

Distributed System and Cloud Computing Lab **Implementation of Identity Management.**

Aim:Protecting Sensitive Information: Ensuring Access for Authorized Users

Theory:

To safeguard sensitive information and IT resources, organizations implement measures to restrict access exclusively to authorized users. This process involves robust security frameworks, authentication mechanisms, and access controls to protect data confidentiality, integrity, and availability.

Key Principles of Access Protection

1. Confidentiality:

- Ensure sensitive information is only accessible to individuals or systems with the correct permissions.
- Prevent unauthorized access or disclosure.

2. Integrity:

- Protect information from being altered or tampered with by unauthorized users.
- Ensure data consistency and accuracy.

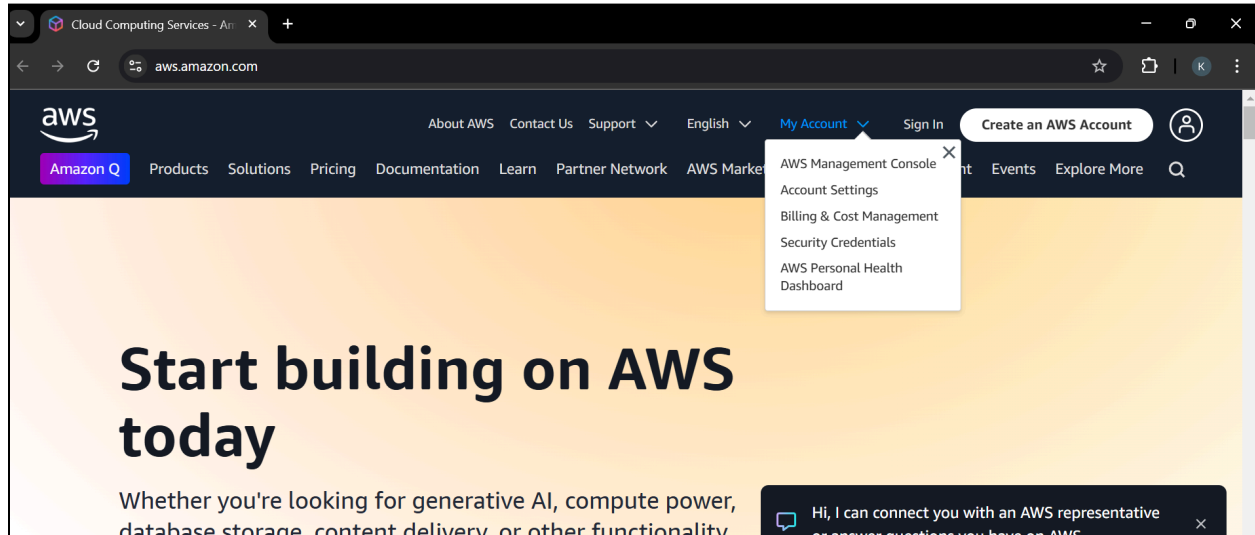
3. Availability:

- Ensure authorized users can access information and systems when needed, without interruption or delay.

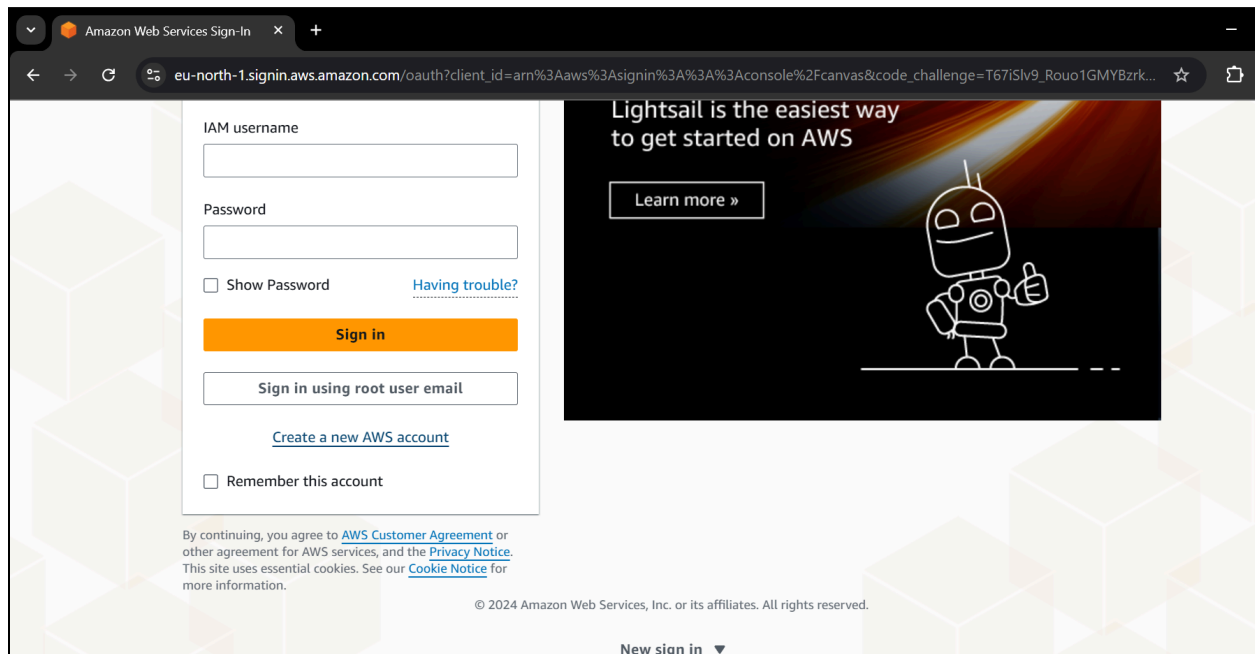
Steps:

Step 1: Open the following link: <https://aws.amazon.com/>.

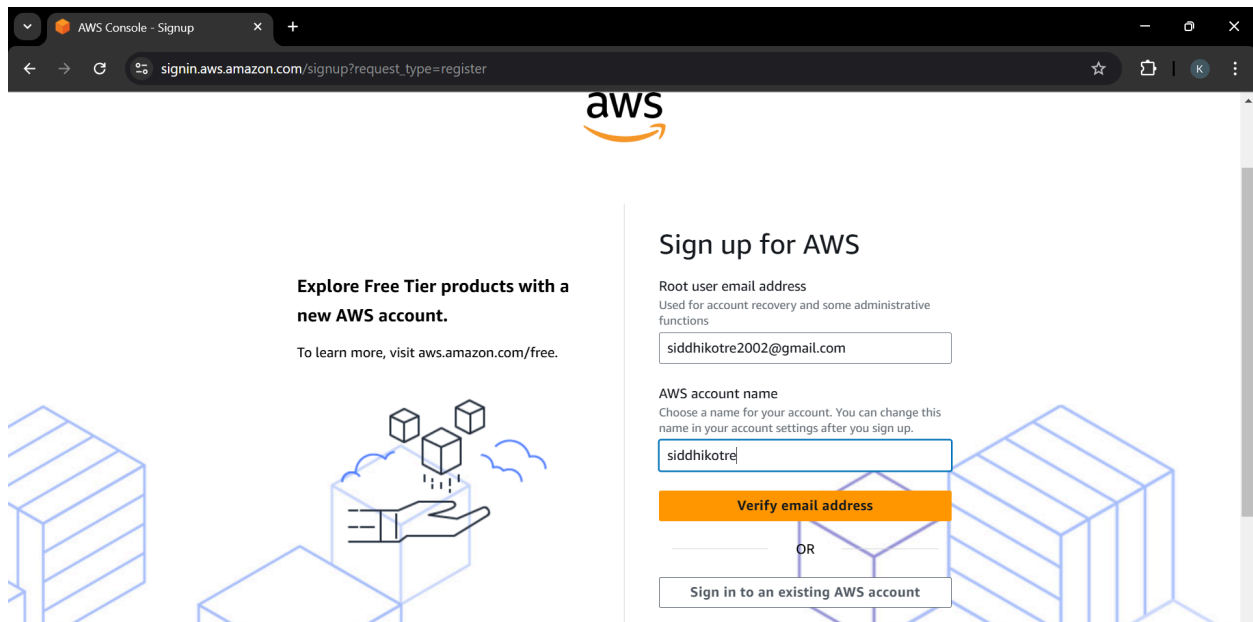
Step 2: Go to **My Account** → **AWS Management Console**.



