

PRACTICAL-3

USERS and GROUPS

USERS :

- In cloud computing, users are individuals entities that require access to some cloud resource and services. Users can be human individuals or non-human entities (such as applications or services).
- Each user has a unique identity and is authenticated through credentials like usernames, passwords, API keys or certificates.
- Users are assigned permissions that define what actions they can perform within the cloud environment.

Key aspects of Users:

- Identity Management : Ensures each user has a unique identity.
- Authentication : Verifies user identity through methods like passwords or multi-factor authentication.
- Authorization : Determines what actions a user can perform based on permissions.
- Types : End users, service accounts, administrators and external users.

GROUPS :

- Groups in cloud computing are collections of users who share similar roles or access needs.
- Groups simplify permission management by allowing administration to assign permissions and policies collectively rather than individually.
- This approach is especially useful in large organizations, where managing individual user permissions can be complex.

Key Aspects of groups :

- Role-based access control (RBAC) : Assigns permissions based on roles to enhance security and reduce administrative tasks.
- Policy enforcement : Ensures consistent application of security processes across all group members.
- Scalability : Facilitates management of permissions for large numbers of users.
- Types : Security groups, resource groups and user groups.

(2) IDENTITY and ACCESS MANAGEMENT (IAM)?

- Identity and Access management (IAM) is a combination of policies of technologies that allows organizations to identify users and provide the right form of access as and when required.
- There has been a bust in the market with new applications and the requirements for an organization to use these applications has increased drastically.
- The services and resources you want to access can be specified in IAM. IAM doesn't provide any replica or backups. IAM can be used for many purpose such as if one wants to control access of individual groups access for your AWS resources.
- With IAM policies, managing permissions to your workforce and system to ensure least privilege permissions becomes easier.
- Components of Identity and Access Management (IAM).
 1. Roles
 2. Groups
 3. Policies
- IAM identifies classified as
 1. IAM users
 2. IAM groups
 3. IAM roles.

