

## Experiment No: 7

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

Theory: ~~with respect to cloud computing~~

- 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 basically IT instances.
- It is a broad concept that encompasses all policies, methodologies and tools to maintain access privilege.
- AM is primarily an information security, IT and data governance process used in granting access to valid users or prohibiting involved users.
- Typically, AM is used in conjunction with identity access management (IAM).
- Identity management creates, provision and controls the different users, roles and groups and policies whereas AM ensures that those roles and policies are allowed.
- An IAM-based application states the different user roles and their policies.

✓ 2020 MAF

## Fundamentals

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 to database with mission critical transaction services and applications hosted in cloud.
- Components in IAM include
  - 1) Authentication
  - 2) Authorization
  - 3) User Management
  - 4) Central User Repository

It can be categorized into four components:-

- 1) Authentication
- 2) Authorization
- 3) User Management
- 4) Central User Repository

Compare the following in AWS:

- 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 user can be created by a root user or another IAM user who has entitlements to create additional IAM user.

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

## 2) Roles and Policies

⇒

### Cloud Roles:

- i) Intended for granting temporary access for entities like application of services.
- ii) AWS resources.
- iii) Temporary access.
- iv) Defines who can assume the role.
- v) Provides a way to grant precise permissions to a specific entity.

### Cloud Policies:

- i) Defines permission and can be attached to user groups or roles.
- ii) Attached to the IAM users/groups.
- iii) Permanent permission.
- iv) This relationship is not applicable as they do not involve.
- v) Defines a set of permissions that can be attached to multiple entities.

- Explain inline and custom policies in AWS
  - ⇒ An inline 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 administered by AWS and doesn't require management.
- Standalone policy that the policy has its own ARN that includes the policy name.
- You can't create a 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 for high additional security.

Written Within (A) S 5/3/2024

## Output:

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

The screenshot shows the AWS EC2 Dashboard for the Europe (Stockholm) Region. Key statistics include 0 Instances (running), 0 Auto Scaling Groups, 0 Dedicated Hosts, 0 Elastic IPs, 1 Instances, 1 Key pairs, 0 Load balancers, 0 Placement groups, 2 Security groups, 0 Snapshots, and 0 Volumes. The 'Launch instance' section allows launching an instance in the Europe (Stockholm) Region. The 'Service health' section shows the AWS Health Dashboard with the status 'This service is operating normally.' The 'Offer usage (monthly)' section tracks Linux EC2 Instances and Storage space on EBS. The 'Account attributes' section provides account-level information.

2. Go to IAM dashboard

The screenshot shows the AWS IAM Dashboard. Under 'Security recommendations', it lists 'Add MFA for root user' and 'Root user has no active access keys'. The 'IAM resources' section displays 0 User groups, 0 Users, 3 Roles, 0 Policies, and 0 Identity providers. The 'AWS Account' sidebar shows the Account ID (533267428271), Account Alias (Create), and Sign-in URL (https://533267428271.signin.aws.amazon.com/console). The 'Quick Links' section includes 'My security credentials' and 'Tools'.

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

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with various navigation options like 'Access management', 'User groups', 'Users', etc. In the center, there's a 'Security recommendations' section with a warning about 'Add MFA for root user' and a note that 'Root user has no active access keys'. Below that is an 'IAM resources' section showing 0 User groups, 0 Users, 3 Roles, 0 Policies, and 0 Identity providers. At the top right, there's a modal window titled 'Create alias for AWS account 533267428271'. It has a 'Preferred alias' input field containing 'myaliascl7', a note that it must be between 1 and 63 characters, and a 'Create alias' button.

This screenshot shows the same IAM Dashboard after the alias has been created. The success message 'Alias myaliascl7 created for this account.' is displayed at the top. The rest of the interface is identical to the previous screenshot, including the security recommendations, IAM resources summary, and the 'Create alias' modal which is now closed.

**4. Click on “users” in the left column**

The screenshot shows the AWS Identity and Access Management (IAM) service interface. In the left sidebar, under the 'Access management' section, the 'Users' option is selected. The main content area displays a table titled 'Users (0) Info' with a single row: 'No resources to display'. At the top right of the table, there are buttons for 'Create user' (orange), 'Delete' (grey), and a search bar.