Step 3: Click on **Create a new AWS account**.



Step 4: Fill in all the details and click **Continue**.



Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.

Sign up for AWS

Root user email address
Used for account recovery and some administrative functions

siddhikotre2002@gmail.com

AWS account name
Choose a name for your account. You can change this name in your account settings after you sign up.

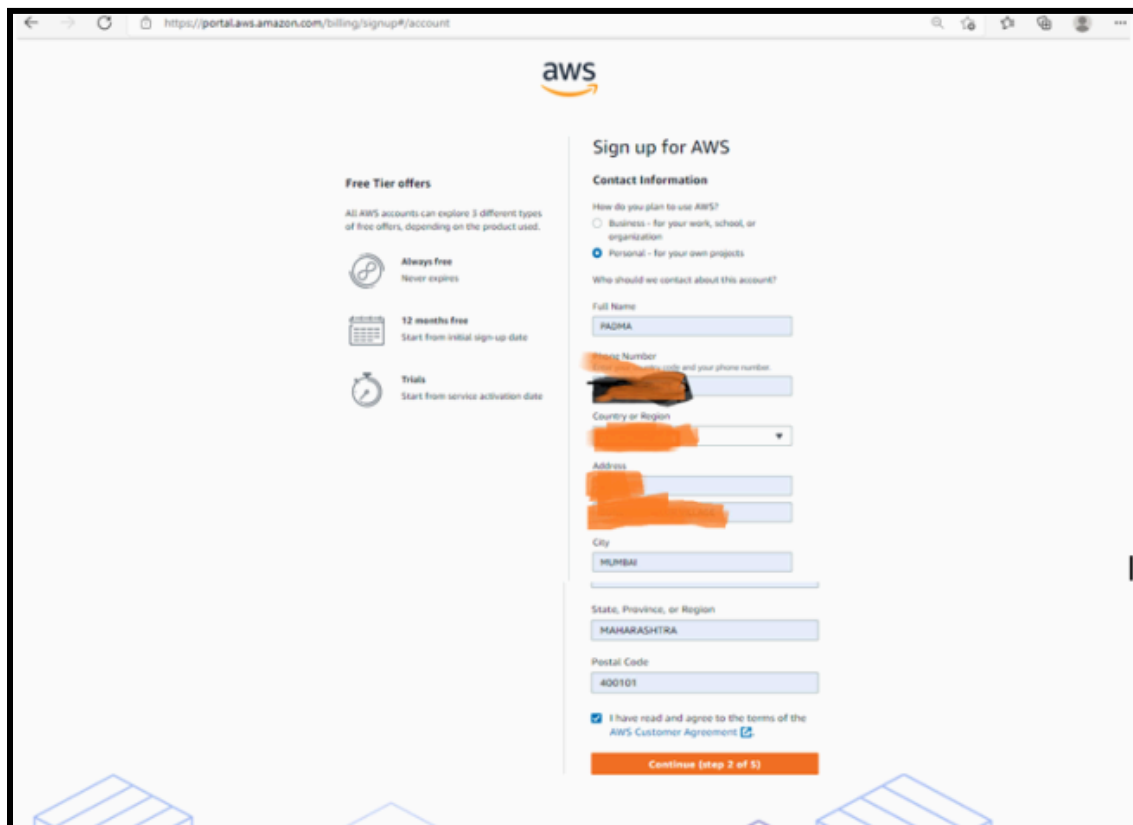
siddhikotre

Verify email address

OR

Sign in to an existing AWS account

Step 5: Provide your contact number and home address, then click **Create Account** and continue.



Sign up for AWS

Free Tier offers

All AWS accounts can explore 3 different types of free offers, depending on the product used.

- Always free**
Never expires
- 12 months free**
Start from initial sign-up date
- Trials**
Start from service activation date

Contact Information

How do you plan to use AWS?

☐ Business - for your work, school, or organization

☒ Personal - for your own projects

Who should we contact about this account?

Full Name
PADMA

Phone Number
Enter your country code and your phone number.
[Redacted]

Country or Region
India

Address
[Redacted]

City
MUMBAI

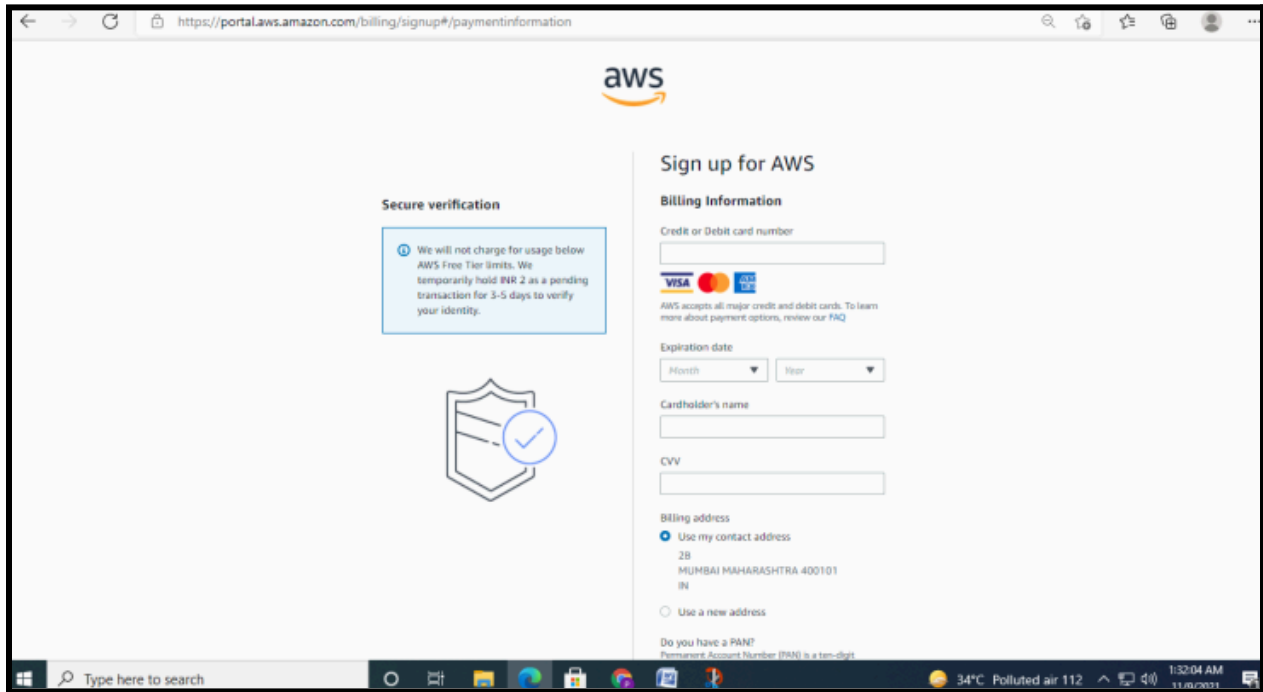
State, Province, or Region
MAHARASHTRA

Postal Code
400101

☒ I have read and agree to the terms of the [AWS Customer Agreement](#)