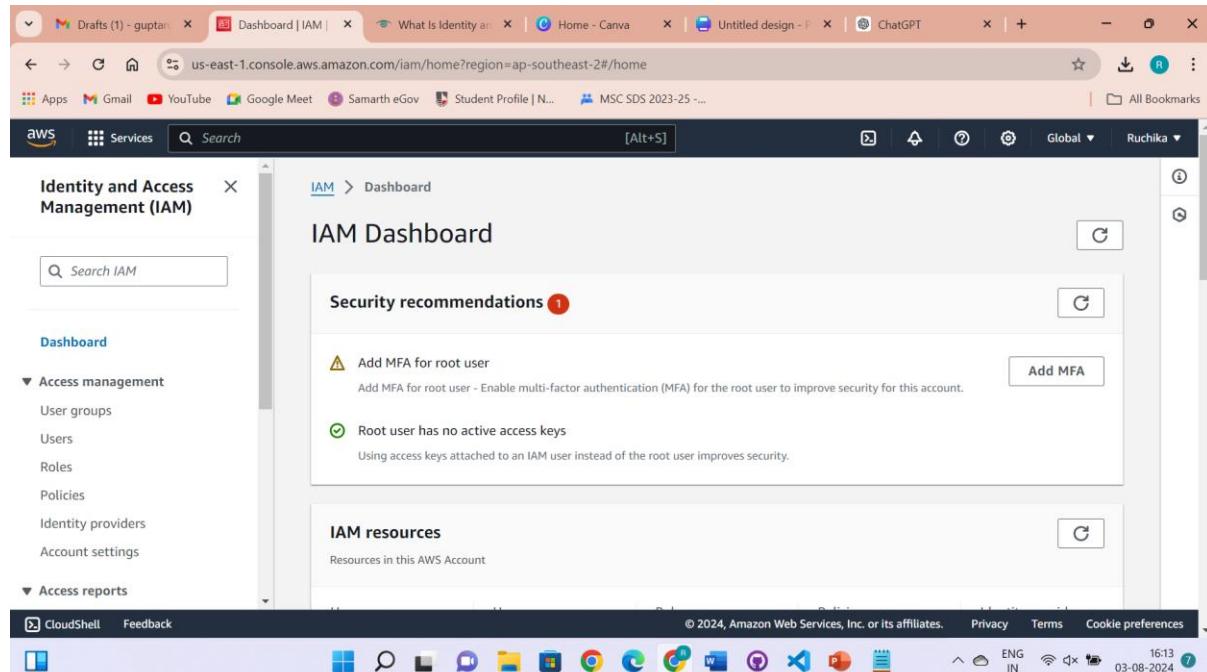
3. IAM ROLES

- A role is a set of permissions that grant access to actions and resources in AWS.
- These permissions are attached to the role, not to an IAM user or a group.
- An IAM user can use a role in the same AWS account or a different account.
- An IAM user is similar to a IAM user & role is also an AWS Identity with permission policies that determine what the identity can & cannot do in AWS.
- A role is not uniquely associated with a single person, it can be used by anyone who needs it.
- A role does not have long term security credential i.e. password or security key instead if the user uses a role, temporarily security credentials are instead created and provided to the user.
- You can use the roles to delegate access to users, application or services that generally do not have access to your AWS account/resources.

