

Aim -

To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud.

Theory -

Identity as a Service (IDaaS) is a cloud-based service model that provides organizations with identity and access management (IAM) capabilities over the internet. In IDaaS, organizations can manage user identities, authentication, authorization, and access control policies centrally through a cloud-based platform, rather than deploying and managing IAM infrastructure on-premises.

Advantages of Identity as a Service (IDaaS):

- Centralized Identity Management: IDaaS enables organizations to centrally manage user identities, access controls, and authentication mechanisms across multiple applications and services. This centralization simplifies identity management tasks and improves administrative efficiency.
- Scalability: IDaaS platforms offer scalability features that allow organizations to easily scale their identity management infrastructure up or down based on changing requirements. This elasticity enables organizations to accommodate growing user populations and expanding application portfolios without the need for manual intervention.
- Cost Efficiency: IDaaS follows a pay-as-you-go pricing model, where organizations only pay for the identity management services and resources they consume. This eliminates the need for upfront investment in IAM infrastructure, reducing capital expenditure and enabling cost-effective scaling based on demand.
- Improved Security: Many IDaaS providers offer advanced security features, such as multi-factor authentication (MFA), single sign-on (SSO), identity federation, and risk-based authentication, to enhance security posture and protect against unauthorized access and data breaches.
- Enhanced User Experience: IDaaS platforms provide seamless and consistent authentication and access experiences for users across multiple applications and devices. Features such as single sign-on (SSO) and self-service password reset improve user convenience and productivity while reducing helpdesk support overhead.

Disadvantages of Identity as a Service (IDaaS):

- Data Privacy and Compliance Concerns: Storing and managing user identities and access control policies in a third-party cloud environment may raise

concerns about data privacy and compliance with regulatory requirements, such as GDPR or HIPAA. Organizations must carefully evaluate the data privacy and compliance measures implemented by IDaaS providers to ensure compliance with relevant regulations.

- Dependency on Internet Connectivity: IDaaS relies on internet connectivity for accessing and managing identity management services, which may pose challenges in environments with limited or unreliable internet connectivity. Organizations should consider the potential impact of internet outages or disruptions on their identity management operations.
- Vendor Lock-In: Migrating user identities and access controls between different IDaaS providers or transitioning from IDaaS to an on-premises IAM deployment may be challenging and costly, leading to vendor lock-in. Organizations should consider the long-term implications of vendor lock-in and evaluate strategies to mitigate this risk.
- Customization and Integration Challenges: IDaaS platforms may have limitations in terms of customization and integration with existing IAM systems, directory services, and legacy applications. Organizations with complex identity management requirements may encounter challenges in fully integrating IDaaS solutions into their existing infrastructure.
- Performance and Reliability: Performance and reliability issues may arise in IDaaS environments, particularly in multi-tenant deployments where resources are shared among multiple users. Organizations should assess the performance characteristics and service level agreements (SLAs) of IDaaS offerings to ensure they meet their performance and reliability requirements.

Procedure-

Login to AWS console

Make sure to check all Ec2 dashboard parameters

The screenshot shows the AWS EC2 Dashboard. On the left, a sidebar lists navigation options like Cloud9, EC2, Elastic Beanstalk, AWS Amplify, Lambda, S3, and API Gateway. The main content area displays 'Resources Info' with a summary of EC2 resources: Instances (running) 0, Auto Scaling Groups 0, Dedicated Hosts 0, Elastic IPs 0, Instances 0, Key pairs 0, Load balancers 0, Placement groups 0, Security groups 1, Snapshots 0, and Volumes 0. Below this is a 'Launch instance' section with 'Launch instance' and 'Migrate a server' buttons. To the right is a 'Service health' section showing the US East (N. Virginia) region with a status of 'This service is operating normally.' On the far right, there's an 'Account attributes' panel for the Default VPC (vpc-06f870b50074eb753) and a 'Explore AWS' panel with links to cost reduction and price performance.

Configuring IAM Dashboard

Go to IAM dashboard

The screenshot shows the AWS IAM Dashboard. The left sidebar includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access Analyzer, External access, Unused access, Analyzer settings), and 'CloudShell' and 'Feedback' buttons. The main area features a 'Security recommendations' section with two items: 'Add MFA for root user' (with a 'Add MFA' button) and 'Root user has no active access keys'. Below this is an 'IAM resources' section showing 0 User groups, 0 Users, 16 Roles, 12 Policies, and 0 Identity providers. To the right is an 'AWS Account' panel with the Account ID (689179663899), Account Alias (Create), and a sign-in URL (https://689179663899.signin.aws.amazon.com/console). A 'Quick Links' panel includes a 'My security credentials' link.

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

The screenshot shows the 'Create alias for AWS account' dialog box. It has a 'Preferred alias' input field containing 'mikil-alias'. Below it is a note: 'Must be no more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).' Under 'New sign-in URL', it shows 'https://mikil-alias.signin.aws.amazon.com/console'. A note below says: 'IAM users will still be able to use the default URL containing the AWS account ID.' At the bottom are 'Cancel' and 'Create alias' buttons.

The screenshot shows the AWS IAM Dashboard. At the top, a green banner displays the message "Alias mikil-alias created for this account." Below the banner, the "Security recommendations" section lists two items: "Add MFA for root user" (with a warning icon) and "Root user has no active access keys" (with a success icon). The "IAM resources" section shows summary counts for User groups (0), Users (0), Roles (16), Policies (12), and Identity providers (0). On the right side, there's a sidebar titled "AWS Account" showing the Account ID (689179663899) and Account Alias (mikil-alias). A "Quick Links" section includes a link to "My security credentials". The bottom of the screen includes standard AWS navigation links like CloudShell and Feedback.

