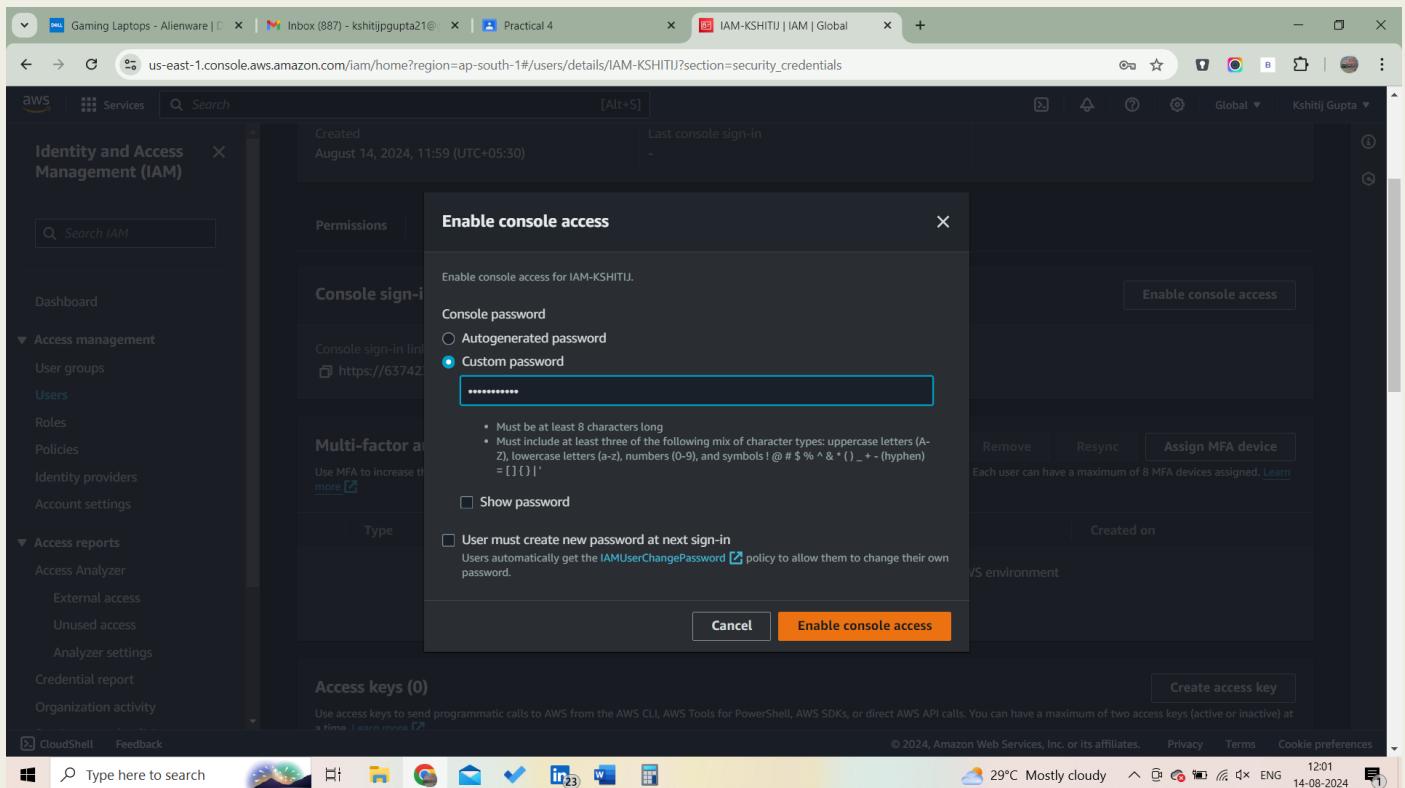
The screenshot shows the IAM user details page for "IAM-KSHITIJ". The "Security credentials" tab is selected. In the "Console sign-in" section, there is a link to "https://637423394361.signin.aws.amazon.com/console" and a note that "Console password Not enabled". The "Enable console access" button is visible. The left sidebar shows the navigation menu for IAM.

Step-15: select the option



The screenshot shows the AWS Identity and Access Management (IAM) console. A modal window titled "Enable console access" is open. Under "Console password", the "Custom password" radio button is selected, and a password "*****" is entered in the text field. The "Enable console access" button at the bottom right is highlighted in orange.