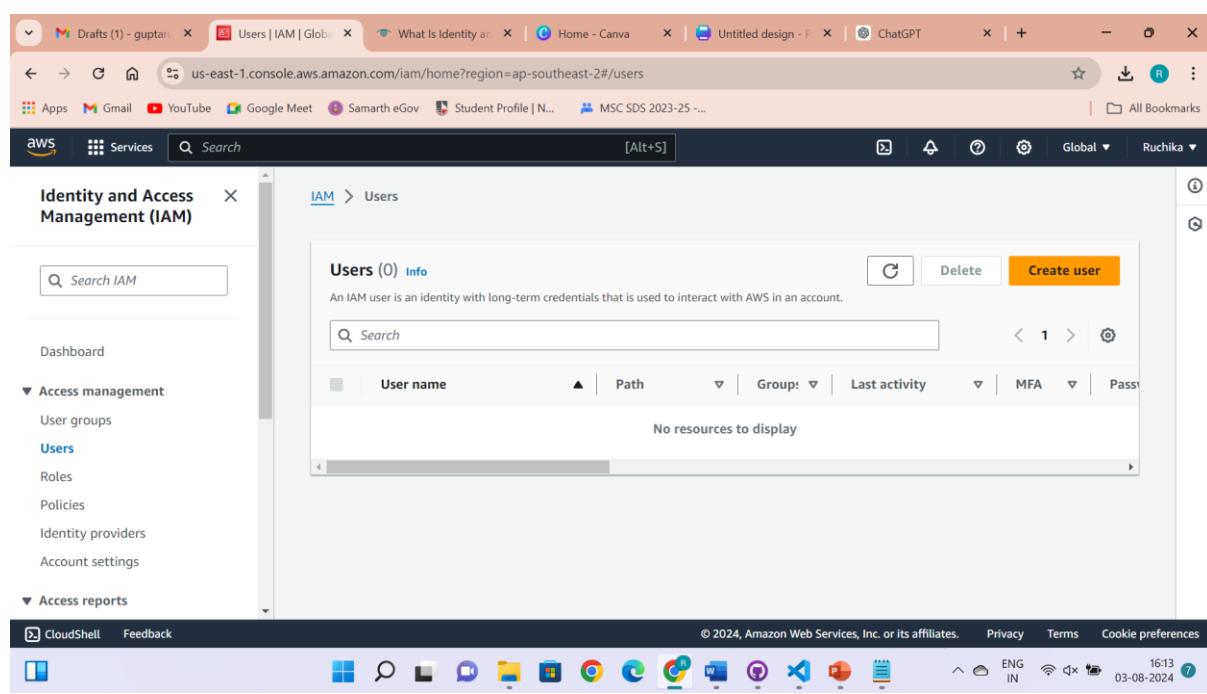
CLOUD COMPUTING

PRACTICAL-3

Ruchika (RollNo-19)
86062300062
Msc. Statistics and Data Science



The screenshot shows the AWS IAM Dashboard. On the left, a sidebar lists 'Identity and Access Management (IAM)' with options like 'Dashboard', 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), and 'Access reports'. The main area is titled 'IAM Dashboard' and contains two sections: 'Security recommendations' and 'IAM resources'. The 'Security recommendations' section has two items: 'Add MFA for root user' (status: 'Pending', button: 'Add MFA') and 'Root user has no active access keys' (status: 'Good'). The 'IAM resources' section shows 'Resources in this AWS Account'.



The screenshot shows the 'Users' page under 'Identity and Access Management (IAM)'. The sidebar is identical to the previous dashboard. The main area is titled 'Users (0) Info' and states 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' A search bar and a table header ('User name', 'Path', 'Group', 'Last activity', 'MFA', 'Pass') are shown. Below the table, it says 'No resources to display'.

The screenshot shows the 'Specify user details' step of the AWS IAM user creation wizard. On the left, a sidebar lists steps: Step 1 (Specify user details), Step 2 (Set permissions), and Step 3 (Review and create). The main area is titled 'User details' and contains a 'User name' field with 'ruchikasds'. Below it is a note about valid character ranges and a checkbox for 'Provide user access to the AWS Management Console - optional'. A callout box provides instructions for generating programmatic access keys. At the bottom right are 'Cancel' and 'Next' buttons.

The screenshot shows the 'Set permissions' step of the AWS IAM user creation wizard. The sidebar shows Step 1 (Specify user details) is selected. The main area is titled 'Permissions options' and displays three choices: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. A callout box at the bottom left encourages creating a group and attaching policies. At the bottom right are 'Create group' and 'Next' buttons.



The screenshot shows the 'Create user' wizard in the AWS IAM console. The user has completed Step 1 ('Specify user details') and Step 2 ('Set permissions'). In Step 1, the user name is set to 'ruchikasds'. In Step 2, the 'Permissions summary' table is empty, indicating 'No resources'. The wizard is currently at Step 3 ('Review and create').

| User name | Console password type | Require password reset |
|------------|-----------------------|------------------------|
| ruchikasds | None | No |

Permissions summary

| Name | Type | Used as |
|--------------|------|---------|
| No resources | | |

The screenshot shows the 'Users' page in the AWS IAM console. A green success message at the top states 'User created successfully'. The main table lists one user: 'ruchikasds'. The table includes columns for User name, Path, Group, Last activity, MFA, and Password last used.

| User name | Path | Group | Last activity | MFA | Password last used |
|------------|------|-------|---------------|-----|--------------------|
| ruchikasds | / | 0 | - | - | - |

Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

The screenshot shows the AWS IAM console interface. On the left, a sidebar lists navigation options like Dashboard, Access management (with sub-options User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports. The main content area displays user details for 'ruchikasds'. It includes a summary card with 'Created' date (August 03, 2024) and 'Last console sign-in' (not shown). Below this, tabs for Permissions, Groups, Tags, Security credentials (which is selected), and Access Advisor are visible. Under the Security credentials tab, there's a 'Console sign-in' section with a 'Console sign-in link' (https://654654461833.signin.aws.amazon.com/console) and a note that 'Console password' is 'Not enabled'. There's also a 'Multi-factor authentication (MFA)' section with a table header for Type, Identifier, Certifications, and Created on.

A modal dialog box titled 'Enable console access' is open. It asks for enabling console access for the user 'ruchikasds'. The 'Custom password' option is selected, and a password field contains '.....'. Below the field are two validation rules: 'Must be at least 8 characters long' and '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) = [] { } ; !'. There are two checkboxes: 'Show password' (unchecked) and 'User must create new password at next sign-in' (unchecked). At the bottom are 'Cancel' and 'Enable console access' buttons.