Creating a new User

Click on “users” in the left column

The screenshot shows the "Users" page under the IAM service. The title bar says "IAM > Users". The main content area is titled "Users (0) Info" with the sub-instruction "An IAM user is an identity with long-term credentials that is used to interact with AWS in an account." Below this is a search bar and a table header with columns: User name, Path, Group, Last activity, MFA, Password age, and Console last sign-in. The table body is empty, displaying the message "No resources to display". The left sidebar follows the same structure as the first screenshot, with "Users" currently selected. The bottom of the screen includes standard AWS navigation links.

Click on Add users button

The screenshot shows the 'Specify user details' step of the IAM user creation wizard. The 'User name' field contains 'mikil1'. A note below it specifies character restrictions: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . - (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.

Step 1
Specify user details

User details

User name
mikil1

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.

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 a custom valid password (Imc: Qwertyuiop123) and check the Require password reset box which will make you create a next password in the next sign in

The screenshot shows the 'Set permissions' step of the IAM user creation wizard. It asks if console access is provided to a person, with the 'I want to create an IAM user' option selected. It then asks for a console password, with 'Custom password' chosen and 'password@123' entered. A note states that users must create a new password at next sign-in. A callout box provides instructions for generating programmatic access keys.

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.
password@123

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](#)

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

Click on Next

The screenshot shows the 'Set permissions' step of a user creation wizard. On the left, a sidebar lists steps: Step 1 (Specify user details), Step 2 (Set permissions - currently selected), Step 3 (Review and create), and Step 4 (Retrieve password). The main area is titled 'Set permissions' with the sub-section 'Permissions options'. It contains three 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.

Below these options is a 'Get started with groups' section with a 'Create group' button. A note says: '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.' A link to 'Learn more' is provided. At the bottom right are 'Cancel', 'Previous', and a large orange 'Next' button.

Add a tag if you want to just to keep track of your activities; then click on Next: Review

The screenshot shows the 'Review and create' step of the user creation wizard. The sidebar shows steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create - currently selected), and Step 4 (Retrieve password). The main area displays 'User details' for a user named 'mikil1'. It shows the console password type as 'Custom password' and 'Require password reset' as 'Yes'. Below this is a 'Permissions summary' table:

Name	Type	Used as
IAMUserChangePassword	AWS managed	Permissions policy

Below the table is a 'Tags - optional' section with a note: '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.' It shows 'No tags associated with the resource.'

At the bottom right are 'Cancel', 'Previous', and a large orange 'Next' button.

Click on Create User Button

The screenshot shows the AWS Management Console with the IAM service selected. A green success message at the top states "User created successfully". The main content area is titled "Retrieve password" and displays "Console sign-in details". It includes a "Console sign-in URL" (https://mikil-alias.signin.aws.amazon.com/console), a "User name" (mikil1), and a "Console password" (password@123). There is a "Hide" link next to the password. Buttons at the bottom include "Cancel", "Download .csv file", and "Return to users list".

Open the URL in Incognito Mode

Logging in as the new User & Checking their permissions

Enter the new user's name and password saved earlier

The screenshot shows the AWS sign-in page for an IAM user. The form fields are filled with the previously created user's information: Account ID (mikil-alias), IAM user name (mikil1), and Password (password@123). Below the form is a "Remember this account" checkbox and a "Sign in" button. To the right of the sign-in form is an advertisement for Amazon Lightsail, featuring a cartoon robot character and the text "Amazon Lightsail" and "Lightsail is the easiest way to get started on AWS". At the bottom of the page are links for "Sign in using root user email" and "Forgot password?", along with language selection ("English") and legal links ("Terms of Use Privacy Policy").

Enter a new valid password

Your authentication information is incorrect. Please try again.

AWS account 689179663899

IAM user name mikil1

Old password

New password

Retype new password

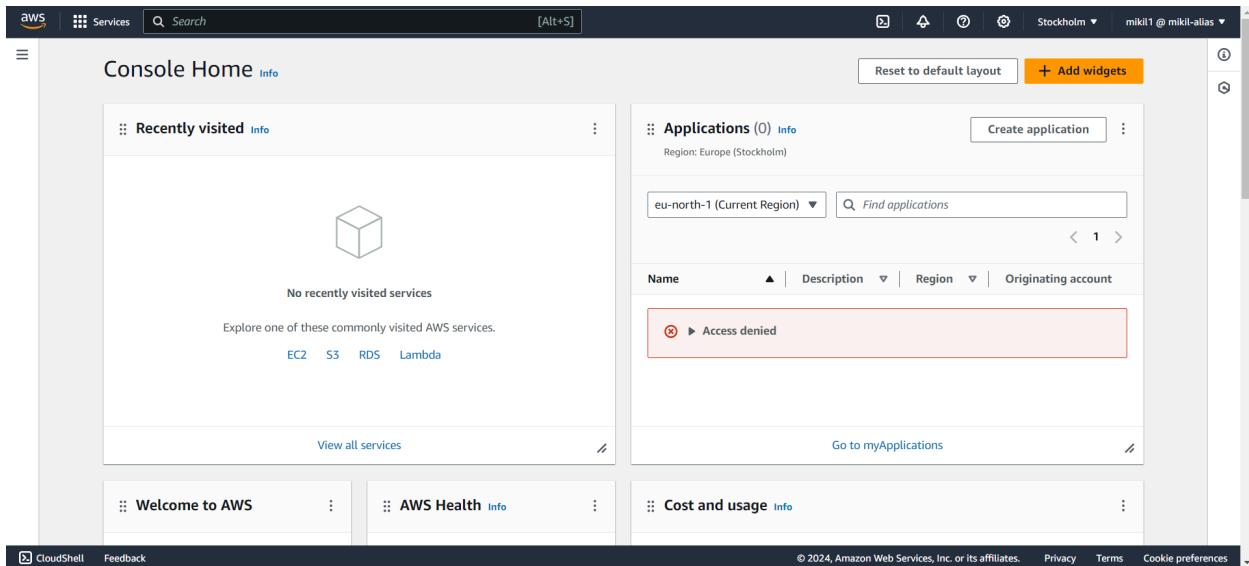
Confirm password change

[Sign in using root user email](#)