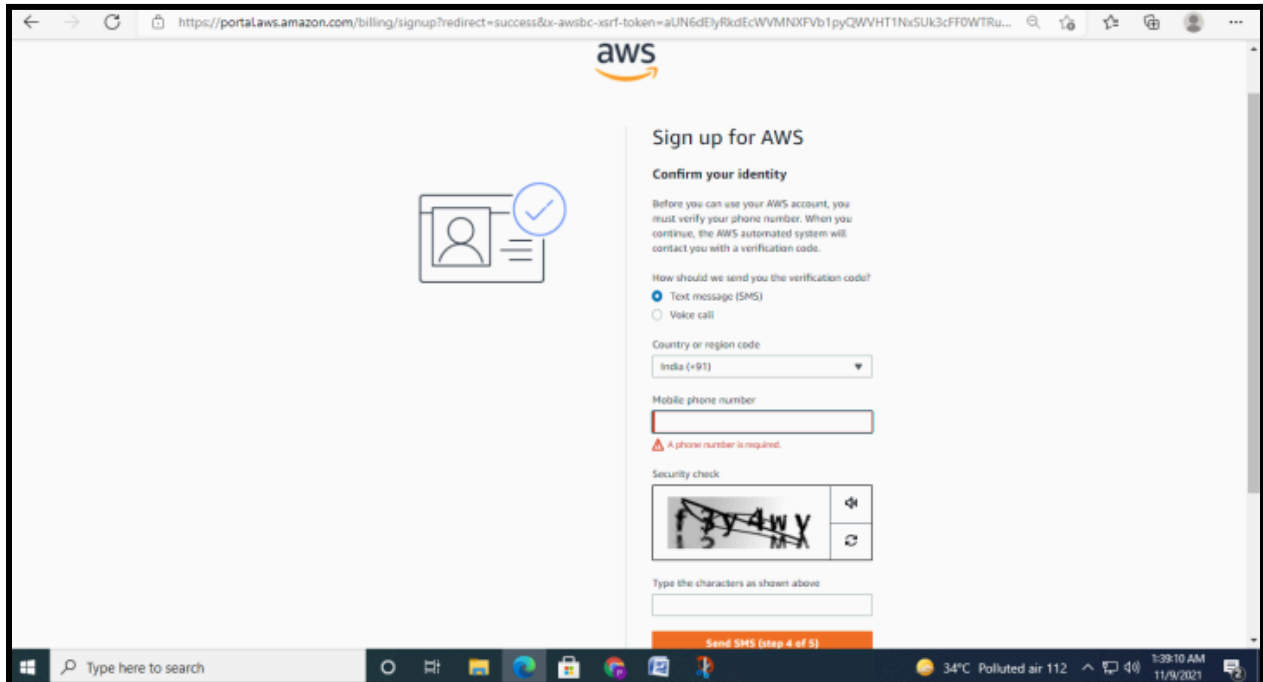
Continue (step 2 of 5)

Step 6: Note that AWS will ask for credit card and debit card details.



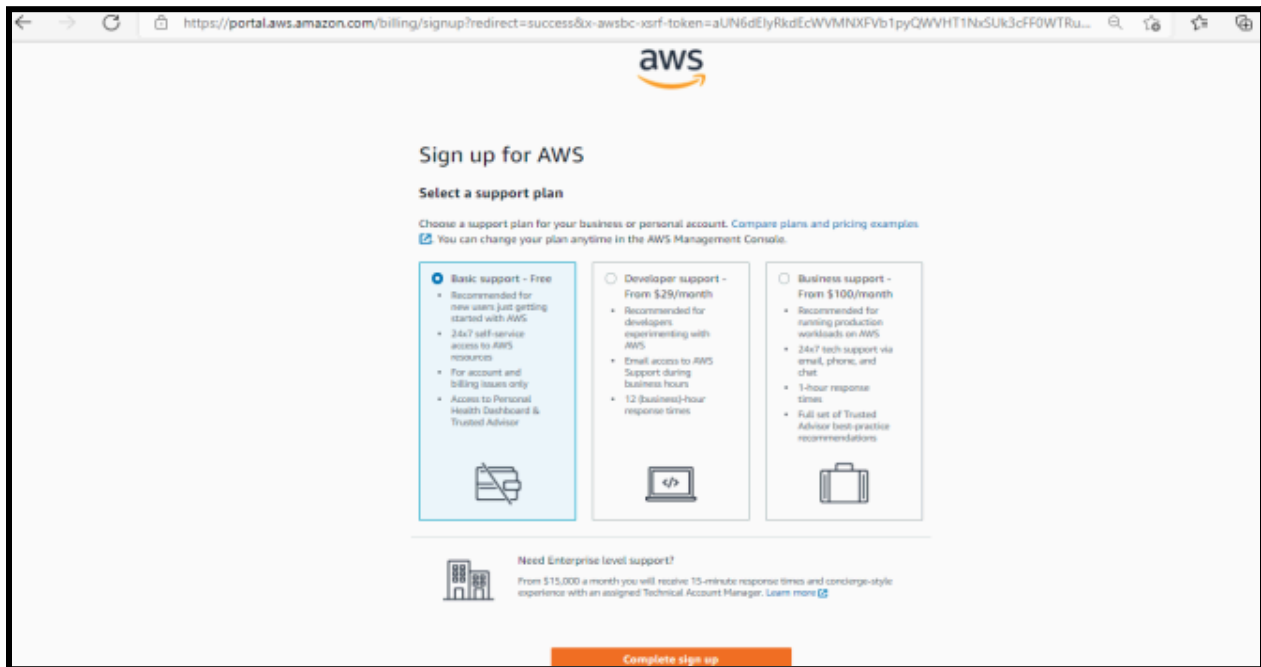
The screenshot shows the AWS Billing console during the sign-up process. The page title is "Sign up for AWS" and the section is "Billing Information". On the left, there is a "Secure verification" box with a shield icon and a checkmark, stating: "We will not charge for usage below AWS Free Tier limits. We temporarily hold INR 2 as a pending transaction for 3-5 days to verify your identity." The main form fields include: "Credit or Debit card number" (with a text input field), "Expiration date" (with month and year dropdowns), "Cardholder's name" (with a text input field), "CVV" (with a text input field), and "Billing address" (with a radio button selected for "Use my contact address" and a text input field showing "28 MUMBAI MAHARASHTRA 400101 IN"). There is also a "Do you have a PAN?" section with a radio button selected for "Yes" and a text input field for the PAN number. The bottom of the page shows a Windows taskbar with the time 1:32:04 AM on 11/8/2021.

Step 7: Confirm your identity.

