

EXPERIMENT NO 8

AIM: To study and Implement Security as a Service on AWS/Azure

STEP 1: Open the AWS home page, Search the IAM, Open the IAM dashboard,

The screenshot shows the AWS IAM dashboard. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Account settings. The main content area displays the 'IAM dashboard' with a 'Security recommendations' section showing 'Add MFA for root user' and 'Root user has no active access keys'. Below this is the 'IAM resources' section with a table showing counts for User groups (0), Users (0), Roles (7), Policies (0), and Identity providers (0). The 'What's new' section lists recent updates. The right sidebar shows the 'AWS Account' information and 'Quick Links'.

Resource	Count
User groups	0
Users	0
Roles	7
Policies	0
Identity providers	0

STEP 2: Create one user group: MITM_TE

The screenshot shows the 'Create user group' page in the AWS IAM console. The 'Name the group' section has a text input field with 'MITM_TE' entered. Below this is the 'Add users to the group - Optional' section, which is currently empty. At the bottom, there is a section for 'Attach permissions policies - Optional' with a 'Create Policy' button.

STEP 3: MITM TE group created. NO user is present in this group.

Identity and Access Management (IAM)

MITM_TE user group created. View group

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity

MITM_TE user group created.

IAM > User groups

User groups (2) Info

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

Filter User groups by property or group name and press enter

	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	MITM-COMPUTER	3	Not defined	12 minutes ago
<input type="checkbox"/>	MITM_TE	0	Not defined	Now

https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Step 4: Add USER in MITM_TE group

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* mitm_user

Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type*

- ☒ Access key - Programmatic access
- ☐ Password - AWS Management Console access

Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

Enables a password that allows users to sign-in to the AWS Management Console.

* Required

Cancel Next: Permissions

Add user

1 2 3 4 5

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

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

Add user to group

Create group Refresh

Search

Showing 2 results

Group	Attached policies
<input checked="" type="checkbox"/> MITM_TE	None
<input type="checkbox"/> MITM-COMPUTER	None

Set permissions boundary

Cancel Previous Next: Tags

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

twishal17

Add user

12345

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name

mitm_user

AWS access type

Programmatic access - with an access key

Permissions boundary

Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	MITM_TE

Tags

No tags were added.

Cancel

Previous

Create user

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

twishal17

Add user

12345

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://721254631510.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
	mitm_user	AKIA2P3RAJBLMABRB6UT	***** Show

Close

Feedback

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

twishal17

Identity and Access Management (IAM)

Introducing the new Users list experience

We've redesigned the Users list experience to make it easier to use. [Let us know what you think.](#)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysts

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > Users

Users (4) Info

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

Find users by username or access key

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	Amit	MITM-COMPUTER	Never	None	None	20 minutes ago
<input type="checkbox"/>	Hemant	MITM-COMPUTER	Never	None	None	20 minutes ago
<input type="checkbox"/>	mitm_user	MITM_TE	Never	None	None	1 minute ago
<input type="checkbox"/>	Vishal	MITM-COMPUTER	Never	None	None	20 minutes ago

Refresh

Delete

Add users

Feedback

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

STEP 5: Set the permission boundary to the USER , select any policy for USER

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with 'Identity and Access Management (IAM)' selected. The main content area is titled 'Permissions' for the user 'mitm_user'. It displays the user's ARN, path, and creation time. Below this, there are tabs for 'Permissions policies', 'Groups (1)', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions policies' tab is active, showing a 'Get started with permissions' section with an 'Add permissions' button. Below that, the 'Permissions boundary (not set)' section is visible, with a 'Set boundary' button. At the bottom, there is a 'Generate policy based on CloudTrail events' section with a 'Generate policy' button.