English

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

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



The screenshot shows the AWS Console Home page. On the left, there's a sidebar with 'Recently visited' services (none listed), a 'Welcome to AWS' section, and an 'AWS Health' section. The main content area is titled 'Applications (0)' and shows a table with one row. The row has a red border and contains a red circle with a white 'X' and the text 'Access denied'. The table has columns for Name, Description, Region, and Originating account. At the bottom of the page, there are links for CloudShell, Feedback, and cookie preferences.

Adding MFA for the user via Root User

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.

AWS Command Line Interface

The AWS Command Line Interface (AWS CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

The AWS CLI v2 offers several [new features](#) including improved installers, new configuration options such as AWS IAM Identity Center (successor to AWS SSO), and various interactive features.

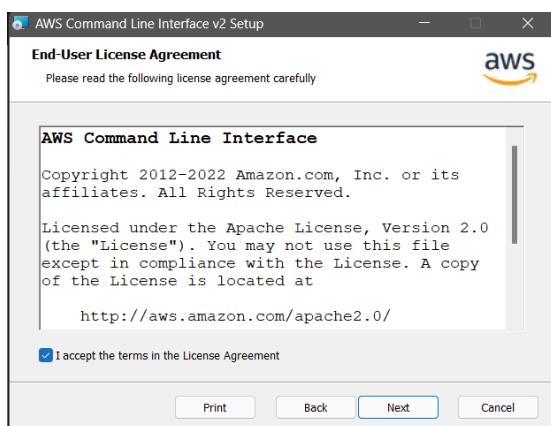
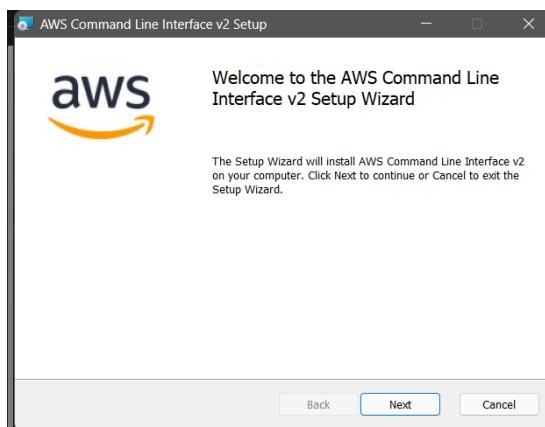
Windows
Download and run the [64-bit Windows installer](#).

MacOS
Download and run the [MacOS PKG installer](#).

Linux
Download, unzip, and then run the [Linux installer](#).

Amazon Linux
The AWS CLI comes pre-installed on [Amazon Linux AMI](#).

Release Notes
Check out the [Release Notes](#) for more information on the latest version.



Generate the AccessKeyID and Key needed for AWS CLI.

Identity and Access Management (IAM)

Console sign-in

Console sign-in link: <https://mikil-alias.signin.aws.amazon.com/console>

Console password: Updated 13 minutes ago (2024-03-16 15:08 GMT+5:30)

Last console sign-in: 14 minutes ago (2024-03-16 15:07 GMT+5:30)

Manage console access

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Device type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			
Assign MFA device			

Access keys (1)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

[Create access key](#)

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

Access Key best practices & alternatives

Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Step 2 - optional

Set description tag

Step 3

Retrieve access keys

Use case

Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

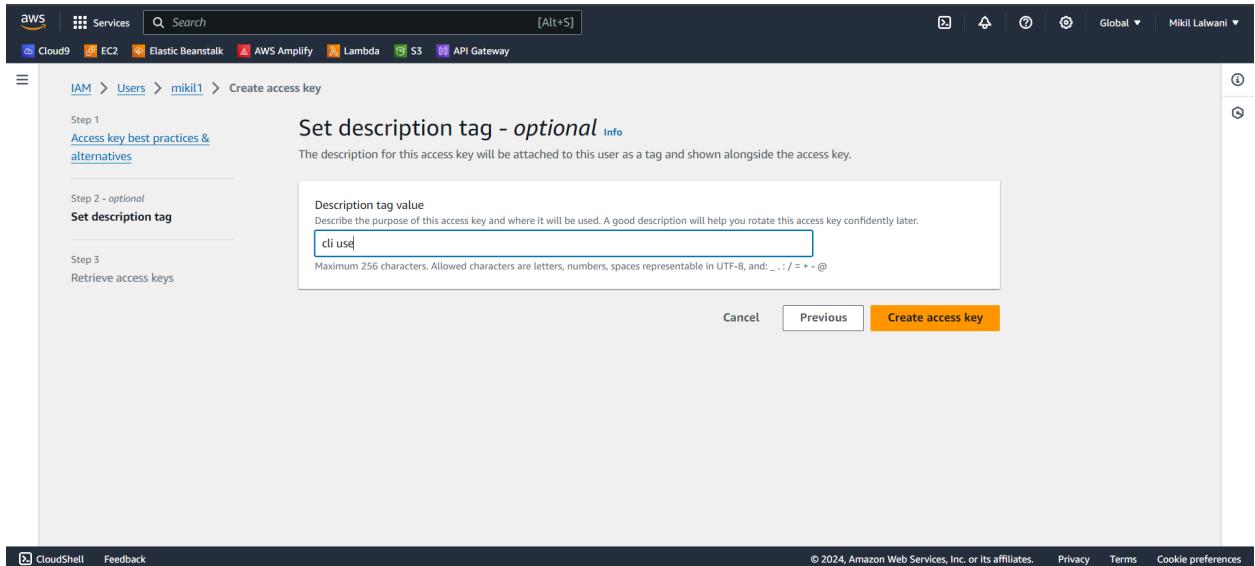
Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