Step-16: set the password



The screenshot shows the AWS IAM console. A modal window titled "Enable console access" is open. Under "Console password", the "Custom password" radio button is selected, and a password "*****" is entered in the text field. The "Enable console access" button at the bottom right is highlighted in orange.

Step-17: download csv

The screenshot shows the AWS IAM console with a modal window titled "Console password". The message inside the modal says: "You have successfully enabled the user's new password. This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one." Below the message, it shows the "Console sign-in URL" as <https://637423394361.signin.aws.amazon.com/console>. The "User name" is listed as "IAM-KSHITIJ". The "Console password" field contains a series of asterisks. At the bottom of the modal, there is a "Download .csv file" button and a "Close" button.

Step-18: copy the link and past on incognito web

The screenshot shows the AWS sign-in page at https://eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=24edhcUDMa0u8rAZ4UhUjAFQh0WTVX56v3nNJ6gB8&code_c.... The page includes a "Try the new sign in UI" message with a "Enable new sign in" button. The main form asks for an "Account ID (12 digits) or account alias" (filled with "637423394361"), "IAM user name" (filled with "IAM-KSHITIJ"), and "Password" (filled with "*****"). There is a "Remember this account" checkbox and a "Sign in" button. To the right of the form is a promotional banner for "Amazon Lightsail" featuring a cartoon robot.

Step-19: only EC2 service's access is provide and other's services are banned for created user

The screenshot shows the AWS Console Home page for the 'eu-north-1' region. On the left, under 'Recently visited', there is a placeholder image of a cube and the text 'No recently visited services'. Below it, links for EC2, S3, RDS, and Lambda are shown. In the center, the 'Applications' section displays a message 'Access denied' in a red-bordered box. On the right, the 'Cost and usage' section also shows 'Access denied' for current month costs and cost breakdown. The bottom navigation bar includes CloudShell, Feedback, a search bar, and system status indicators.

Step-20: you can see

The screenshot shows the AWS EC2 Instances page for the 'ap-south-1' region. The left sidebar lists various EC2-related services like EC2 Dashboard, Global View, Events, Instances, Images, Elastic Block Store, and Network & Security. The main panel displays a table for 'Instances (1)'. One instance is listed: 'IAM-kshitij' (Instance ID: i-031013af1a4d377f4), which is 'Running' on a 't2.micro' instance type. The status check shows '2/2 checks passed'. The instance is located in 'ap-south-1b' availability zone and has a public IP 'ec2-52-'. A modal window titled 'Select an instance' is open over the table. The bottom navigation bar includes CloudShell, Feedback, a search bar, and system status indicators.

- Create an MFA for all users.

Step-21: I have already set the MFA so I just provide you demo of it

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. The main area displays 'Security recommendations' with two items highlighted by a yellow box:

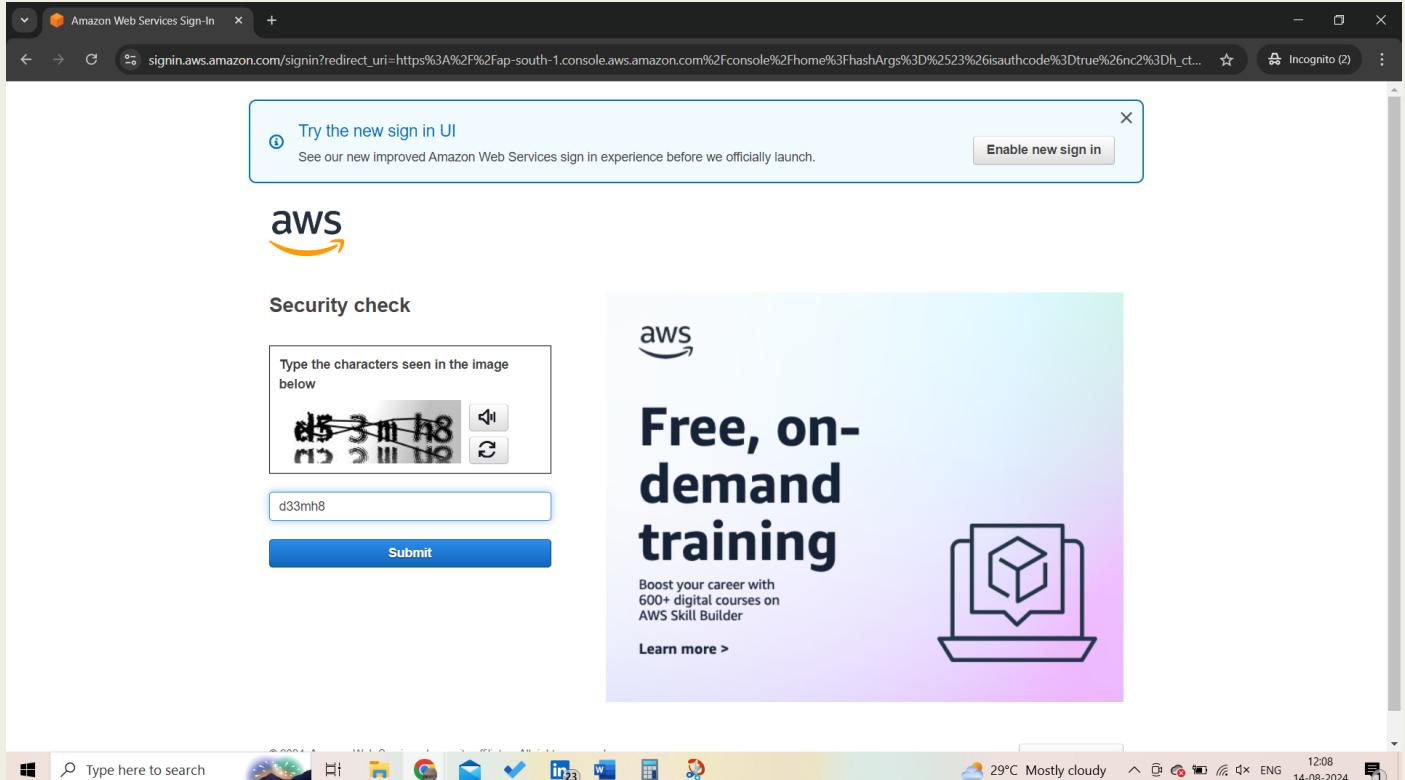
- Root user has MFA
Having multi-factor authentication (MFA) for the root user improves security for this account.
- Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

To the right, there's a 'AWS Account' section with details like Account ID (637423394361), Account Alias (Create), and Sign-in URL (https://637423394361.signin.aws.amazon.com/console).

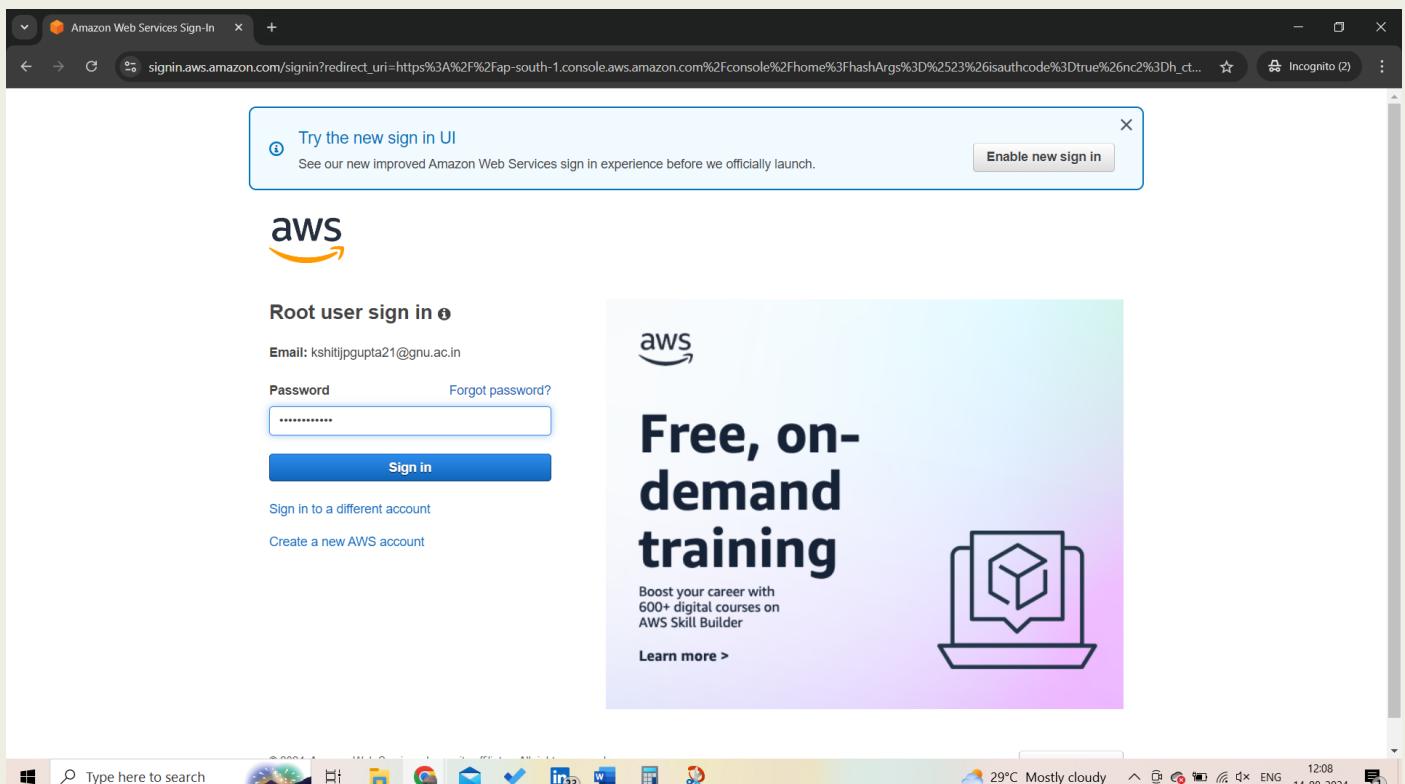
Step-22:

The screenshot shows the AWS sign-in page. It features a 'Try the new sign in UI' message with an 'Enable new sign in' button. The sign-in form includes fields for 'Root user' (selected) and 'IAM user'. Below the form is a 'Root user email address' field containing 'kshitijpgupta21@gnu.ac.in' and a 'Next' button. To the right, there's a promotional banner for 'Free, on-demand training' with a 'Learn more >' link. At the bottom, there's a search bar, a taskbar with various icons, and a system tray showing weather (29°C), battery status, and date/time (12:07 14-08-2024).

Step-23:



Step-24:



Step-25:

Amazon Web Services Sign-In

signin.aws.amazon.com/signin?redirect_uri=https%3A%2F%2Fap-south-1.console.aws.amazon.com%2Fconsole%2Fhome%3FhashArgs%3D%2523%26isauthcode%3Dtrue%26nc%3Dh_ct...

Try the new sign in UI
See our new improved Amazon Web Services sign in experience before we officially launch.

aws

Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: kshitijpgupta21@gnu.ac.in

MFA code

Submit

Troubleshoot MFA

Cancel

aws

Free, on-demand training

Boost your career with 600+ digital courses on AWS Skill Builder

Learn more >

29°C Mostly cloudy 12:08 14-08-2024

Step-26:

Amazon Web Services Sign-In

signin.aws.amazon.com/signin?redirect_uri=https%3A%2F%2Fap-south-1.console.aws.amazon.com%2Fconsole%2Fhome%3FhashArgs%3D%2523%26isauthcode%3Dtrue%26nc%3Dh_ct...

Try the new sign in UI
See our new improved Amazon Web Services sign in experience before we officially launch.