The screenshot shows the AWS IAM console with a modal window titled "Console password" open. The message inside 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 this, it shows the "Console sign-in URL" as <https://654654461833.signin.aws.amazon.com/console>, the "User name" as "ruchikads", and the "Console password" as a masked string. There are "Download .csv file" and "Close" buttons at the bottom. The background shows the IAM service dashboard with various navigation options like Dashboard, Access management, and Policies.

Console sign-in link copied

https://654654461833.signin.aws.amazon.com/console

IAM USER (S3 CREATING BUCKET)

The screenshot shows the AWS Console Home page. On the left, there's a service menu with a "Next" button. In the center, there's a "No recently visited services" message with links to EC2, S3, RDS, and Lambda. On the right, there's a "Applications" section showing a single entry for "eu-north-1 (Current Region)" with a note: "Region: Europe (Stockholm)". Below this, there's a table with a single row showing an "Access denied" message. The top of the screen shows the AWS logo, a search bar, and the user "ruchikads @ 6546-5446-1833". The bottom of the screen shows standard Windows taskbar icons and system status indicators.

Create S3 bucket | S3 | ap-south-1

ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general

Gmail YouTube Google Meet Samarth eGov Student Profile | N... MSC SDS 2023-25 ... Mumbai ruchikasds @ 6546-5446-1833 All Bookmarks

Services Search [Alt+S] Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-1

Bucket name [Info](#)
gjnvfjdfkscdnvjnsj

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)
Format: s3://bucket/prefix

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership

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

CloudShell Feedback ENG IN 16:35 03-08-2024

Create S3 bucket | S3 | ap-south-1

ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general

Gmail YouTube Google Meet Samarth eGov Student Profile | N... MSC SDS 2023-25 ... Mumbai ruchikasds @ 6546-5446-1833 All Bookmarks