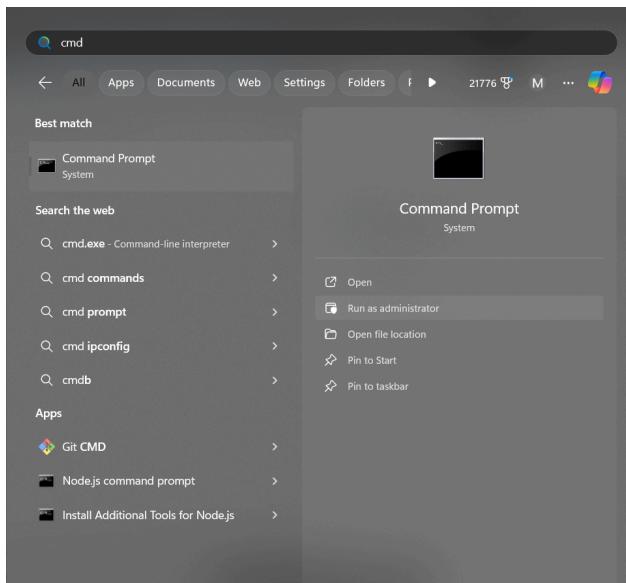
Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

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



Type “cmd” in the windows search bar and run it as an administrator



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: **ap-south-1**

The output format is **json** in our case

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>aws configure
AWS Access Key ID [None]: AKIA2A5SPDYN7T4UR5GN
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json

```

The next two steps are OPTIONAL:

`aws --version`

`aws s3 ls`

```

C:\Windows\System32>aws --version
aws-cli/2.15.30 Python/3.11.8 Windows/10 exe/AMD64 prompt/off

C:\Windows\System32>aws s3 ls
An error occurred (AccessDenied) when calling the ListBuckets operation: Access Denied