**5. Click on the Create Users button**

The screenshot shows the 'Specify user details' step of the AWS IAM User creation wizard. On the left, a sidebar lists steps: Step 1 (selected), Step 2, Step 3, and Step 4. The main area is titled 'User details' and contains a 'User name' input field with 'Om\_Shete' typed in. Below it is a checkbox for 'Provide user access to the AWS Management Console - optional'. A callout box highlights the 'User type' section, which offers two options: 'Specify a user in Identity Center - Recommended' (radio button unselected) and 'I want to create an IAM user' (radio button selected). The 'I want to create an IAM user' option includes a note about enabling programmatic access through access keys. At the bottom, there are three password options: 'Console password', 'Autogenerated password', and 'Custom password'.

**Are you providing console access to a person?**

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

**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](#)

**Set permissions boundary - optional**

Cancel **Previous** **Next**

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

**User details**

|                       |  |                               |
|-----------------------|--|-------------------------------|
| User name<br>Om_Shete | Console password type<br>Custom password | Require password reset<br>Yes |
|-----------------------|--|-------------------------------|

**Permissions summary**

| Name                                  | Type        | Used as            |
|---------------------------------------|-------------|--------------------|
| <a href="#">IAMUserChangePassword</a> | 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<br><input type="text" value="NewUser"/> | Value - optional<br><input type="text" value="Om_Shete"/> | <b>Remove</b> |
|---|---|---------------|

**Add new tag**  
You can add up to 49 more tags.

Cancel **Previous** **Create user**

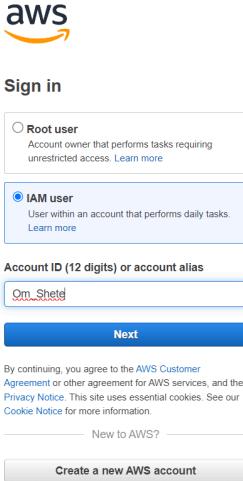
CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS Management Console with the IAM service selected. A green success banner at the top states "User created successfully" and provides instructions to view and download the user's password and email instructions for signing in to the AWS Management Console. Below the banner, the "Create user" step is completed, showing the "Specify user details" section. The "Console sign-in details" section displays the console sign-in URL (<https://myaliascd7.signin.aws.amazon.com/console>), user name (Om\_Shete), and console password (represented by a series of asterisks). Buttons for "Download .csv file" and "Return to users list" are visible at the bottom right.

The screenshot shows the Windows File Explorer interface. The left sidebar shows navigation options like Home, Gallery, Om - Personal, Desktop, Documents, Pictures, Downloads, and This PC. The main area displays three recently downloaded files: "Om\_Shete\_create\_dentails" (Excel document icon), "mykeypair.pem" (text file icon), and "CCL\_EXP6" (Chrome icon). A "Today" folder is also visible. The status bar at the bottom indicates there are 31 items in the folder.

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

---



The screenshot shows the AWS sign-in interface. It has two radio button options: "Root user" (unchecked) and "IAM user" (checked). Below the "IAM user" option is a text input field containing "Om\_Shete". A blue "Next" button is at the bottom. To the right of the input fields, there is a link "New to AWS?" and a button "Create a new AWS account". At the bottom of the form, a small note about AWS Customer Agreement and Privacy Notice is visible.

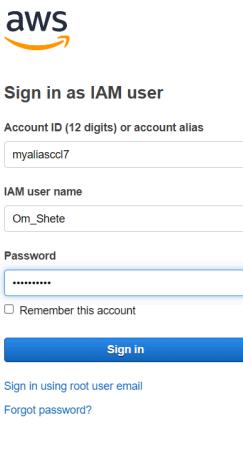
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.  
[https://aws.amazon.com/premiumsupport/plans/?sc\\_icampaign=aware\\_console\\_signin\\_Serv...](https://aws.amazon.com/premiumsupport/plans/?sc_icampaign=aware_console_signin_Serv...)

English ▾



The screenshot shows the AWS Support landing page. It features a purple gradient background with the "AWS Support" logo at the top. Below it, the text "Save time and move faster with expert guidance and assistance" is displayed, followed by a "Select a Support plan >" link. A small note at the bottom left says "New to AWS?".

---



The screenshot shows the "Sign in as IAM user" interface. It includes fields for "Account ID (12 digits) or account alias" (containing "myaliascd7"), "IAM user name" (containing "Om\_Shete"), and "Password" (containing "\*\*\*\*\*"). There is also a "Remember this account" checkbox and a "Sign in" button. Below the form are links for "Sign in using root user email" and "Forgot password?".