Set the permissions boundary on mitm_user

Setting the permissions boundary is an advanced feature
The permissions boundary can restrict the permissions currently allowed for this user. [Learn more](#)

Select a policy to set as the permissions boundary

Filter policies Search Showing 944 results

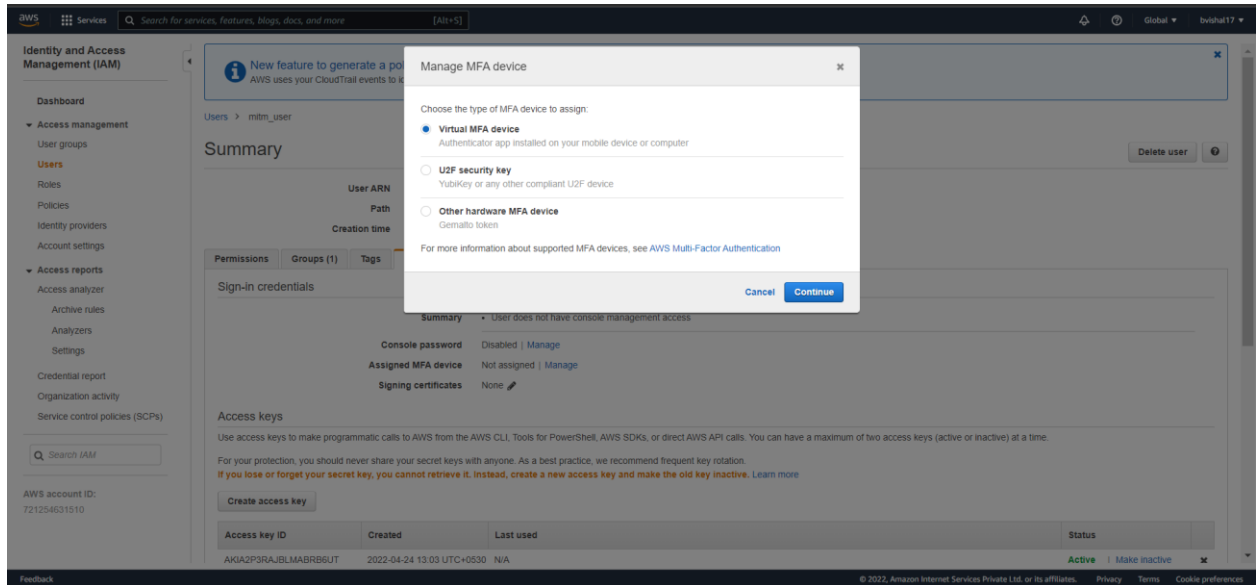
Policy name	Type	Used as
AccessAnalyzerServiceRolePolicy	AWS managed	None
AdministratorAccess	Job function	Boundary (1)
AdministratorAccess-Amplify	AWS managed	None
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
AlexaForBusinessDeviceSetup	AWS managed	None
AlexaForBusinessFullAccess	AWS managed	None
AlexaForBusinessGatewayExecution	AWS managed	None
AlexaForBusinessLifeSizeDelegatedAccessPolicy	AWS managed	None
AlexaForBusinessNetworkProfileServicePolicy	AWS managed	None
AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
AlexaForBusinessReadOnlyAccess	AWS managed	None