C:\Windows\System32>

```

Go in the security credentials tab under Users of IAM Dashboard

The screenshot shows the AWS IAM User Details page for a user named 'mikil1'. The 'Summary' section displays the ARN (arn:aws:iam::689179663899:user/mikil1), Console access status (Enabled without MFA), and two access keys. The 'Permissions' section shows one policy attached: 'Permissions policies (1)'. A 'Filter by Type' dropdown is visible.

ARN	Console access	Access key 1
arn:aws:iam::689179663899:user/mikil1	Enabled without MFA	AKIA2A5SPDYN7T4UR5GN - Active Never used. Created today.
Created March 16, 2024, 15:06 (UTC+05:30)	Last console sign-in Today	Access key 2 Create access key

Permissions policies (1)

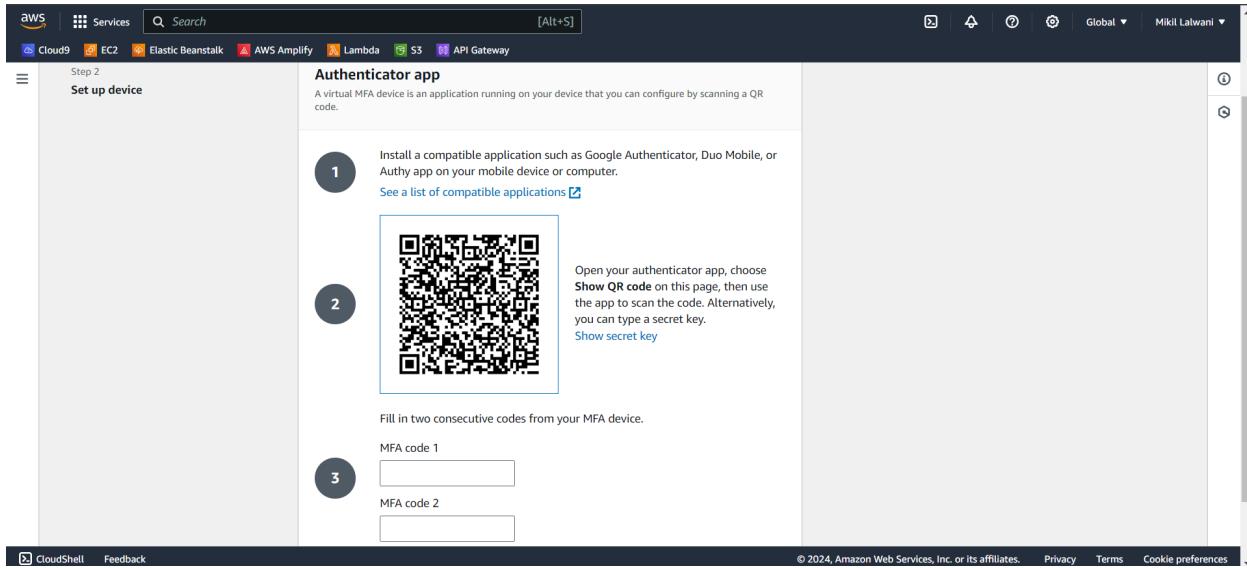
Filter by Type

Click on the “Assign MFA Device” Hyperlink

Screenshot of the AWS IAM console showing the Security credentials tab. It displays the 'Console sign-in' section with a link to the sign-in page and a 'Manage console access' button. Below it is the 'Multi-factor authentication (MFA)' section, which is currently empty and has a button to 'Assign MFA device'.

Screenshot of the AWS IAM console showing the 'Set up device' step for MFA setup. It shows the 'MFA device name' input field with 'mikil1-mfa' entered. Below it is the 'MFA device' selection section, which includes options for 'Authenticator app' (selected) and 'Security Key'.

Use the Google Authenticator app downloaded earlier to scan the QR Code



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 IAM 'Identity and Access Management (IAM)' page. It displays the assigned MFA device details, including the ARN, status, creation date, last sign-in information, and access key details. The 'Security credentials' tab is selected.

ARN	Status	Created	Last console sign-in	Access key
arn:aws:iam::689179663899:user/mikil1	Enabled with MFA	March 16, 2024, 15:06 (UTC+05:30)	Today	AKIA2A5SPDYN/T14UR5GN - Active Never used. Created today.

Console sign-in

Console sign-in link: <https://mikil-alias.sigin.aws.amazon.com/console>

Console password: Updated 26 minutes ago (2024-03-16 15:08 GMT+5:30)

Last console sign-in: 26 minutes ago (2024-03-16 15:07 GMT+5:30)

Multi-factor authentication (MFA) (1)

Buttons: Remove, Resync, Assign MFA device

Logging in as the new user after MFA

Again try logging in via the new user created earlier; this time it will ask for MFA after you click on Sign In

Sign in as IAM user

Account ID (12 digits) or account alias
mikil-alias

IAM user name
mikil1

Password

Remember this account

Sign in

[Sign in using root user email](#)
[Forgot password?](#)



Use the code being shown in the Google Authenticator

 aws

Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code:

[Cancel](#)

[Submit](#)

Now, after opening the root user window again
After going in the Users section of IAM Dashboard, we can see that MFA has been activated for the new user

The screenshot shows the AWS IAM service interface. In the left sidebar, under 'Access management', 'Users' is selected. The main area displays a table titled 'Users (1) Info' with one entry: 'mikil1'. The table includes columns for User name, Path, Group, Last activity, MFA, Password age, and Console last sign-in. The 'Last activity' column shows 'Now' with a green circular icon. The 'Password age' column shows '27 minutes' with a green circular icon. The 'Console last sign-in' column shows 'March 16, 2024, 15:31' with a green circular icon.

Adding 2 More Users and Giving them permissions

Now, Adding 2 More Users

Not giving them an Access key and not checking the Psw Reset Checkbox; Click on the Next: Permissions

The screenshot shows the 'Create New User' wizard at Step 3: Set permissions. The 'User details' section shows the user name 'mikil2' entered. Below it, there's a note about character restrictions and a checkbox for 'Provide user access to the AWS Management Console - optional'. A large callout box highlights the 'User type' section, which contains two options: 'Specify a user in Identity Center - Recommended' (radio button unselected) and 'I want to create an IAM user' (radio button selected). A note below explains that IAM users are needed for programmatic access. The 'Console password' section shows 'Autogenerated password' selected, with a note that the password can be viewed after creation. 'Custom password' is also listed with a text input field containing 'password@123' and a note that it must be at least 8 characters long.

We will create a group later

We can see the previous user listed under the copy "permission from existing user" section (just for observation purpose)

Click on the third section: Attach existing policies directly

The screenshot shows the 'Set permissions' step of creating a new AWS user. The 'Copy permissions' option is selected. Below it, a table lists a single user named 'mikil1' with the policy 'IAMUserChangePassword' attached.

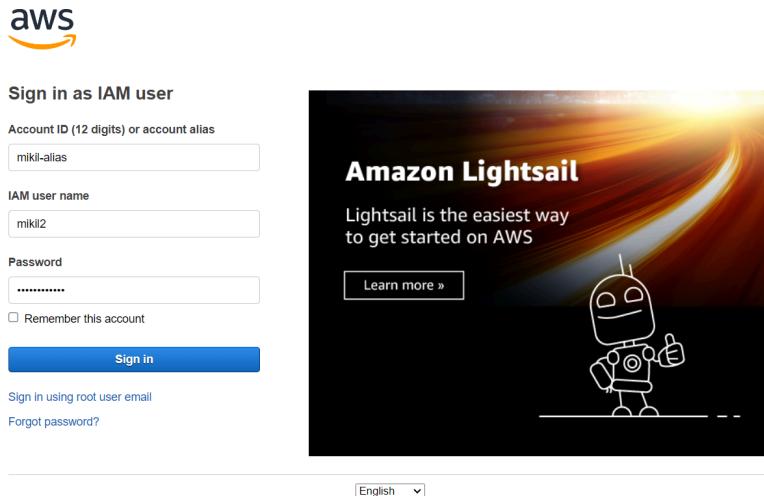
User name	Groups	Attached policies
mikil1	-	IAMUserChangePassword

Type in `ec2fullaccess` in the search box and click the check box for it; click on Next

The screenshot shows the 'Set permissions' step again. The 'Attach policies directly' option is selected. In the 'Permissions policies' section, the search bar contains 'ec2full'. A table lists one policy: 'AmazonEC2FullAccess' (AWS managed). This policy is checked.

Policy name	Type	Attached entities
AmazonEC2FullAccess	AWS managed	0