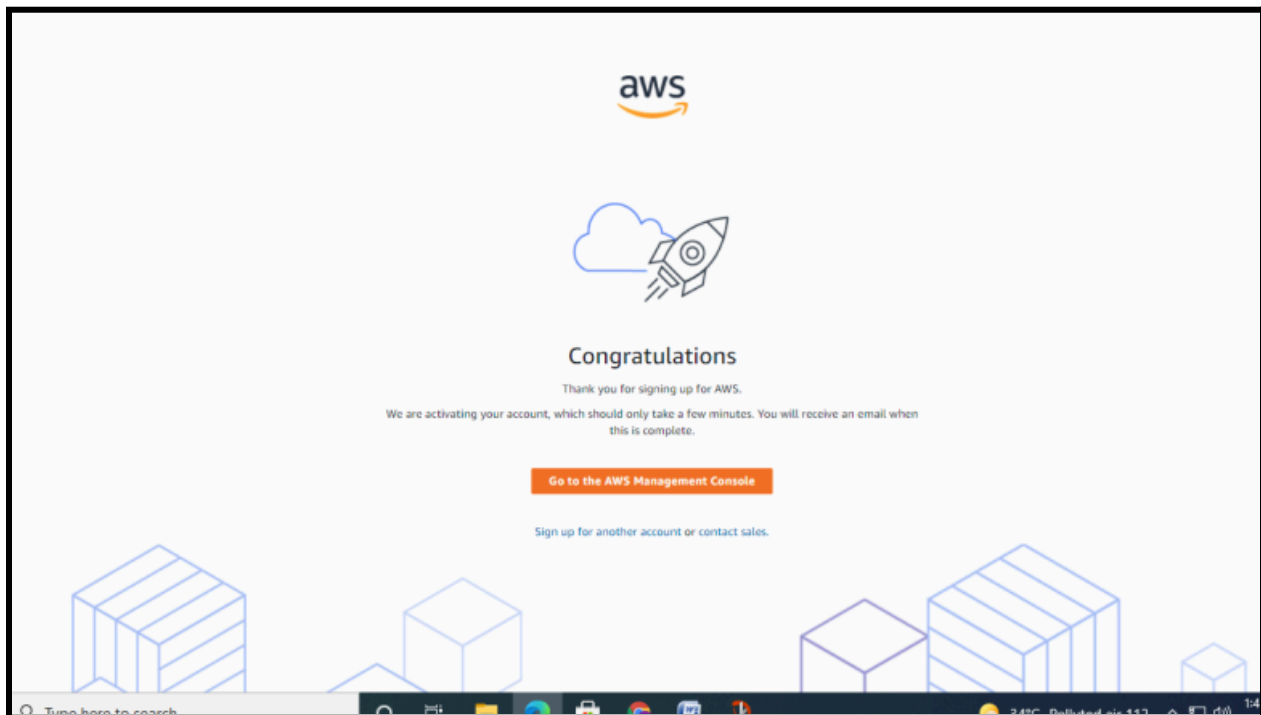


The screenshot shows the AWS Billing console during the sign-up process. The page title is "Sign up for AWS" and the section is "Confirm your identity". On the left, there is a "Confirm your identity" box with a person icon and a checkmark, stating: "Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code." The main form fields include: "How should we send you the verification code?" (with radio buttons for "Text message (SMS)" and "Voice call"), "Country or region code" (with a dropdown menu showing "India (+91)"), "Mobile phone number" (with a text input field and a red error message "A phone number is required."), and "Security check" (with a CAPTCHA image showing the characters "1394wY" and a text input field for the characters). The bottom of the page shows a Windows taskbar with the time 1:39:10 AM on 11/9/2021.

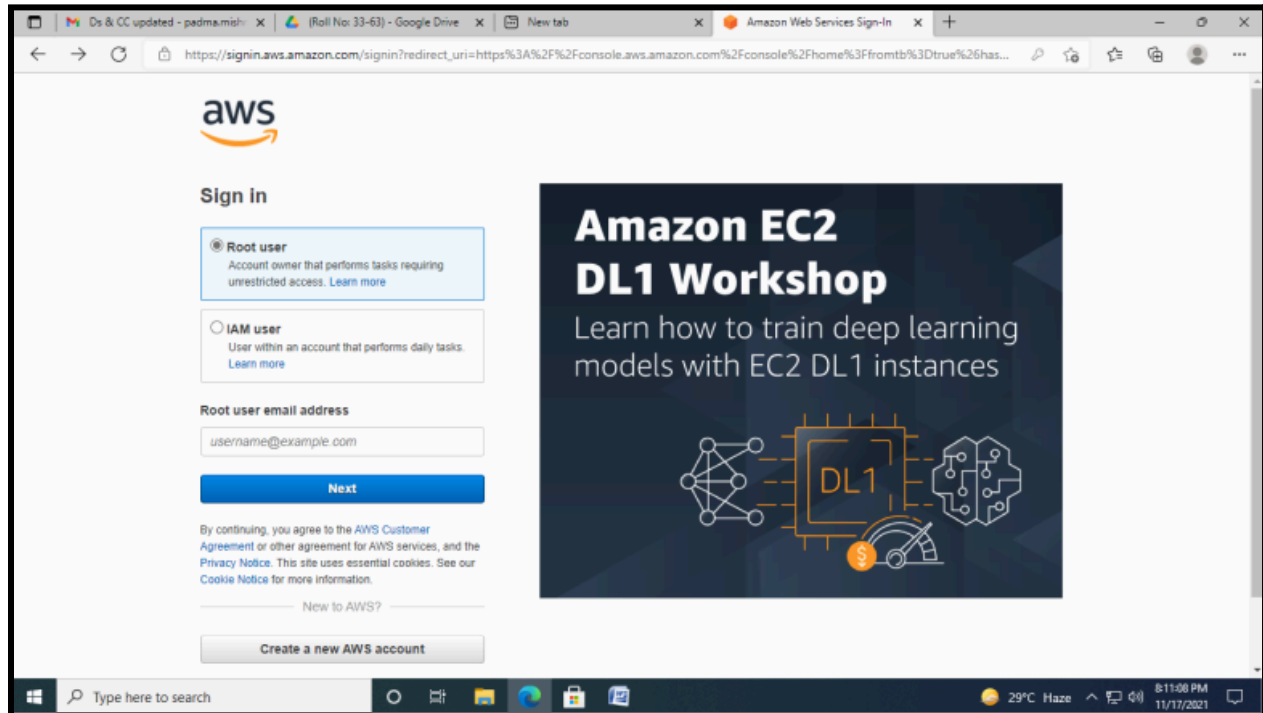
Step 8: Choose the support plan: **1. Basic Support.**



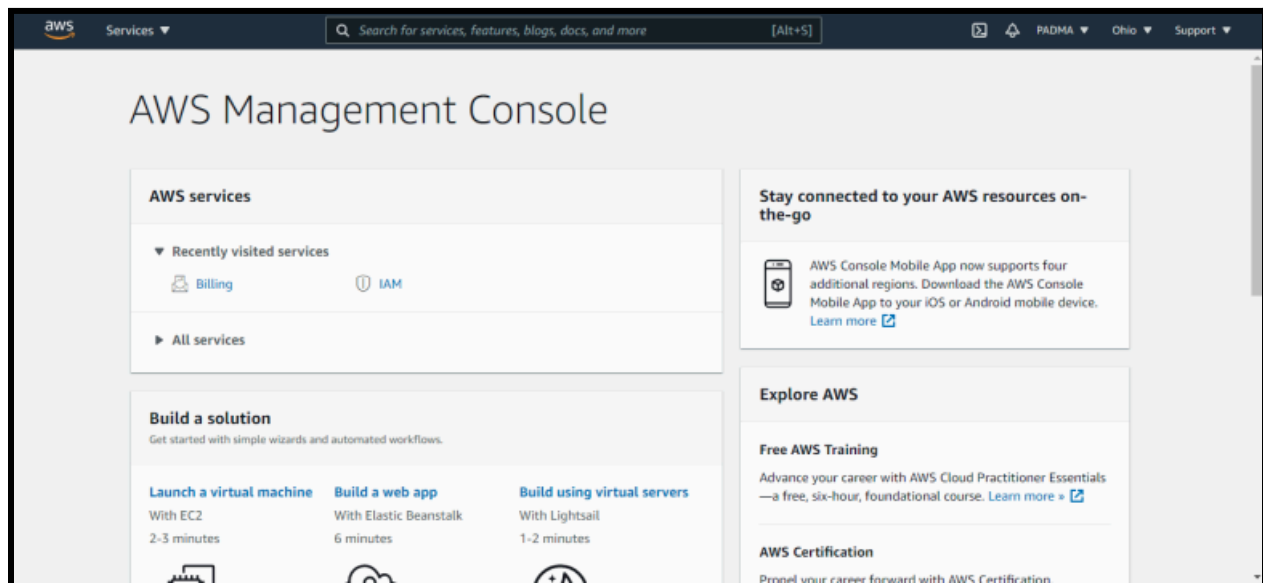
Step 9: Now, open the link: <https://aws.amazon.com/>.