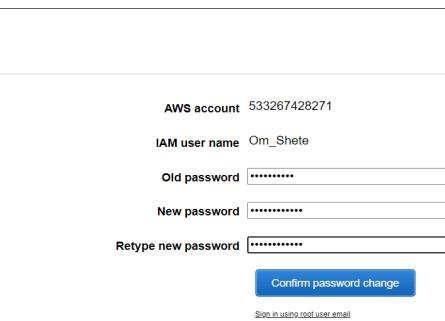
English ▾

<https://aws.amazon.com>



The screenshot shows the Amazon Lightsail landing page. It features a dark background with a bright orange and yellow swoosh graphic. The "Amazon Lightsail" logo is at the top, followed by the text "Lightsail is the easiest way to get started on AWS". A "Learn more >" button and a cartoon robot icon are present. At the bottom, there is a "Sign in" button.

---



The screenshot shows the "Change Password" interface. It displays the "AWS account" number (533267428271), "IAM user name" (Om\_Shete), and three password input fields: "Old password", "New password", and "Retype new password", all containing "\*\*\*\*\*". A "Confirm password change" button is at the bottom. Below the form is a link "Sign in using root user email".

English ▾

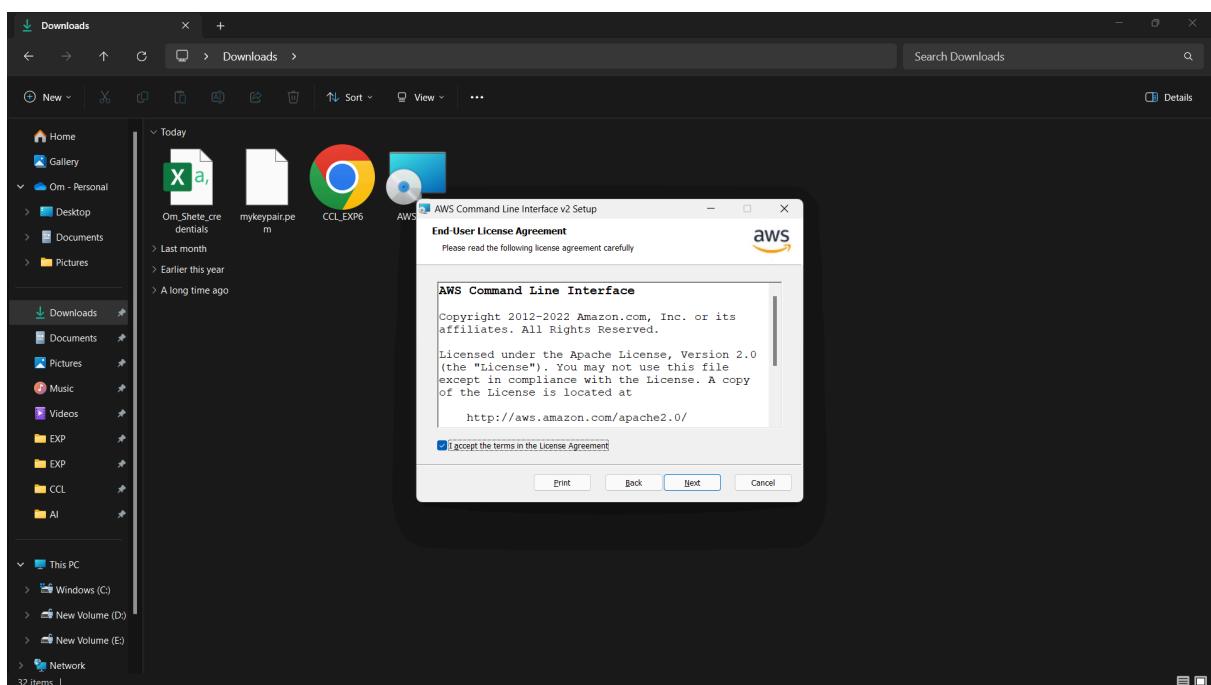
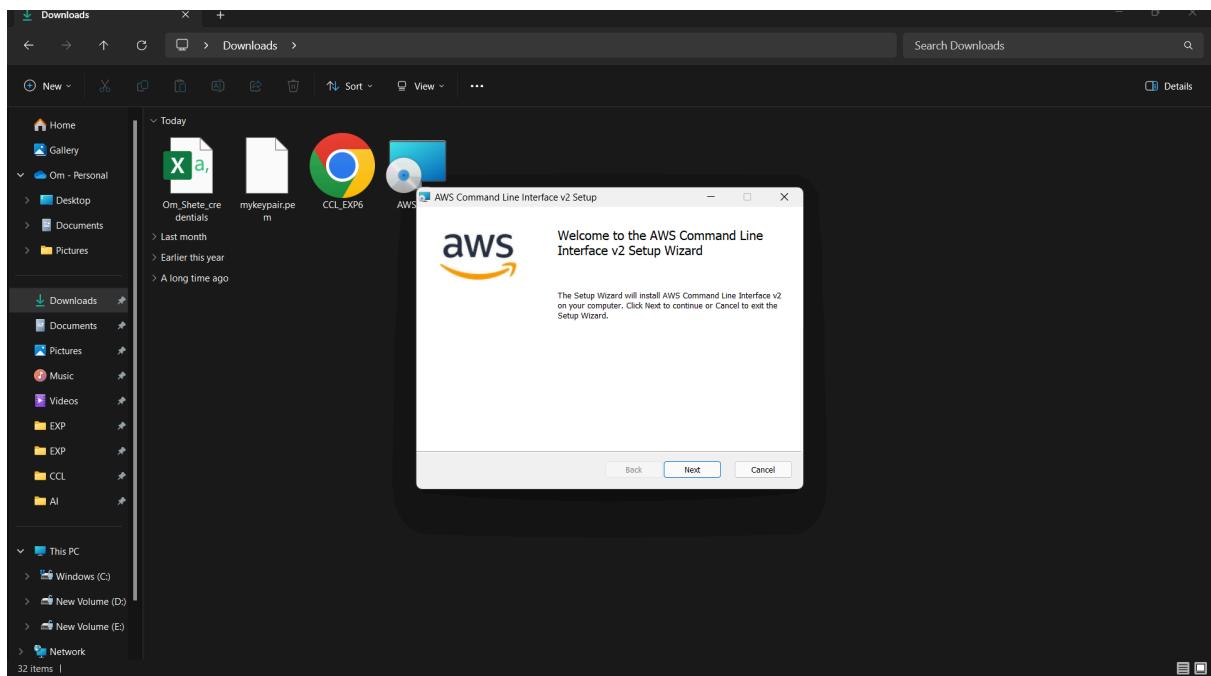
<https://aws.amazon.com>