Logging in as one of the 2 new Users and Checking their permissions



The image shows the AWS sign-in interface and a promotional banner for Amazon Lightsail.

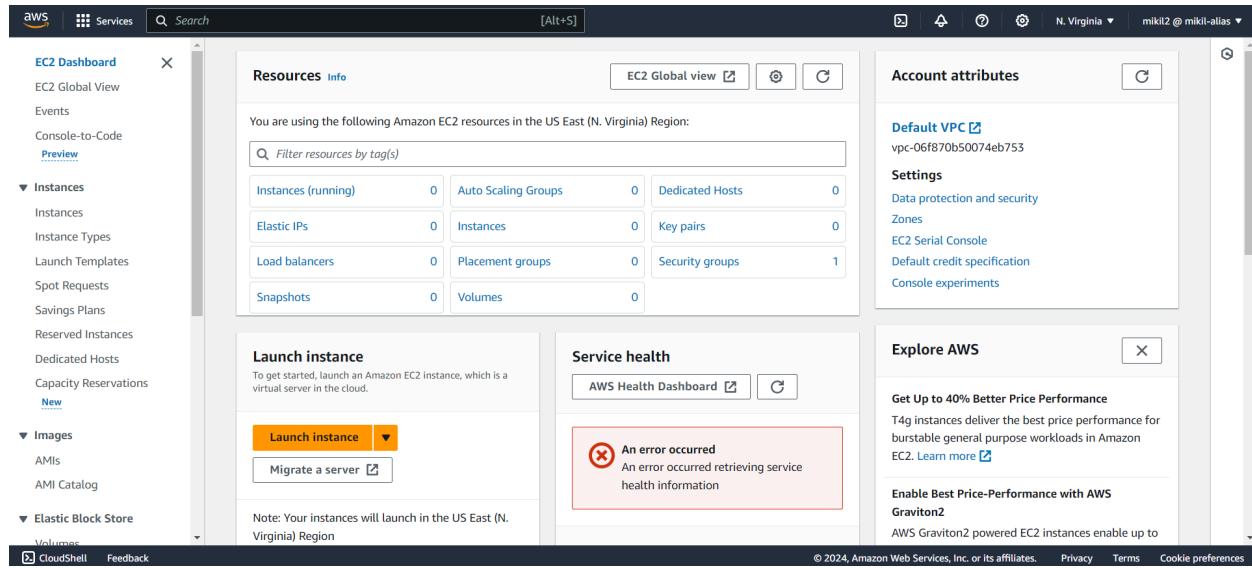
AWS Sign-in:

- Form fields: Account ID (12 digits) or account alias (miki-alias), IAM user name (miki2), Password (*****).
- Checkboxes: Remember this account (unchecked).
- Buttons: Sign in (blue), Sign in using root user email, Forgot password?.

Amazon Lightsail Banner:

- Text: "Amazon Lightsail", "Lightsail is the easiest way to get started on AWS".
- Image: A cartoon robot holding a thumbs-up.
- Link: Learn more »

Try launching an EC2 instance via the new user



The image shows the EC2 Dashboard in the AWS Management Console.

Left sidebar (EC2 Dashboard):

- EC2 Global View
- Events
- Console-to-Code (Preview)
- Instances** (selected)
 - Instances
 - Instance Types
 - Launch Templates
 - Launch Requests
 - Spot Requests
 - Savings Plans
 - Reserved Instances
 - Dedicated Hosts
 - Capacity Reservations
 - New
- Images
- Elastic Block Store
- CloudShell Feedback

Center Content:

- Resources Info:** You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	0
Load balancers	0	Placement groups	0	Security groups	1
Snapshots	0	Volumes	0		
- Launch instance:** To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
 - Launch instance (button)
 - Migrate a server (button)
- Service health:** AWS Health Dashboard
 - An error occurred: An error occurred retrieving service health information.

Right Sidebar:

- Account attributes:**
 - Default VPC (vpc-06f870b50074eb753)
 - Settings
 - Data protection and security
 - Zones
 - EC2 Serial Console
 - Default credit specification
 - Console experiments
- Explore AWS:**
 - Get Up to 40% Better Price Performance
 - T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. [Learn more](#)
 - Enable Best Price-Performance with AWS Graviton2
 - AWS Graviton2 powered EC2 instances enable up to

AWS Services Search [Alt+S] N. Virginia mikil2@mikil-alias

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible

Description

Amazon Linux 2023 AMI 2023.3.20240312.0 x86_64 HVM kernel-6.1

Architecture Boot mode AMI ID

64-bit (x86) uefi-preferred ami-0d7a109bf30624c99 Verified provider

Summary

Number of instances 1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t1.micro in the Regions in which

Cancel Launch instance Review commands

CloudShell Feedback

Instance type Info | Get advice

Instance type

t2.micro Free tier eligible

All generations Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Select Create new key pair

Network settings Info Edit

Summary

Number of instances 1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t1.micro in the Regions in which

Cancel Launch instance Review commands

The screenshot shows the AWS EC2 'Launch an instance' success page. At the top, there's a green success banner stating 'Successfully initiated launch of instance (i-0b12231215c2291bb)'. Below it, a 'Next Steps' section lists several options: 'Create billing and free tier usage alerts', 'Connect to your instance', 'Connect an RDS database', and 'Create EBS snapshot policy'. Each option has a corresponding button or link. The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, and a footer with copyright information.

Hence, an instance has been created

The screenshot shows the AWS EC2 Instances page. On the left, a sidebar lists various EC2 services: EC2 Dashboard, EC2 Global View, Events, Console-to-Code (Preview), Instances (selected), Instances Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations (New), Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes). The main pane displays a table titled 'Instances (1) Info' with one row: 'test' (Instance ID: i-0b12231215c2291bb, Instance state: Running, Instance type: t2.micro, Status check: -, Alarm status: -, Availability Zone: us-east-1a, Public IPv4 DNS: ec2-52-91-192-1). Below the table is a 'Select an instance' dropdown menu.

Delete the bucket when done with your work

Creating a new Group and Giving it permissions

Select the members to be present in the group (max 4 per group)

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar is titled "Identity and Access Management (IAM)" and includes sections for "User groups", "Users", "Roles", "Policies", "Identity providers", and "Account settings". The main content area is titled "User groups (0) Info" and contains a message: "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." Below this is a search bar and a table header with columns: "Group name", "Users", "Permissions", and "Creation time". A message at the bottom of the table says "No resources to display".

Giving this group `ec2fullaccess` and `s3fullaccess`

The screenshot shows the "Create user group" wizard. The first step, "Name the group", has a "User group name" input field containing "testgrp". The second step, "Add users to the group - Optional (2/3)", lists three users: "mikil1" (unchecked), "mikil2" (checked), and "mikil3" (checked). The third step, "Attach permissions policies - Optional (924)", is partially visible. The bottom of the screen shows the AWS navigation bar.

Add users to the group - Optional (2/5) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time
mikit1	0	8 minutes ago	37 minutes ago
<input checked="" type="checkbox"/> mikil2	0	5 minutes ago	5 minutes ago
<input checked="" type="checkbox"/> mikil3	0	None	Now

Attach permissions policies - Optional (2/924) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type

Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>  AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets via t...

Cancel

Create group

Add users to the group - Optional (2/5) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time
mikit1	0	8 minutes ago	37 minutes ago
<input checked="" type="checkbox"/> mikil2	0	5 minutes ago	5 minutes ago
<input checked="" type="checkbox"/> mikil3	0	None	Now

Attach permissions policies - Optional (2/924) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type

Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>  AmazonEC2FullAccess	AWS managed	None	Provides full access to Amazon EC2 via...

Cancel

Create group

The screenshot shows the AWS IAM User Groups page. A green banner at the top indicates that 'testgrp user group created.' Below this, the 'User groups (1) Info' section is displayed. A table lists one user group:

Group name	Users	Permissions	Creation time
testgrp	2	Loading	Now

The screenshot shows the 'testgrp' User Group details page. The 'Summary' section displays the group's name, creation time, and ARN. The 'Users (2)' tab is selected, showing two users assigned to the group: 'miki2' and 'miki3'. The table below lists these users with their respective activity details.

User name	Groups	Last activity	Creation time
miki2	1	5 minutes ago	6 minutes ago
miki3	1	None	1 minute ago

Logging in as a member of the Group & Checking their permissions

Now, login as one of the users from the group and try creating a S3 bucket

Sign in as IAM user

Account ID (12 digits) or account alias
mikil-alias

IAM user name
mikil3

Password
.....

Remember this account

Sign in

Sign in using root user email
Forgot password?



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

Success! Successfully created bucket "test-bucket37". To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Amazon S3 > Buckets

▼ Account snapshot

Last updated: Mar 15, 2024 by Storage Lens. Metrics are generated every 24 hours. Metrics don't include directory buckets. [Learn more](#)

Total storage	Object count	Average object size	You can enable advanced metrics in the "default-account-dashboard" configuration.
56.0 B	1	56.0 B	

[View Storage Lens dashboard](#)

[General purpose buckets](#) [Directory buckets](#)

General purpose buckets (2) [Info](#)

Buckets are containers for data stored in S3.

Name	AWS Region	Access	Creation date
elasticbeanstalk-us-east-1-689179663899	US East (N. Virginia) us-east-1	Objects can be public	October 31, 2022, 19:38:53 (UTC+05:30)
test-bucket37	US East (N. Virginia) us-east-1	Bucket and objects not public	March 16, 2024, 15:46:50 (UTC+05:30)

[Create bucket](#)

[CloudShell](#) [Feedback](#)

Delete the bucket when done with your work

Creating a new Role

Go in the root user window and click on “create role” button in the “Roles” section of IAM Dashboard

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a navigation sidebar with options like Dashboard, Access management (Roles, Policies, Identity providers, Account settings), and Access reports (Access Analyzer, External access, Unused access, Analyzer settings). The main content area is titled "Roles (16) Info" and contains a table with 16 rows, each representing a role. The columns are Role name, Trusted entities, and Last activity. Some roles listed include "analytics_role", "aws-elasticbeanstalk-service-role", and various AWS CodePipeline and ServiceRole entries.

Let it be the default options (you can choose any use case you like)

Click in Next button

This screenshot shows the second step of creating a new IAM role. It's titled "Step 2: Add permissions". The first section, "Trusted entity type", has five options: "AWS service" (selected), "AWS account", "Web identity", "SAML 2.0 federation", and "Custom trust policy". Below this, the "Use case" section says "Allow an AWS service like EC2, Lambda, or others to perform actions in this account." A dropdown menu for "Service or use case" shows "EC2" selected. Under "Choose a use case for the specified service.", "EC2" is also selected. At the bottom, there are links for "CloudShell" and "Feedback".

Give the permission suitable to the use case chosen

The screenshot shows the 'Add permissions' step of the IAM role creation wizard. The 'Permissions policies' section lists the 'AmazonEC2FullAccess' policy, which provides full access to Amazon EC2. The 'Description' for this policy is partially visible as 'Provides full access to Amazon EC2 via th...'. The 'Next Step' button is highlighted in orange at the bottom right.

Give a suitable Role name and description; rest would remain as default. click on Create Role button

The screenshot shows the 'Name, review, and create' step of the IAM role creation wizard. In the 'Role details' section, the 'Role name' is set to 'ec2accessRole' and the 'Description' is 'Allows EC2 instances to call AWS services on your behalf.'. The 'Step 1: Select trusted entities' section is collapsed. The 'Next Step' button is highlighted in orange at the bottom right.

The role has been successfully created