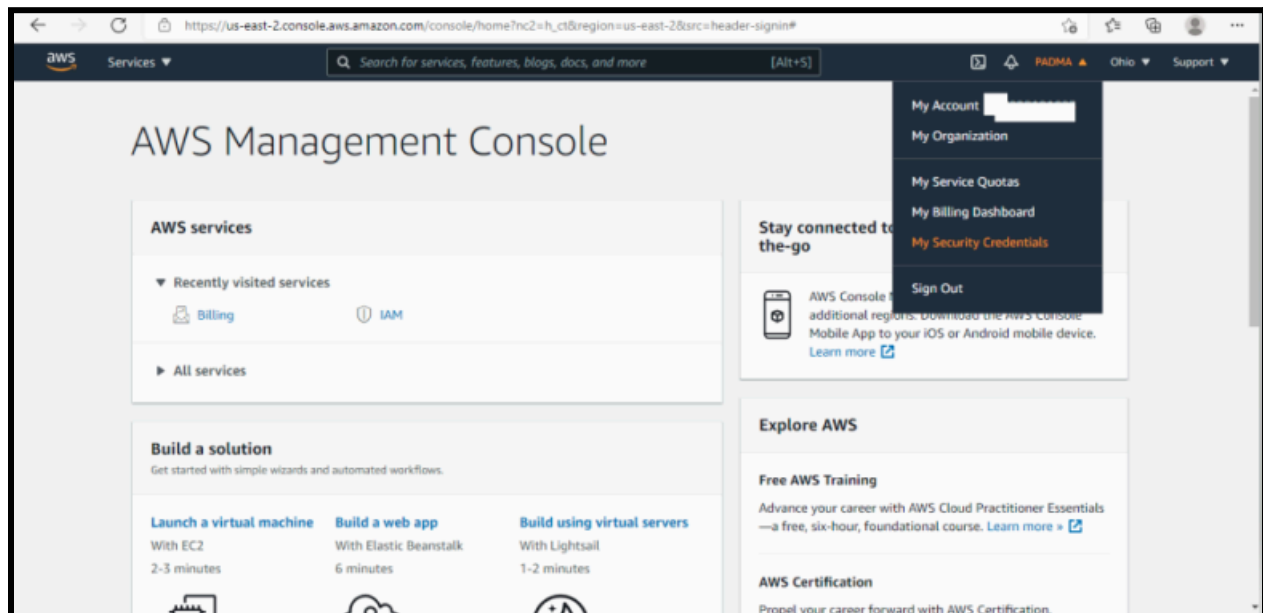
Step 10: Go to **My Account** → **AWS Management Console**. Enter your ID and click Next. After that, enter your password and click Sign In.



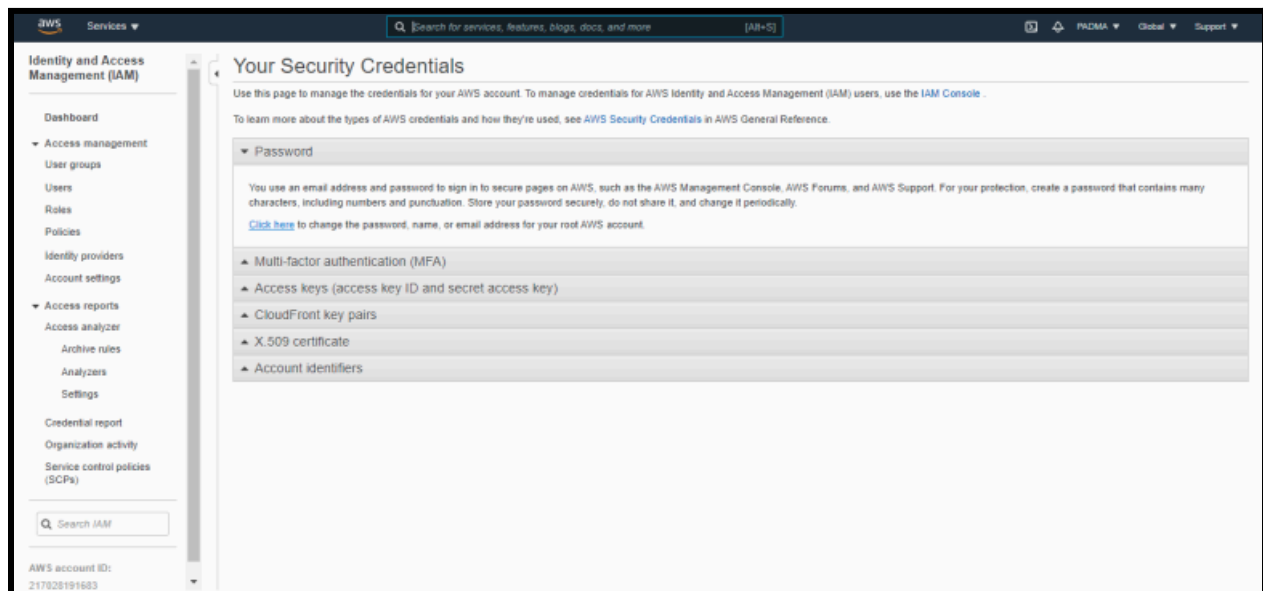
Step 11: The AWS Management Console will open.



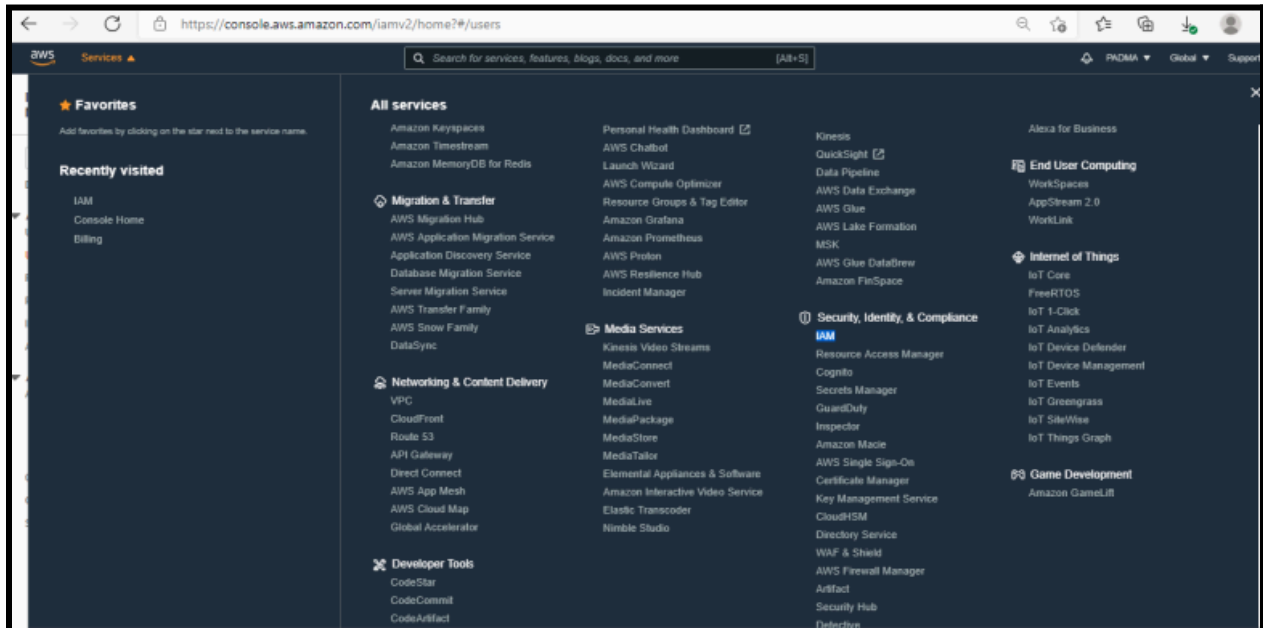
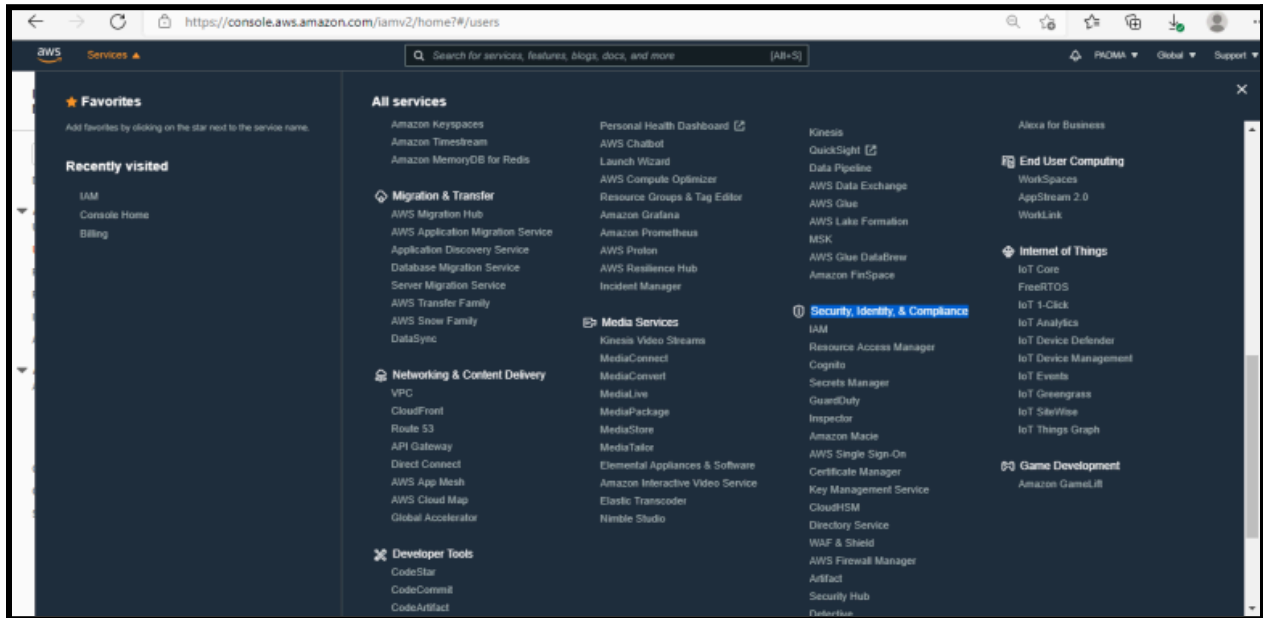
Step 12: Click on My Security Credentials.