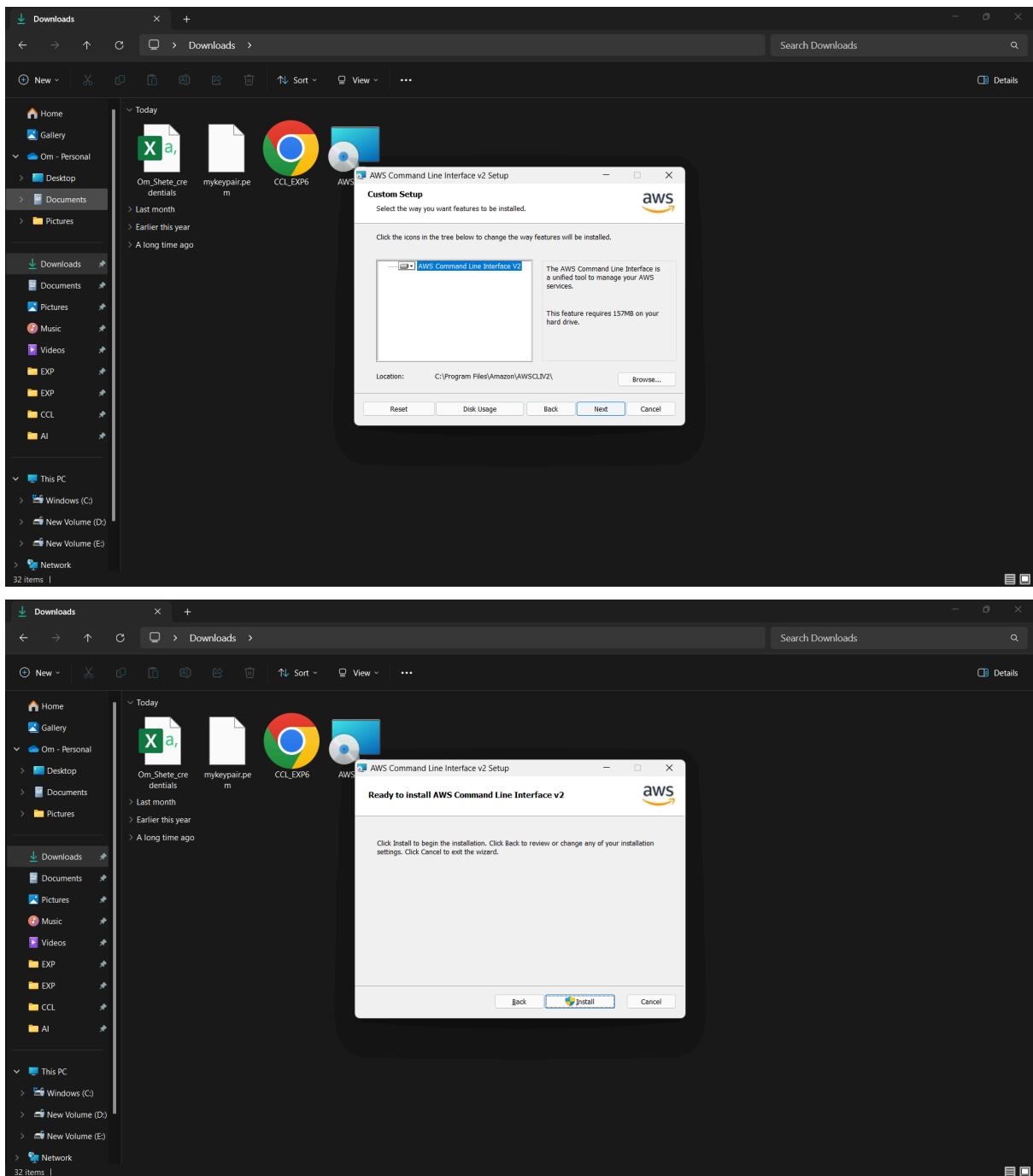
After logging in, you will notice that you don't have permission to do anything yet