aws

Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: kshitijpgupta21@gnu.ac.in

MFA code 430393

Submit

Troubleshoot MFA

Cancel

aws

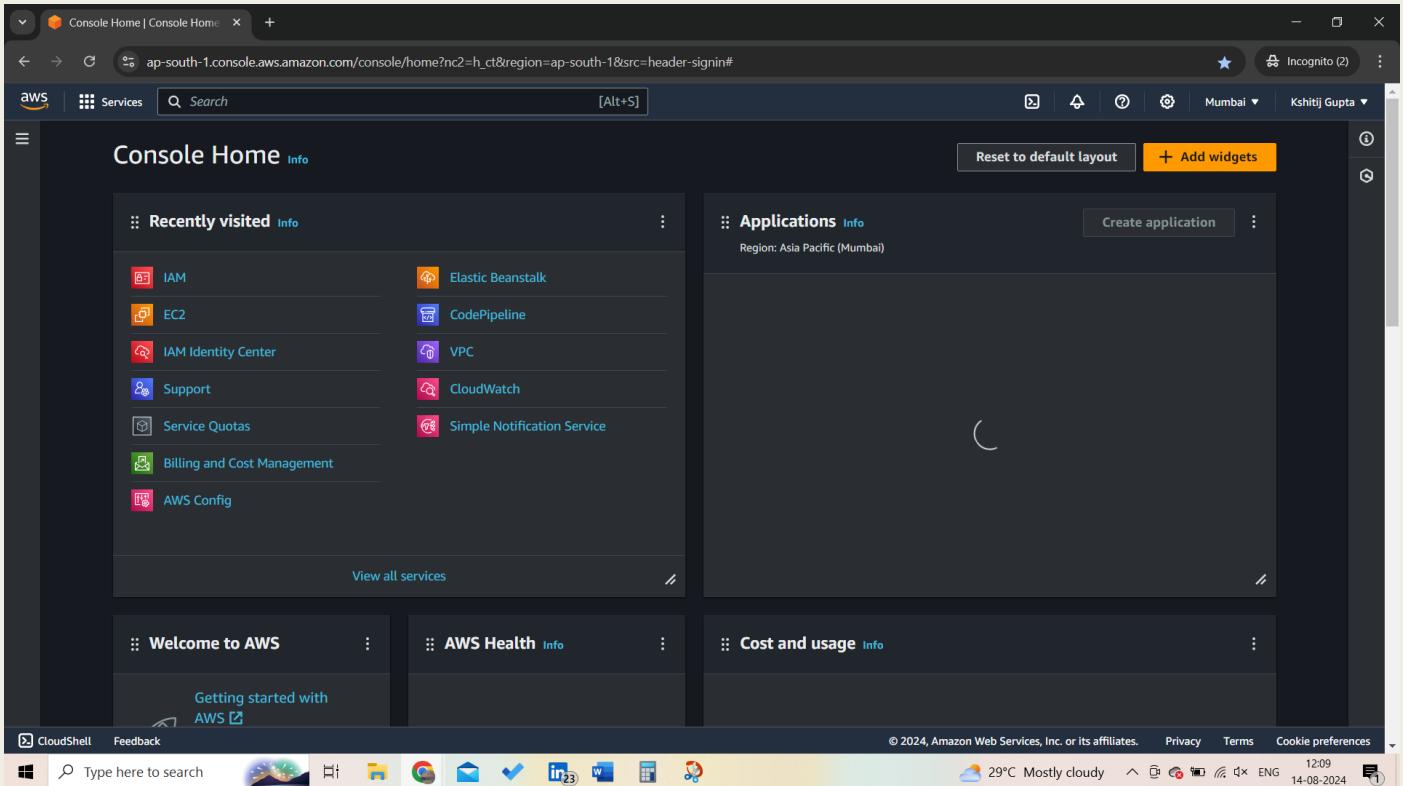
Free, on-demand training

Boost your career with 600+ digital courses on AWS Skill Builder

Learn more >

29°C Mostly cloudy 12:09 14-08-2024

Step-27:



- Set The MFA for created user:

The screenshot shows the IAM User details page for a user named "IAM-KSHITIJ". The "Security credentials" tab is selected. Under "Console sign-in", it shows a "Console sign-in link" (https://637423394361.signin.aws.amazon.com/console). Under "Multi-factor authentication (MFA)", it says "No MFA devices. Assign an MFA device to improve the security of your AWS environment" and has a "Assign MFA device" button. The left sidebar shows navigation options like Dashboard, Access management, and Access reports. The status bar at the bottom shows the date (14-08-2024), time (12:36), weather (30°C Mostly cloudy), and battery level.

Gaming Laptops - Alienware | X | Gmail - Inbox (887) - kshitijgupta21@... | Practical 4 | Assign MFA device | IAM | Global | +

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/IAM-KSHITIJ/mfa

aws Services Q mfa

Select MFA device

Step 2 Set up device

MFA device name

Device name This name will be used within the identifying ARN for this device.

IAM-TESTING Maximum 64 characters. Use alphanumeric and * = , . @ - _ characters.

MFA device

Device options In addition to username and password, you will use this device to authenticate into your account.