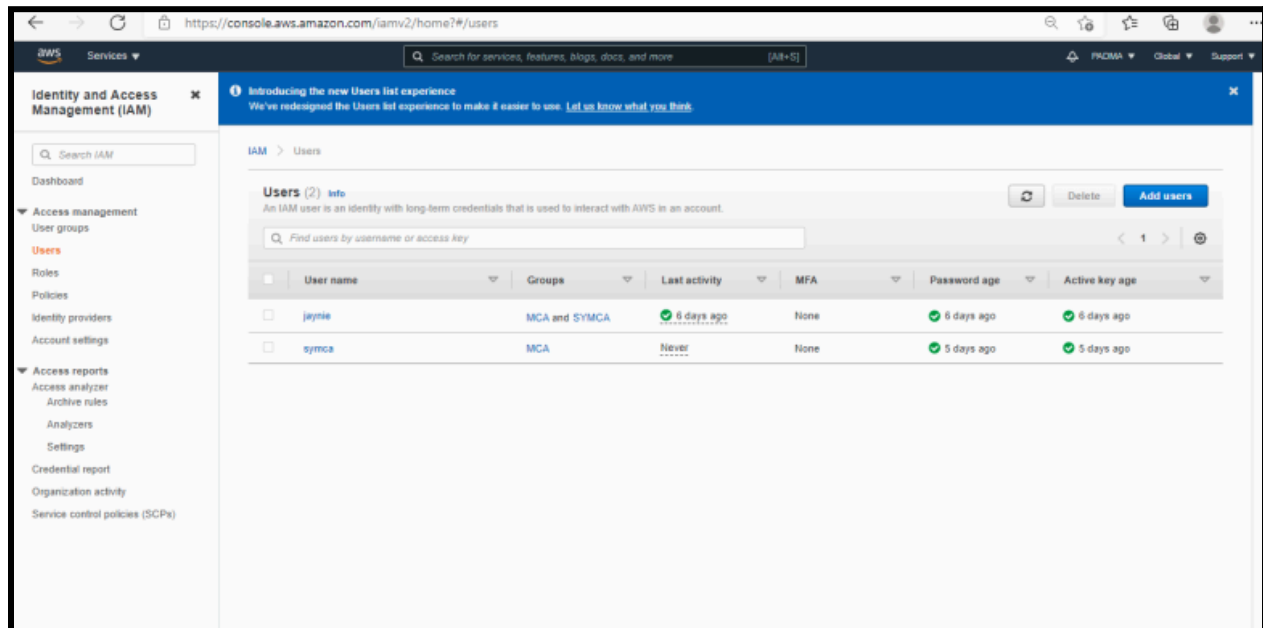
Step 13: Click on Click here to change the password, name, or email address for your root AWS account.



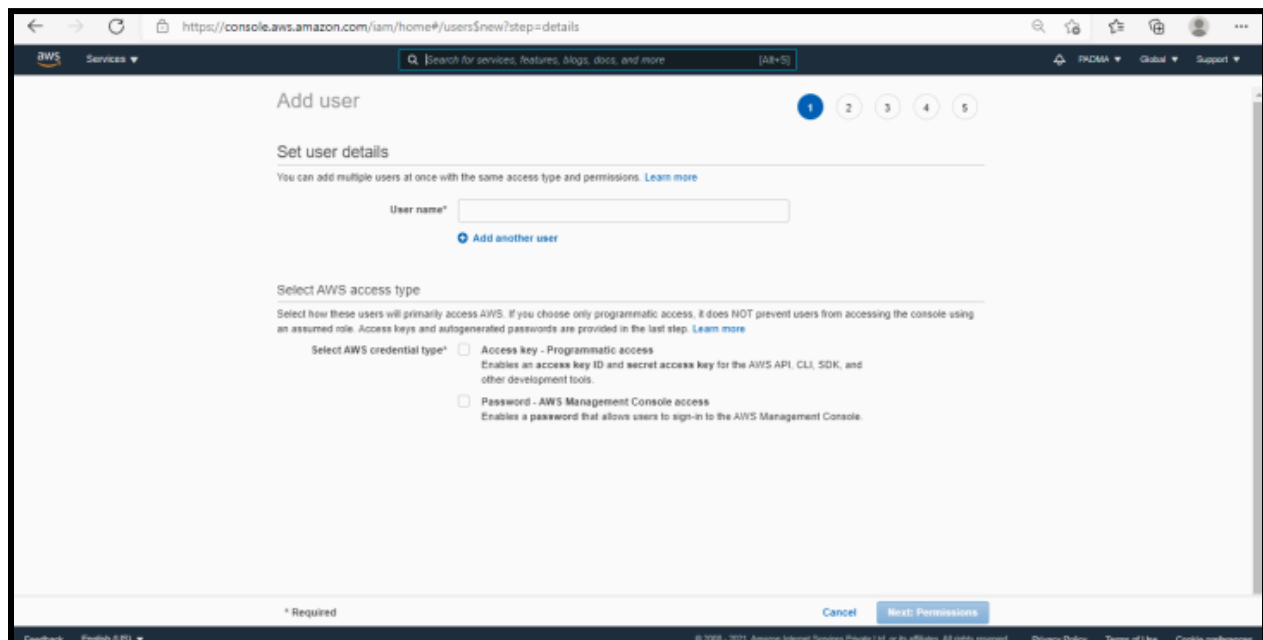
Step 14: Click on Services → Security, Identity, & Compliance → IAM.