Services Search [Alt+S] Create bucket Info

Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

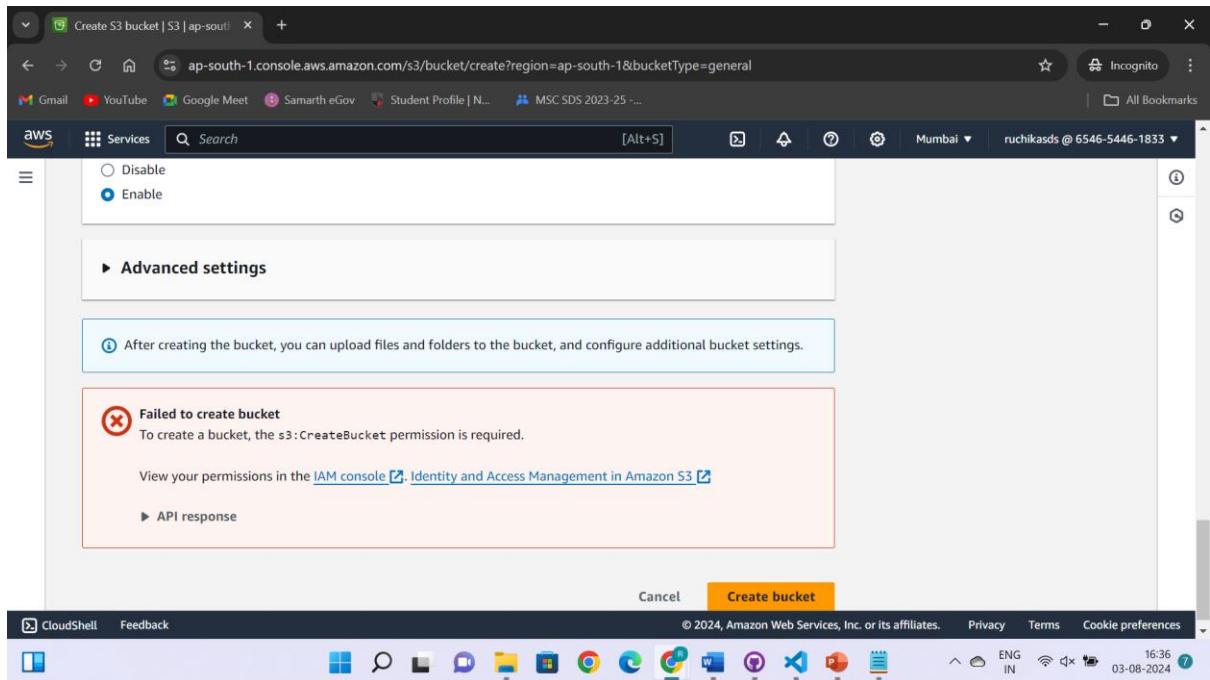
Disable Enable

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel [Create bucket](#)

CloudShell Feedback ENG IN 16:35 03-08-2024



POLICY

The screenshot shows the AWS IAM console. The left sidebar has sections for 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'User groups', 'Users', 'Roles', 'Policies' selected), 'Identity providers', and 'Account settings'. The main area is titled 'Policies (1221) Info' and describes a policy as an object in AWS that defines permissions. It includes a search bar, a filter for 'All types', and a table with columns: Policy name, Type, Used as, and Description. The table lists several AWS managed policies like 'AccessAnalyzerServiceRolePolicy', 'AdministratorAccess', etc. The bottom of the screen shows a Windows taskbar with various icons and system status.

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

S3

Set permissions for S3

Specify what actions can be performed on specific resources in S3.

Actions allowed

Specify actions from the service to be allowed.

All S3 actions (s3:*)

Effect

Allow Deny

Dependent permissions not selected.
To grant permissions for the selected resource actions, including additional dependent actions might be required.

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

S3

Set permissions for S3

Specify what actions can be performed on specific resources in S3.

Actions allowed

Specify actions from the service to be allowed.

All S3 actions (s3:*)

Effect

Allow Deny

Dependent permissions not selected.
To grant permissions for the selected resource actions, including additional dependent actions might be required.

Screenshot of the AWS IAM console showing the creation of a new policy. The policy is titled "Create policy" and is being created in the "ap-south-1" region.

The "Resources" section is expanded, showing the following configuration:

- Resource ARNs: All
- Action: s3:PutReplicationConfiguration
- Condition: None

A note at the top right of the Resources section states:
• s3:PauseReplication requires [2 more actions](#).
• s3:PutReplicationConfiguration requires [1 more action](#).

The "Request conditions - optional" section is collapsed.

At the bottom of the Resources section, there is a button to "Add more permissions".

Below the Resources section, a summary bar shows:
Security: 0 Errors: 0 Warnings: 0 Suggestions: 2

The "Permissions defined in this policy" section is expanded, showing the following details:

- Policy Name: Create policy
- Description: Add a short explanation for this policy.
- Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

The "Allow (1 of 420 services)" table shows the following permission entry:

| Service | Access level | Resource | Request |
|---------|--------------|---------------|---------|
| S3 | Full access | All resources | None |

There is a link to "Edit" the policy.

The browser status bar at the bottom indicates: © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 16:49 03-08-2024

The screenshot shows the 'Create policy' wizard in the AWS IAM console. The current step is 'Specify permissions'. A table lists one service, S3, with 'Full access' as the access level and 'All resources' as the resource. An optional 'Add tags' section is present.

| Service | Access level | Resource | Request |
|---------|--------------|---------------|---------|
| S3 | Full access | All resources | None |

Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.

Cancel Previous Create policy

The screenshot shows the 'Review and create' step of the wizard. It displays the policy name 'S3policy', a description 'Full ACCESS', and a summary of permissions: 'Permissions defined in this policy'.

Step 1
Specify permissions

Step 2
Review and create

Policy details

Policy name
Enter a meaningful name to identify this policy.
S3policy
Maximum 128 characters. Use alphanumeric and '+,-,@,_' characters.