Cancel Set boundary

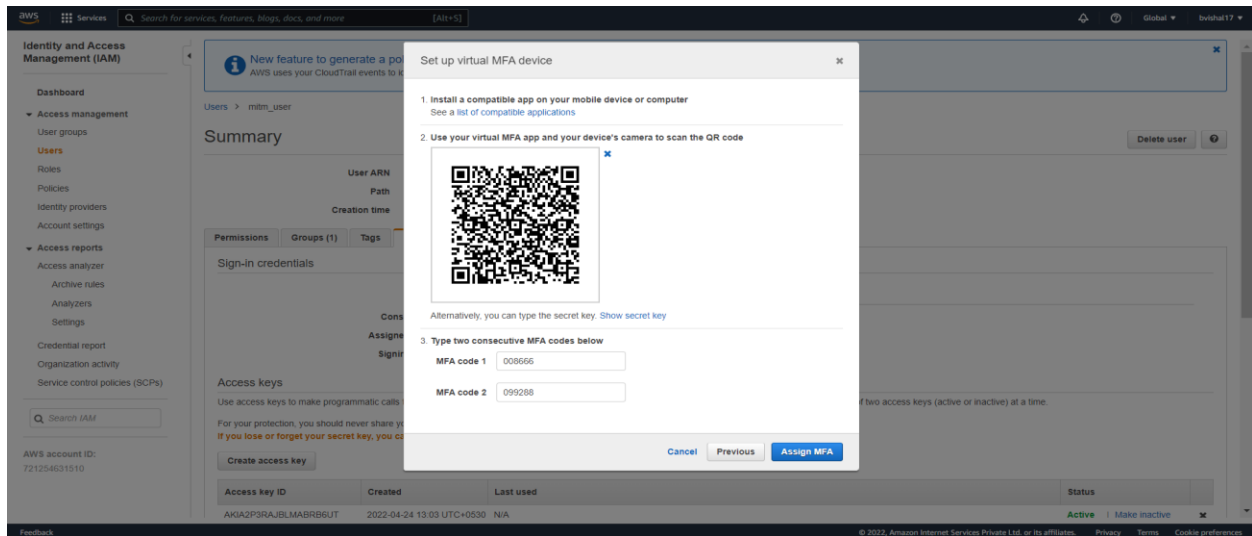
The screenshot shows the AWS IAM console interface for the user 'mitm_user'. The 'Security credentials' tab is active, displaying a 'Summary' section with a 'Delete user' button. Below the summary, there are sections for 'Sign-in credentials' and 'Access keys'. The 'Sign-in credentials' section shows that the user does not have console management access, and the 'Access keys' section shows that the user has no access keys. At the bottom, there is a table with columns for 'Access key ID', 'Created', 'Last used', and 'Status'.

Access key ID	Created	Last used	Status
AKIA2P3RAJBLMABR6UT	2022-04-24 13:03 UTC+0530	N/A	Active

STEP 6: Assigned MFA Device, click on Manage and select the Virtual MFA Device



STEP 7: Download the Google Authenticator application on your mobile device , scan the Qr code & submit the Mfa code1 & MFA code 2.



Set up virtual MFA device

You have successfully assigned virtual MFA. This virtual MFA will be required during sign-in.

Close

New feature to generate a policy based on CloudTrail events.
AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.

Users > mfm_user

Summary

User ARN: arn:aws:iam::721254631510:user:mfm_user

Path: /

Creation time: 2022-04-24 13:03 UTC+0530

Permissions Groups (1) Tags **Security credentials** Access Advisor

Sign-in credentials

Summary

- User does not have console management access
- MFA is required when signing in. [Learn more](#)

Console password Disabled | [Manage](#)

Assigned MFA device am.aws.iam:721254631510:mfa/mfm_user (Virtual) | [Manage](#)

Signing certificates None

Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, 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.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)

[Create access key](#)

Access key ID	Created	Last used	Status
---------------	---------	-----------	--------

Feedback

© 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Q Search IAM

AWS account ID: 721254631510

New feature to generate a policy based on CloudTrail events.
AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.

Users > mfm_user

Summary

Delete user **?**

User ARN: arn:aws:iam::721254631510:user:mfm_user

Path: /

Creation time: 2022-04-24 13:03 UTC+0530

Permissions Groups (1) Tags **Security credentials** Access Advisor

Sign-in credentials

Summary

- User does not have console management access
- MFA is required when signing in. [Learn more](#)

Console password Disabled | [Manage](#)

Assigned MFA device am.aws.iam:721254631510:mfa/mfm_user (Virtual) | [Manage](#)

Signing certificates None

Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, 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.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)

[Create access key](#)

Access key ID	Created	Last used	Status
---------------	---------	-----------	--------

Feedback

© 2022, Amazon Internet Services Private Ltd. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)