Step 15: Click on the **Add Users** button to create a new IAM user.



Step 16: Provide a username and check the boxes for **Programmatic access** and **AWS Management Console access**. Enter a password for the new user, select **Custom password**, and click **Next: Permissions**.



Step 17: Select AWS credential type:

1. **Access Type:** Programmatic access
2. **Password:** AWS Management Console Access: Generate custom password, requiring password reset. Then click **Next: Permissions**.

Console password* ☐ Autogenerated password ☒ Custom password

☐ Show password

Require password reset ☒ User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required Cancel Next: Permissions

Step 18: Provide a group name, select the policies, and then click **Create Group**.

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. [Learn more](#)

Group name

Create policy Refresh

Filter policies Search Showing 710 results

	Policy name	Type	Used as	Description
<input type="checkbox"/>	AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
<input type="checkbox"/>	AdministratorAccess-Ampify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct access to resources n...
<input type="checkbox"/>	AdministratorAccess-AWS-ElasticBeanstalk	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and administrators to g...
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None	Grants full access to AlexaForBusiness resources and access to related AWS Services
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessLifsizeDelegatedAccess...	AWS managed	None	Provide access to Lifsize AVS devices

Cancel Create group

Step 19: The screen will show that the **Test Group** has been created.

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

Analysts

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups

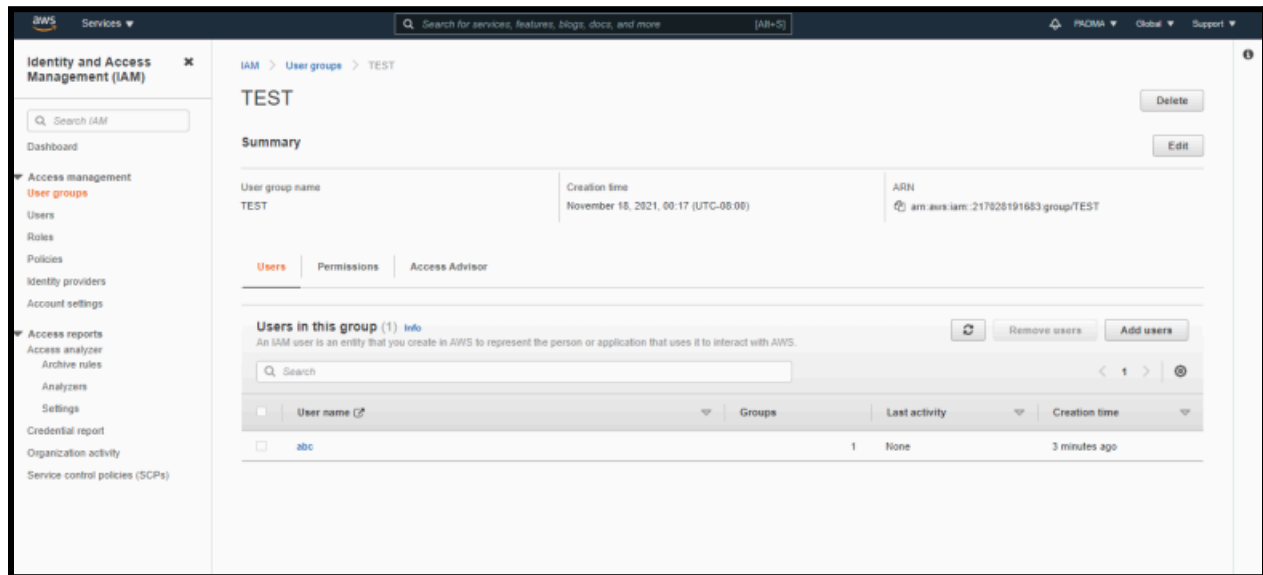
User groups (3) info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

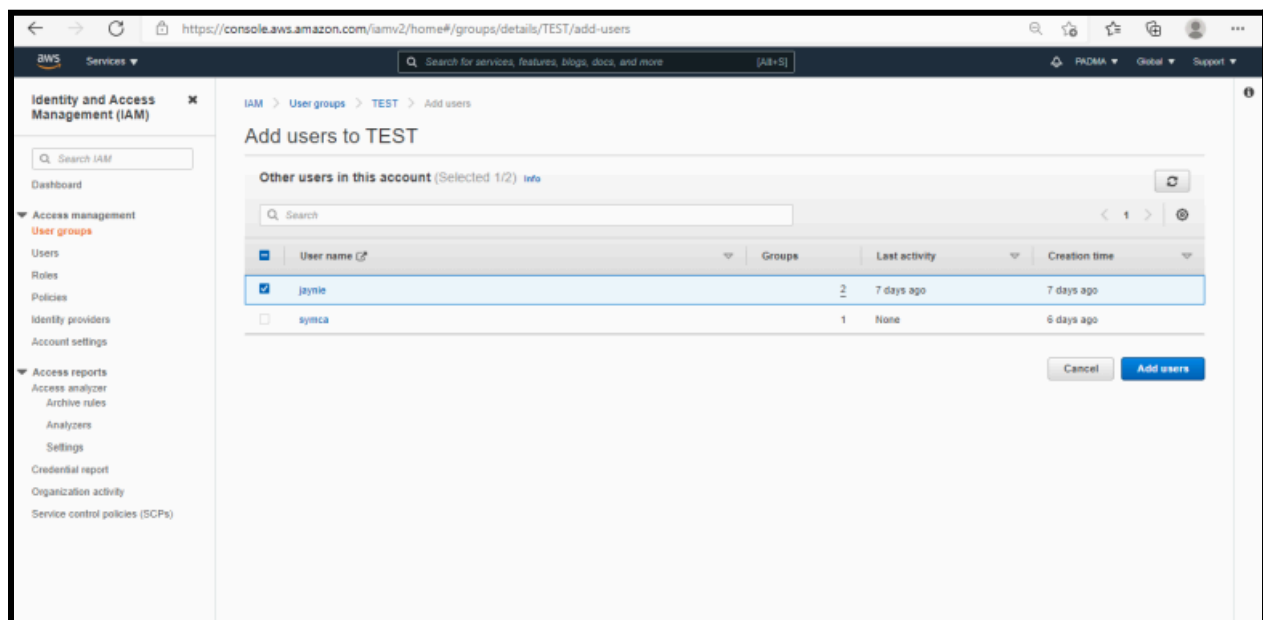
Filter User groups by property or group name and press enter

Group name	Users	Permissions	Creation time
MCA	5 days ago
SYMCA	6 days ago
TEST	42 minutes ago