Description - optional
Add a short explanation for this policy.
Full ACCESS
Maximum 1,000 characters. Use alphanumeric and '+,-,@,_' characters.

Permissions defined in this policy Info

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

CloudShell Feedback 16:50 03-08-2024

Screenshot of the AWS IAM Policies page showing a newly created policy named "S3policy".

The "Policies" table shows one item:

| Policy name | Type | Used as | Description |
|-------------|------------------|---------|-------------|
| S3policy | Customer managed | None | Full ACCESS |

Screenshot of the AWS IAM Users page showing a single user named "ruchikasds".

The "Users" table shows one item:

| User name | Path | Group | Last activity | MFA | Password last changed |
|------------|------|-------|----------------|-----|-----------------------|
| ruchikasds | / | 0 | 17 minutes ago | - | 15 days ago |

The screenshot shows the AWS IAM User Details page for the user 'ruchikasds'. The 'Summary' tab is selected, displaying the following information:

- ARN:** arn:aws:iam::654654461833:user/ruchikasds
- Console access:** Enabled without MFA
- Access key 1:** Create access key
- Created:** August 03, 2024, 16:15 (UTC+05:30)
- Last console sign-in:** Never

The navigation bar on the left includes links for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports.

The screenshot shows the 'Add permissions' step in the AWS IAM User Details page. The 'Permissions' tab is selected in the top navigation bar.

Permissions policies (0): Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Actions: Search, Remove, Add permissions

The URL in the browser is <https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/ruchikasds?section=permissions>.

The screenshot shows the first step of the 'Add permissions' wizard in the AWS IAM console. It displays three options:

- Add user to group: Adds user to an existing group, or creates a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions: Copies all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
- Attach policies directly: Attaches 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.

Below this, a section titled 'Permissions policies (1224)' is shown, with a search bar and filters for 'Policy name' (S3policy), 'Type' (Customer managed), and 'Attached entities' (0). Buttons for 'Cancel' and 'Next' are at the bottom right.

The screenshot shows the second step of the 'Add permissions' wizard, displaying a summary message: '1 policy added'. The summary table shows the following details for the attached policy:

| ARN | Console access | Access key 1 |
|---|---------------------|-------------------|
| arn:aws:iam::654654461833:user/ruchikasds | Enabled without MFA | Create access key |

The 'Permissions' tab is selected in the navigation bar. A link to 'Permissions policies (1)' is shown below the summary table.

The screenshot shows the AWS S3 console with a green success message at the top: "Successfully created bucket 'gjnvfjkscdnvjns'". Below it, a sub-header says "To upload files and folders, or to configure additional bucket settings, choose View details." The main interface displays an "Account snapshot - updated every 24 hours" with a "View Storage Lens dashboard" button. Below this, there are tabs for "General purpose buckets" and "Directory buckets", with "General purpose buckets" selected. It shows 4 buckets in the list, each with a "C" icon, "Copy ARN" button, "Empty" button, and "Delete" button. A prominent orange "Create bucket" button is located on the right. The bottom of the screen includes a navigation bar with "CloudShell" and "Feedback" buttons, and a system tray showing the date and time as "03-08-2024 16:53".

IAM USER (EC2 CREATING INSTANCE)

The screenshot shows the AWS IAM console with the "Policies" page open. The left sidebar shows the "Identity and Access Management (IAM)" navigation pane with options like "Dashboard", "Access management", "Policies", and "Access reports". The main area shows a table of policies with 1222 entries. The columns include "Policy name", "Type", "Used as", and "Description". Some visible policy names include "AccessAnalyzerServiceRole", "AdministratorAccess", "AdministratorAccess", "AdministratorAccess", and "AlexaForBusinessDeviceSetup". The bottom of the screen includes a navigation bar with "CloudShell" and "Feedback" buttons, and a system tray showing the date and time as "03-08-2024 16:55".