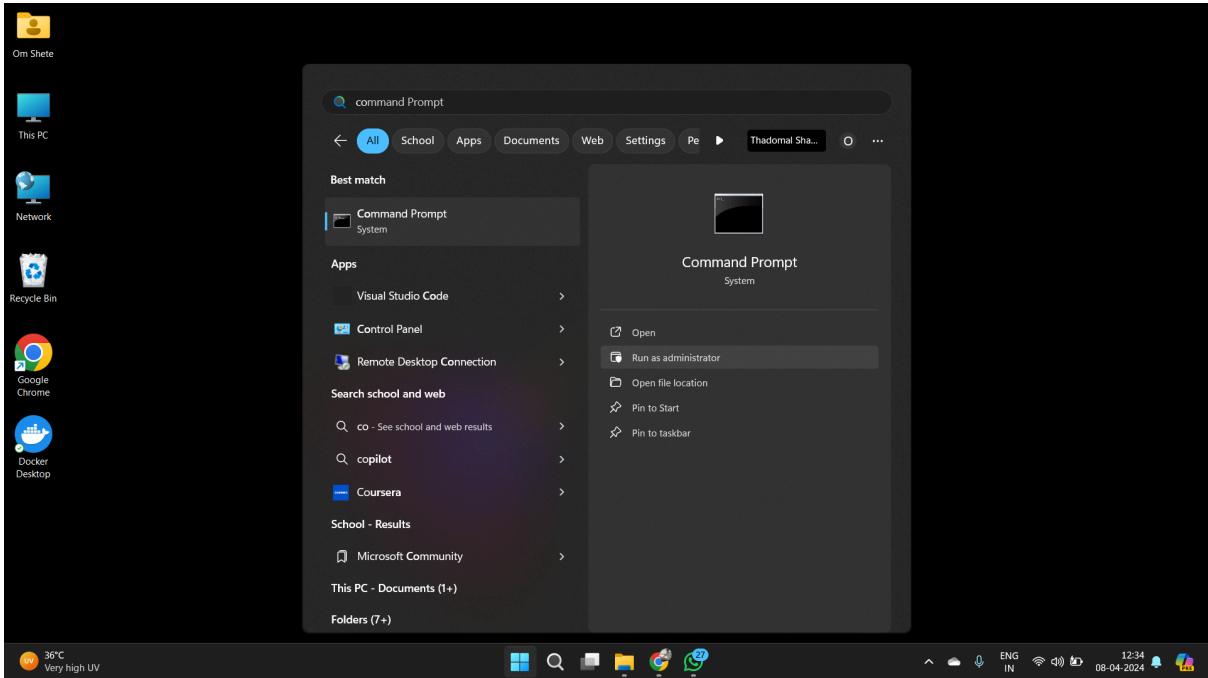
The image consists of three vertically stacked screenshots of the AWS console, all showing an "Access denied" error message.