The screenshot shows the AWS IAM Roles page. At the top, a green banner says "Role ec2AccessRole created." Below it, the "Roles (17) Info" section defines a Role as an identity with specific permissions. A search bar is at the top of the list table. The table has columns for "Role name" (sorted by last activity), "Trusted entities" (AWS Service: sagemaker), and "Last activity" (155 days ago). One row is selected: "sagemaker_role". To the right of the table are three cards: "Access AWS from your non AWS workloads" (using X.509 Standard), "X.509 Standard" (using your own PKI or AWS Certificate Manager Private Certificate Authority), and "Temporary credentials" (using temporary credentials for enhanced security). The left sidebar shows navigation options like Dashboard, Access management (selected), Roles, Policies, Identity providers, and Account settings.

Just to check the overall users, groups and roles, you can check out the IAM Dashboard

The screenshot shows the AWS IAM Dashboard. The main header says "Role ec2AccessRole created." Below it, the "IAM Dashboard" section includes "Security recommendations" (with one item: "Add MFA for root user"), "IAM resources" (with counts: User groups 1, Users 3, Roles 17, Policies 12, Identity providers 0), and "AWS Account" details (Account ID: 689179663899, Account Alias: mikil-alias, Sign-in URL: https://mikil-alias.sigin.aws.amazon.com/console). On the left, the same navigation sidebar as the previous screen is visible.

Deleting a User

Screenshot of the AWS IAM console showing the 'Users' page. The user 'mikil3' is selected for deletion.

Users (1/3) Info

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

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
mikil1	/	0	13 minutes ago	Virtual	40 minutes	March 16, 2024, 15:31
mikil2	/	1	9 minutes ago	-	-	March 16, 2024, 15:31
mikil3	/	1	-	-	-	-

Delete mikil3?

Delete mikil3 permanently? This will also delete all its user data, security credentials and inline policies.

User name	Last activity
mikil3	-

Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. [Learn more](#)

This action cannot be undone.

To confirm deletion, enter the user name in the text input field.

Delete user

User "mikil3" deleted.

Users (2) Info

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

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
mikil1	/	0	13 minutes ago	Virtual	40 minutes	March 16, 2024, 15:31
mikil2	/	1	9 minutes ago	-	-	March 16, 2024, 15:31

Deleting a Role

The screenshot shows the AWS IAM Roles page. A green banner at the top says "User 'mikil3' deleted." Below it, the "Roles (1/17) Info" section shows a search bar with "ec" and a result for "ec2accessRole". The role details show it was created for the "ec" service. Below this is the "Roles Anywhere" section with three options: "Access AWS from your non AWS workloads", "X.509 Standard", and "Temporary credentials".

A modal dialog titled "Delete ec2accessRole?" asks if the user wants to delete the role permanently. It shows the role name "ec2accessRole" and its last activity. A note says recent activity appears within 4 hours. The user is prompted to enter the role name again to confirm. The "Delete" button is highlighted.

The screenshot shows the AWS IAM Roles page again. A green banner at the top says "Role deleted ec2accessRole." The "Roles (16) Info" section shows a search bar with "ec" and a results table with no matches. The "Clear filters" button is visible. The "Roles Anywhere" section is also present.

Deleting a Group

The screenshot shows the AWS IAM User groups page. A single user group named 'testgrp' is listed. Below the main table, a modal window titled 'Delete testgrp?' is displayed, asking for confirmation to delete the group. The modal includes a text input field containing 'testgrp' and two buttons: 'Cancel' and 'Delete'.

Check the IAM dashboard to see the results after deletion activities

The screenshot shows the AWS IAM Dashboard. On the left, the navigation menu includes 'User groups' under 'Access management'. In the center, there's a 'Security recommendations' section with one item: 'Add MFA for root user'. Below it is an 'IAM resources' section showing 0 User groups, 2 Users, 16 Roles, 12 Policies, and 0 Identity providers. To the right, there are sections for 'AWS Account' (Account ID: 689179663899, Account Alias: mikil-alias), 'Quick Links' (My security credentials), and 'Tools'.

Check the ec2 dashboard in case there are any running instances

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with navigation links like Cloud9, EC2, Elastic Beanstalk, AWS Amplify, Lambda, S3, and API Gateway. The main content area has tabs for 'Resources' and 'Info'. Under 'Resources', it says 'You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:' with a table showing 0 instances (running), 0 Auto Scaling Groups, 0 Dedicated Hosts, 0 Elastic IPs, 1 Instances, 0 Key pairs, 0 Load balancers, 0 Placement groups, 2 Security groups, 0 Snapshots, and 0 Volumes. Below this is a 'Launch instance' section with a large orange 'Launch instance' button and a 'Migrate a server' link. To the right is a 'Service health' section showing 'Region: US East (N. Virginia)' and 'Status: This service is operating normally.' At the bottom, a note says 'Note: Your instances will launch in the US East (N. Virginia) Region.' On the far right, there are sections for 'Account attributes' (Default VPC set to 'vpc-06f870b50074eb753'), 'Settings' (Data protection and security, Zones, EC2 Serial Console, Default credit specification, Console experiments), and 'Explore AWS' (Enable Best Price-Performance with AWS Graviton2, 10 Things You Can Do Today to Reduce AWS Costs). The top right corner shows the user 'Mikil Lalwani'.

Conclusion -

Thus we have successfully studied and implemented Identity and Access Management (IAM) practices on AWS.