The screenshot shows the AWS IAM Policy Editor interface. The top navigation bar includes links for Drafts (1), www.techtarget.com, Home - Canva, Untitled design, ChatGPT, Create policy, Authentication, and other browser tabs. The main title is "Specify permissions". Below it, a sub-header says "Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor." The "Policy editor" section has tabs for "Visual" (selected), "JSON", and "Actions". Under "Actions allowed", there is a search bar labeled "Filter Actions" and an "Effect" dropdown with "Allow" selected. A "Policy Errors" modal is open, displaying a red circle with an "X" and the message "Missing required field Action cannot be empty!". The JSON code area shows a partially defined policy statement:

```
1 Version: "2012-10-17",
2 Statement: [
3   {
4     Sid: "ruchikasds",
5     Effect: "Allow",
6     Action: [],
7     Resource: []
8   }
9 ]
10 ]
11 }
```

The screenshot shows the 'Actions allowed' section of the AWS IAM 'Create policy' wizard. It lists various actions under 'All EC2 actions (ec2:*)'. A search bar labeled 'Filter Actions' is available. The 'Effect' dropdown is set to 'Allow'. A note at the top says 'Specify what actions can be performed on specific resources in EC2.'

Actions allowed

Specify actions from the service to be allowed.

Filter Actions

Effect
Allow Deny

Manual actions | Add actions

All EC2 actions (ec2:*)

Access level

List (Selected 175/175)

Read (Selected 36/36)

Write (Selected 420/420)

Permissions management (Selected 5/5)

Tagging (Selected 2/2)

Expand all | Collapse all

The screenshot shows the 'Resources' section of the AWS IAM 'Create policy' wizard. It allows specifying resource ARNs for actions. A note says 'The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.' A 'Request conditions - optional' section is also present.

Resources

Specify resource ARNs for these actions.

All

Specific

The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.

Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

Add more permissions

Security: 0 Errors: 0 Warnings: 0 Suggestions: 2

Cancel Next

Screenshot of the AWS IAM 'Create policy' wizard - Step 1: Specify permissions.

Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+,-,@-' characters.

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+,-,@-' characters.

Allow (1 of 420 services) Show remaining 419 services

| Service | Access level | Resource | Request |
|---------|--------------|---------------|---------|
| EC2 | Full access | All resources | None |

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag
You can add up to 50 more tags.

Create policy

Drafts (1) - g... | www.techarg... | Home - Canva | Untitled desi... | ChatGPT | Policies | IAM | Authentication | +

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies

aws Services Search [Alt+S]

Identity and Access Management (IAM)

Policy ec2service created.

IAM > Policies

Policies (1223) Info

A policy is an object in AWS that defines permissions.

Filter by Type

| Policy name | Type | Used as | Description |
|-------------|------------------|----------------------|-------------|
| ec2service | Customer managed | None | Full access |
| S3policy | Customer managed | Permissions polic... | Full ACCESS |

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 16:59 03-08-2024

Drafts (1) - g... | www.techarg... | Home - Canva | Untitled desi... | ChatGPT | ec2service | IAM | Authentication | +

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A654654461833%3Apolicy%2F...

aws Services Search [Alt+S]

Identity and Access Management (IAM)

Policy ec2service created.

IAM > Policies > ec2service

ec2service Info

Full access

Policy details

| Type | Creation time | Edited time | ARN |
|------------------|------------------------------------|------------------------------------|---|
| Customer managed | August 03, 2024, 16:59 (UTC+05:30) | August 03, 2024, 16:59 (UTC+05:30) | arn:aws:iam::654654461833:policy/ec2service |

Permissions Entities attached Tags Policy versions (1) Access Advisor

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 16:59 03-08-2024

Screenshot of the AWS IAM "Add permissions" step 1 screen.

The URL is us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/details/ruchikasds/add-permissions.

The "Permissions options" section shows three choices:

- 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, inline policies, and any existing permissions boundaries 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.