- Screenshot 1: AWS Console Home**  
Shows the "Recently visited" section with a placeholder icon and the message "No recently visited services". Below it, a link to "View all services". To the right, the "Applications" section shows "0" items with the message "Access denied".
- Screenshot 2: EC2 Dashboard**  
Shows the "Instances" section. A search bar at the top has the placeholder "Find Instance by attribute or tag (case-sensitive)". Below it, a table header includes columns for "Name", "Instance ID", "Instance state", "Instance type", "Status check", "Alarm status", and "Availability Zone". A prominent error message states: "You are not authorized to perform this operation. User: arn:aws:iam::533267428271:user/Om\_Shete is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action".
- Screenshot 3: Amazon S3**  
Shows the "Buckets" section. The "General purpose buckets" tab is selected. A search bar at the top has the placeholder "Find buckets by name". Below it, a table header includes columns for "Name", "AWS Region", "IAM Access Analyzer", and "Creation date". A prominent error message states: "You don't have permissions to list buckets. After you or your AWS administrator has updated your permissions to allow the s3>ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3".

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







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

```
C:\Windows\System32>aws configure
AWS Access Key ID [None]: AKIAKYKJXGOXV4Z3JQKJ
AWS Secret Access Key [None]: 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
Default region name [None]: Stockholm
Default output format [None]: json

C:\Windows\System32>
```

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

```
C:\Windows\System32>aws --version
aws-cli/2.15.36 Python/3.11.8 Windows/10 exe/AMD64 prompt/off

C:\Windows\System32>aws s3 ls
Could not connect to the endpoint URL: "https://s3.Stockholm.amazonaws.com/"

C:\Windows\System32>
```

Go in the security credentials tab under Users of IAM Dashboard

The screenshot shows the AWS IAM Dashboard. On the left, there's a navigation sidebar with options like Dashboard, Access management (Users, Roles, Policies, Identity providers, Account settings), Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity), and Service control policies (SCPs). The main area is titled "Identity and Access Management (IAM)". It shows basic user information: Created (April 08, 2024, 12:49 UTC+05:30), Last console sign-in (Never), and an Access key (Access key 2, with a "Create access key" button). Below this, there are tabs for Permissions, Groups, Tags, Security credentials (which is selected), and Access Advisor. Under the "Permissions" tab, it says "Permissions policies (1)". A table lists one policy: "Policy name: IAMUserChangePassword" (Type: AWS managed, Attached via Directly). There are buttons for "Add permissions" and "Create inline policy". Below this, there's a section for "Permissions boundary (not set)" and a note about generating policies based on CloudTrail events.

This screenshot shows the "Policies" page under the IAM section. The navigation bar includes IAM, Policies, and the specific policy name, IAMUserChangePassword. The policy details are shown in a table: Type (AWS managed), Creation time (November 15, 2016, 05:55 UTC+05:30), Edited time (November 16, 2016, 04:48 UTC+05:30), and ARN (arn:aws:iam::aws:policy/IAMUserChangePassword). Below this, there are tabs for Permissions, Entities attached, Policy versions (2), and Access Advisor. The "Permissions defined in this policy" section shows a summary table for the "Allow (1 of 407 services)" rule. The rule details are: Service (IAM), Access level (Limited: Read, Write), Resource (Multiple), and Request condition (None). There are buttons for "Summary" and "JSON".

Click on the “Manage” Hyperlink

**Screenshot 1: IAM User Summary**

**Screenshot 2: Select MFA device**

**Screenshot 3: Authenticator app setup**

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

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the navigation pane is visible with sections like 'Identity and Access Management (IAM)', 'Access management', 'Users', 'Access reports', and 'Organization activity'. The main content area displays a summary for a user named 'Om\_Shete'. A prominent green banner at the top states 'MFA device assigned' with a note about registering up to 8 MFA devices. Below this, the 'Summary' section provides details: ARN (arn:aws:iam::533267428271:user/Om\_Shete), Console access (Enabled with MFA), and two access keys (Access key 1 and Access key 2). The 'Security credentials' tab is selected. The 'Console sign-in' section shows a console sign-in link (https://myaliascl7.signin.aws.amazon.com/console) and a console password (Updated 25 minutes ago). The 'Multi-factor authentication (MFA)' section shows one MFA device assigned, with buttons for 'Remove', 'Resync', and 'Assign MFA device'.