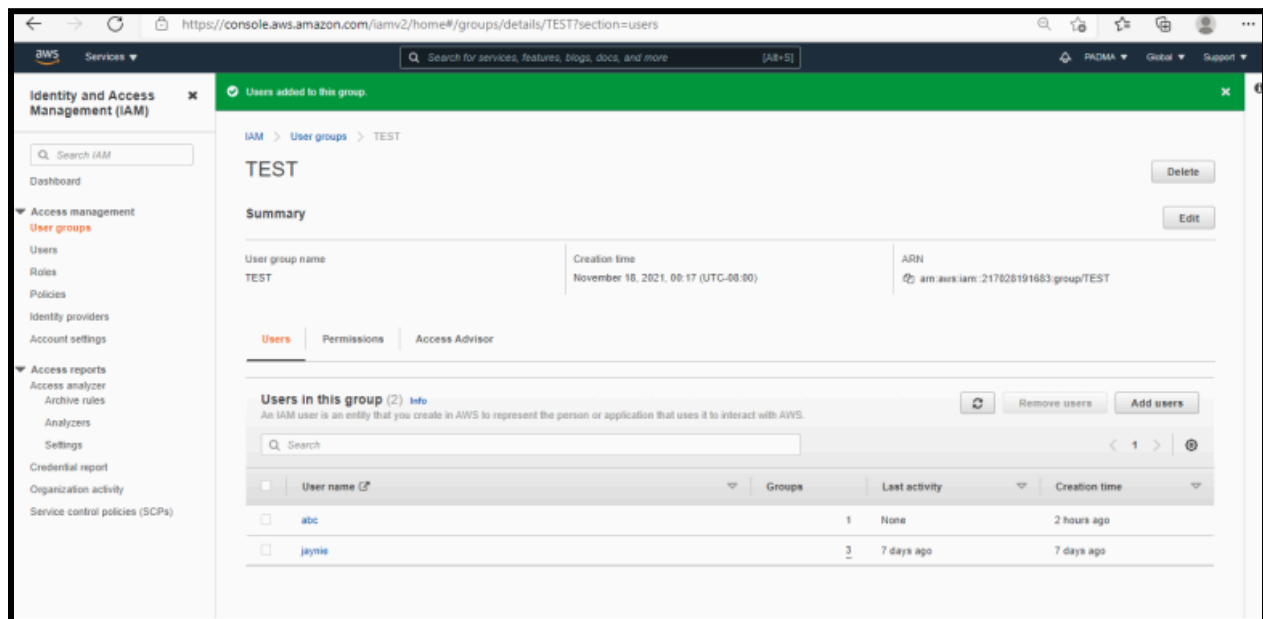
Step 20: Demonstrate how to add existing users to the group.



Step 21: Select the user and click on Add Users.

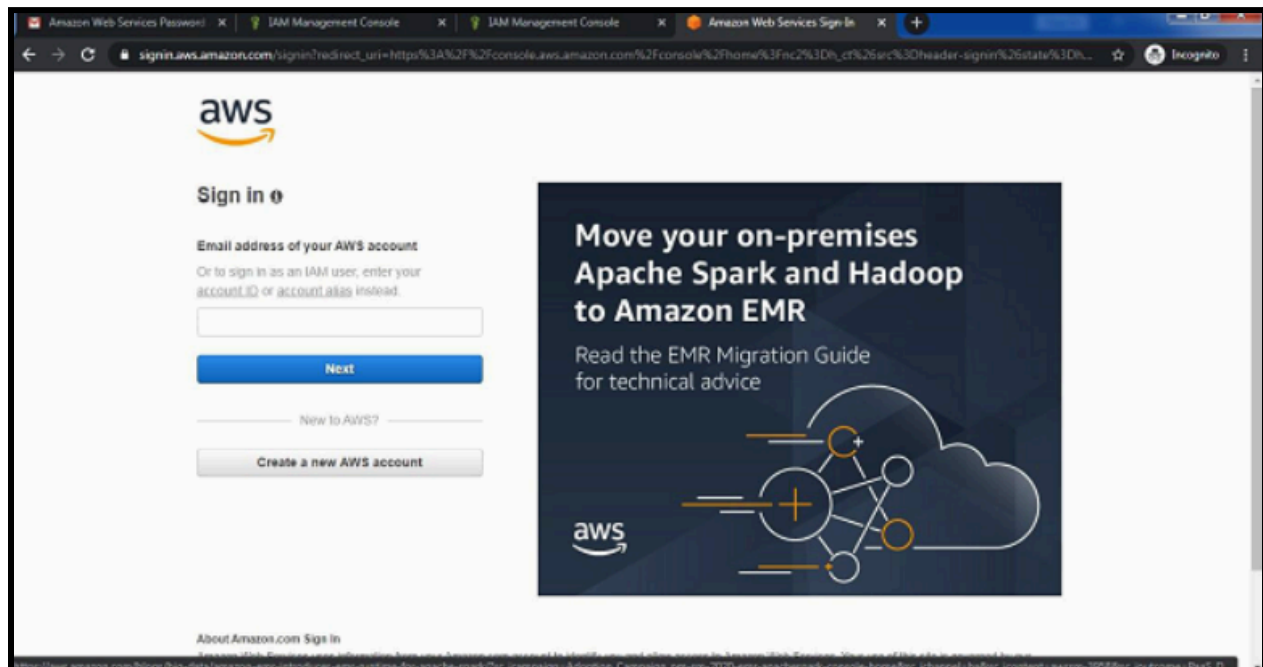


Step 22: The screen will show that two users have been added to the **Test Group**.

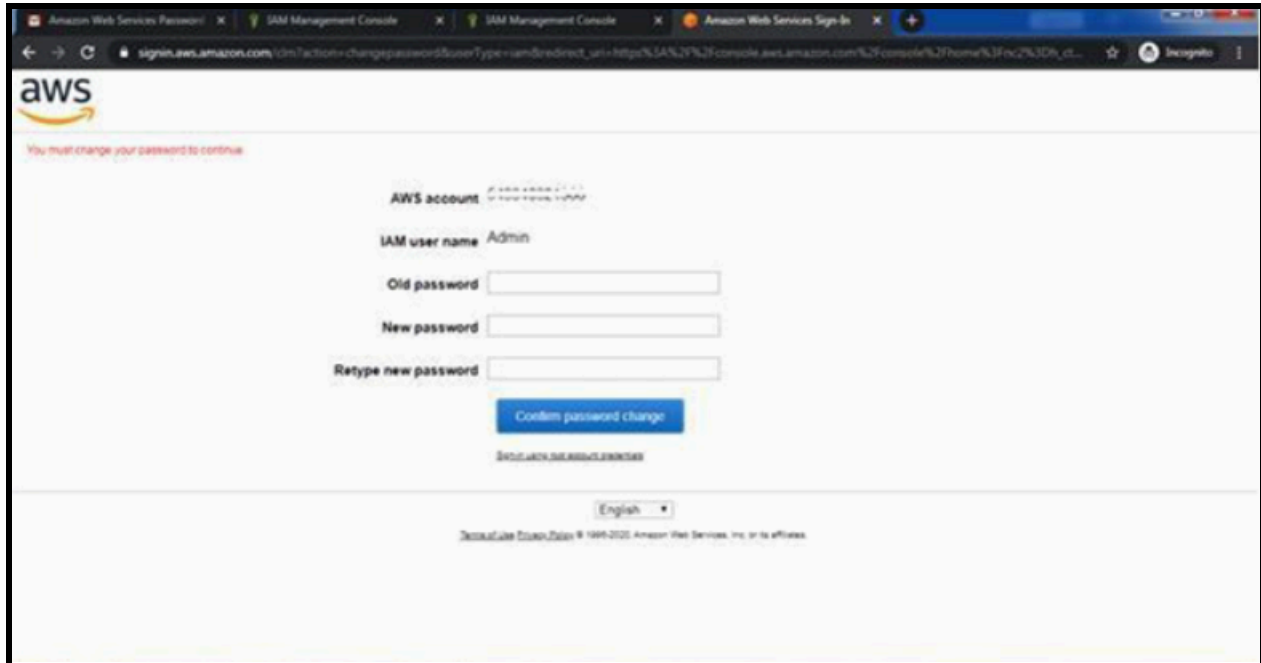


Step 23: Copy the account ID. Now, log out of the root account and try to log in as the newly created IAM user.

Step 24: Go to **My Account** → **AWS Management Console**.



Click on **Next**, provide the account ID, username, and password, and click **Sign In**. It will ask you to change the password that was set by the administrator.



The screenshot shows the AWS IAM console's password change interface. At the top, there's a message: "You must change your password to continue." Below this, the "AWS account" is identified as "1111-1111-1111-1111". The "IAM user name" is "Admin". There are three input fields: "Old password", "New password", and "Retype new password". A blue "Confirm password change" button is located below the input fields. At the bottom, there's a language selector set to "English" and a copyright notice: "© 1996-2020 Amazon Web Services, Inc. or its affiliates."

You will be redirected to the home screen.