The "Permissions policies (1224)" section lists policies:

| Policy name | Type | Attached entities |
|----------------------------|------------------|-------------------|
| ec2service | Customer managed | 0 |

Buttons at the bottom: "Cancel" and "Next".

Screenshot of the AWS IAM 'Add permissions' review step.

User details:

| | |
|-----------|------------|
| User name | ruchikasds |
|-----------|------------|

Permissions summary (1):

| Name | Type | Used as |
|------------|------------------|--------------------|
| ec2service | Customer managed | Permissions policy |

Buttons: Cancel, Previous, Add permissions.

Screenshot of the AWS IAM user details page after adding a policy.

Identity and Access Management (IAM)

Summary:

| | | |
|--|-------------------------------------|---------------------------------|
| ARN: arn:aws:iam::654654461833:user/ruchikasds | Console access: Enabled without MFA | Access key 1: Create access key |
| Created: August 03, 2024, 16:15 (UTC+05:30) | Last console sign-in: Never | |

Permissions policies (2):

| | |
|--------|-----------------|
| Remove | Add permissions |
|--------|-----------------|

Permissions are defined by policies attached to the user directly or through groups.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 17:01 03-08-2024

Launch an instance | EC2 | ap-south-1

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

Name: k3g

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux, macOS, Ubuntu, Windows, Red Hat, ...

Browse more AMIs Including AMIs from AWS Marketplace

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 24.04 LTS, ...

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Launch instance

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 17:03 03-08-2024

Launch an instance | EC2 | ap-south-1

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

Create security group

We'll create a new security group called 'launch-wizard-3' with the following rules:

Allow SSH traffic from Anywhere

Allow HTTPS traffic from the internet

Allow HTTP traffic from the internet

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Configure storage

Root volume (Not encrypted): 1x 8 GiB gp3

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 24.04 LTS, ...

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Launch instance

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 17:03 03-08-2024

The screenshot shows the AWS EC2 Launch Instances wizard. The current step is "Select an existing key pair or create a key pair". A note at the top says: "We noticed that you didn't select a key pair. If you want to be able to connect to your instance it is recommended that you create one or select an existing one." There are three options: "Existing key pair" (radio button), "Create new key pair" (selected radio button), and "Proceed without key pair". Below these is a "Key pair name" input field with placeholder text "Enter key pair name". At the bottom right are "Cancel" and "Launch instance" buttons.

Select an existing key pair or create a key pair

We noticed that you didn't select a key pair. If you want to be able to connect to your instance it is recommended that you create one or select an existing one.

Existing key pair Create new key pair Proceed without key pair

Key pair name
Key pairs allow you to connect to your instance securely.
Enter key pair name

Cancel **Launch instance**

Success
Successfully initiated launch of instance (i-028b6ecaa17a3291c)

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email

Connect to your instance
Once your instance is running, log into it from your local computer.

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 17:04 03-08-2024 7

Instances | EC2 | ap-south-1

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:

Gmail YouTube Google Meet Samarth eGov Student Profile | N... MSCSDS 2023-25 ... Mumbai ruchikads @ 6546-5446-1833 All Bookmarks

EC2 Dashboard Services Search [Alt+S] Instance state Actions Launch Instances

Instances (2) Info Find Instance by attribute or tag (case-sensitive) All states

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status |
|----------|---------------------|----------------|---------------|--------------|-------------------|
| k3g | i-028b6ecaa17a3291c | Running | t2.micro | Initializing | User: arn:aws:ap- |
| cc_putty | i-05a2230ae513611c4 | Stopped | t2.micro | - | User: arn:aws:ap- |

Select an instance

AMI Catalog CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 17:04 03-08-2024 7

The screenshot shows the AWS EC2 Instances page with two instances listed: 'k3g' (running, t2.micro) and 'cc_putty' (stopped, t2.micro). The 'Launch Instances' button is highlighted. The left sidebar shows navigation options like EC2 Dashboard, Instances, and Images. The bottom of the screen shows the Windows taskbar with various pinned icons.