Passkey or security key Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

Authenticator app Authenticate using a code generated by an app installed on your mobile device or computer.

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

Type here to search 30°C Mostly cloudy 12:36 14-08-2024

Gaming Laptops - Alienware | X | Gmail - Inbox (887) - kshitijgupta21@... | Practical 4 | Assign MFA device | IAM | Global | +

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/IAM-KSHITIJ/mfa

aws Services Q mfa

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)

2 Open your authenticator app, choose Show QR code on this page, then use the app to scan the code. Alternatively, you can type a secret key.
[Show secret key](#)

3 Type two consecutive MFA codes below
Enter a code from your virtual app below

Wait 30 seconds, and enter a second code entry.

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

Type here to search 30°C Mostly cloudy 12:37 14-08-2024

Gaming Laptops - Alienware | × | 📧 Inbox (887) - kshitijgupta21@... | 🔑 Practical 4 | Assign MFA device | IAM | Global | +

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/IAM-KSHITIJ/mfa

aws Services Q mfa

code.

1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
See a list of compatible applications

2 Open your authenticator app, choose Show QR code on this page, then use the app to scan the code. Alternatively, you can type a secret key.
Show QR code
Show secret key

3 Type two consecutive MFA codes below
Enter a code from your virtual app below
398496
Wait 30 seconds, and enter a second code entry.
475152

Cancel Previous Add MFA

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

Type here to search 30°C Mostly cloudy 12:38 14-08-2024

Amazon Web Services Sign-In eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3aws%3asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=p7ShNsWL1KeDVG7TVmn7sXyqTPBxVXDNI---d7hOp0A&code_c... ☆ Incognito

Try the new sign in UI See our new improved Amazon Web Services sign in experience before we officially launch. Enable new sign in

aws

Sign in as IAM user

Account ID (12 digits) or account alias
637423394361

IAM user name
IAM-KSHITIJ

Password
.....

Remember this account

Sign in

Sign in using root user email
Forgot password?

Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

English

30°C Mostly cloudy 12:40 14-08-2024



Multi-factor Authentication

Enter an MFA code to complete sign-in.

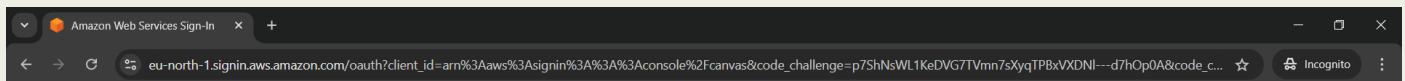
MFA Code:

Submit

[Cancel](#)

English ▾

[Terms of Use](#) [Privacy Policy](#) © 1996-2024, Amazon Web Services, Inc. or its affiliates.



Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code:

Submit

[Cancel](#)

English ▾

[Terms of Use](#) [Privacy Policy](#) © 1996-2024, Amazon Web Services, Inc. or its affiliates.



Console Home | Console Home

ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1#

Mumbai IAM-KSHITU @ 6374-2339-4361

Services Search [Alt+S]

Reset to default layout + Add widgets

Recently visited

EC2

View all services

Welcome to AWS

Getting started with AWS

AWS Health

Applications (0)

Create application

Region: Asia Pacific (Mumbai)

ap-south-1 (Current Region) Find applications

Name Description Region Originating account

Access denied

Go to myApplications

CloudShell Feedback

Type here to search

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

30°C Mostly cloudy 12:41 14-08-2024

Gaming Laptops - Alienware |

Inbox (887) - kshitijgupta21@ | Practical 4 | IAM-KSHITU | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/IAM-KSHITU?section=security_credentials

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
- Analyzer settings
- Credential report
- Organization activity

CloudShell Feedback

Type here to search

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

30°C Mostly cloudy 12:41 14-08-2024

Console sign-in

Console sign-in link: https://637423394361.signin.aws.amazon.com/console

Console password: Updated 6 minutes ago (2024-08-14 12:35 GMT+5:30)

Last console sign-in: Now (2024-08-14 12:40 GMT+5:30)

Multi-factor authentication (MFA) (1)

Type Identifier Certifications Created on

Virtual arn:aws:iam:637423394361:mfa/IAM-TESTING Not Applicable Wed Aug 14 2024

Access keys (0)

Create access key

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials.