

### Experiment No:6

**Aim:** Study and implement Identity and Access Management (IAM)

#### Theory

##### 1. Study Identity and Access Management

Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. With an IAM framework in place, information technology (IT) managers can control user access to critical information within their organizations. Systems used for IAM include single sign-on systems, two-factor authentication, multifactor authentication and privileged access management. These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared.

IAM systems can be deployed on premises, provided by a third-party vendor through a cloud-based subscription model or deployed in a hybrid model. On a fundamental level, IAM encompasses the following components:

- how individuals are identified in a system (understand the difference between identity management and authentication); how roles are identified in a system and how they are assigned to individuals;
- adding, removing and updating individuals and their roles in a system;
- assigning levels of access to individuals or groups of individuals; and
- protecting the sensitive data within the system and securing the system itself.

##### 2. Explain need for Access Management Services in cloud computing

Businesses leaders and IT departments are under increased regulatory and organizational pressure to protect access to corporate resources. As a result, they can no longer rely on manual and error-prone processes to assign and track user privileges. IAM automates these tasks and enables granular access control and auditing of all corporate assets on premises and in the cloud. IAM, which has an ever-increasing list of features -- including biometrics, behavior analytics and AI -- is well suited to the rigors of the new security landscape. For example, IAM's tight control of resource access in highly distributed and dynamic environments aligns with the industry's transition from firewalls to zero-trust models and with the security requirements of IoT. For more information on the future of IoT security, check out this video. While IT professionals might think IAM is for larger organizations with bigger budgets, in reality, the technology is accessible for companies of all sizes.

##### 3. Explain Functional architecture and Component of IAM

There are other basic components of IAM. First, we have the user; many users together form a group. Policies are the engines that allow or deny a connection based on policy. Roles are temporary credentials that can be assumed to an instance as needed. Users

An IAM user is an identity with an associated credential and permissions attached to it. This could be an actual person who is a user, or it could be an application that is a user. With IAM, you can securely manage access to AWS services by creating an IAM user name for each employee in your organization. Each IAM user is associated with only one AWS account. By default, a newly created user is not authorized to perform any action in AWS. The advantage of having one-to-one user specification is that you can individually assign permissions to each user. Groups A collection of IAM users is an IAM group. You can use IAM groups to specify permissions for multiple users so that any permissions applied to the group are applied to the individual users in that group as well. Managing groups is quite easy. You set permissions for the group, and those permissions are automatically applied to all the users in the group. If you add another user to the group, the new user will automatically inherit all the policies and the permissions already assigned to that group. This lessens the administrative burden. Policies

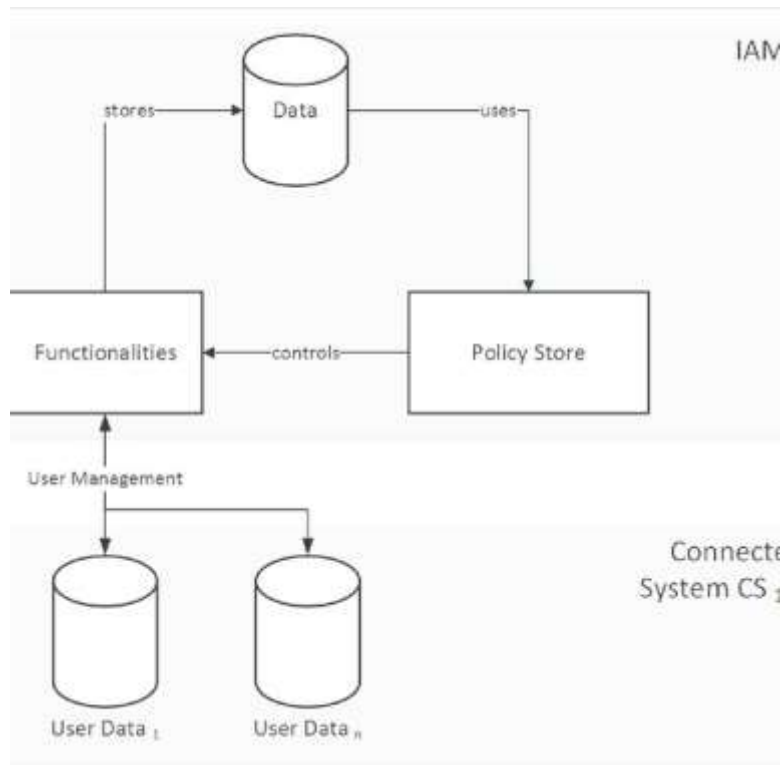
An IAM policy sets permission and controls access to AWS resources. Policies are stored in AWS as JSON documents. Permissions specify who has access to the resources and what actions they can perform. For example, a policy could allow an IAM user to access one of the buckets in [Amazon S3](#). The policy would contain the following information:

Who can access it

What actions that user can take

Which AWS resources that user can access

When they can be accessed



## Implementation:

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

Services Search for services, features, blogs, docs, and more [Alt+S] Global

### Identity and Access Management (IAM)

Search IAM

Dashboard

- Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
  - Archive rules
  - Analysers
  - Settings
  - Credential report
  - Organization activity
  - Service control policies (SCPs)

### IAM dashboard

Security recommendations 1

**Add MFA for root user**

Sign in as the root user (or contact your administrator) and register a multi-factor authentication (MFA) device for the root user to improve security for this account.

### IAM resources

User groups	Users	Roles	Policies	Identity providers
3	4	14	2	0

### What's new

Updated for features in IAM

- Right-size permissions for more roles in your account using IAM Access Analyzer to generate 50 fine-grained IAM policies per day. 2 months ago
- Amazon S3 Object Ownership can now disable access-control lists to simplify access management for data in S3. 3 months ago
- Amazon Redshift simplifies the use of other AWS services by introducing the default IAM role. 4 months ago
- IAM Access Analyzer helps you generate fine-grained policies that specify the required actions for more than 50 services. 7 months ago

more

Feedback English (US)

© 2022, Amazon Web Services

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

[Alt+Q]

Global

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access analyzer
- Archive rules
- Analysts
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

IAM > User groups

User groups (3) [Help](#)

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

Filter User groups by property or group name and press enter

Group name	Users	Permissions
<a href="#">EC2 Admin</a>	<a href="#">f Loading</a>	<a href="#">f Loading</a>
<a href="#">EC2-Support</a>	<a href="#">f Loading</a>	<a href="#">f Loading</a>
<a href="#">S3-Support</a>	<a href="#">f Loading</a>	<a href="#">f Loading</a>

Feedback

English (US)

© 2022, Amazon Web Services, Inc.

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

[Alt+Q]

Global

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access analyzer
- Archive rules
- Analysts
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

IAM > User groups > S3-Support

S3-Support

Summary

User group name	Creation time	ARN
S3-Support	March 10, 2022, 13:36 (UTC+00:30)	<a href="#">arn:aws:iam:::user-group/S3-Support</a>

Users

Permissions

Access Advisor

User groups in this group (0) [Help](#)

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

Search

User name	Groups	Last activity
-----------	--------	---------------

No resources to display

Feedback

English (US)

© 2022, Amazon Web Services, Inc.

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

[Alt+Q]

Global

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

- Access analyzer
- Archive rules
- Analysts
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

IAM > User groups > S3-Support > Add users

Add users to S3-Support

Other users in this account (4) [Help](#)

Search

User name	Groups	Last activity
<a href="#">awsuser</a>	You need permissions	None
<a href="#">user-1</a>	<a href="#">E</a>	None
<a href="#">user-2</a>	<a href="#">E</a>	None
<a href="#">user-3</a>	<a href="#">E</a>	None

Feedback

English (US)

© 2022, Amazon Web Services, Inc. or its affiliates

Search for services, features, docs, and more

[Alt+F]

Identity and Access Management (IAM)

Dashboard

Access management

User groups

**Users**

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Active rules

Analyzer

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

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 > user-1

Summary

User ARN

arn:aws:iam::754561232483:user:sp66/user-1

Path

/sp66/

Creation time

2022-03-10 13:35 UTC+0530

Permissions

Groups

Tags (1)

Security credentials

Access Advisor

Permissions policies

Get started with permissions

This user doesn't have any permissions yet. Get started by adding the user to a group, copying permissions from another user, or attaching a policy.

Add permissions

Permissions boundary (not set)

You need permissions

You do not have the permission required to perform this operation. Ask your administrator to add permissions.

Feedback

English (US)

© 2022, Amazon Web Services, Inc. or its affiliates

Search for services, features, docs, and more

[Alt+F]

Identity and Access Management (IAM)

Dashboard

Access management

User groups

**Users**

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Active rules

Analyzer

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

Users > user-1

Summary

User ARN

arn:aws:iam::754561232483:user:sp66/user-1

Path

/sp66/

Creation time

2022-03-10 13:35 UTC+0530

Permissions

**Groups (1)**

Tags (1)

Security credentials

Access Advisor

Add user to groups

Group name	Attached permissions
SS-Support	AmazonSSMReadOnlyAccess

Feedback

English (US)

© 2022, Amazon Web Services, Inc. or its affiliates

Search for services, features, docs, and more

[Alt+F]

Identity and Access Management (IAM)

Dashboard

Access management

User groups

**Users**

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Active rules

Analyzer

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

Users > user-2

Summary

User ARN

arn:aws:iam::754561232483:user:sp66/user-2

Path

/sp66/

Creation time

2022-03-10 13:36 UTC+0530

Permissions

**Groups (1)**

Tags (1)

Security credentials

Access Advisor

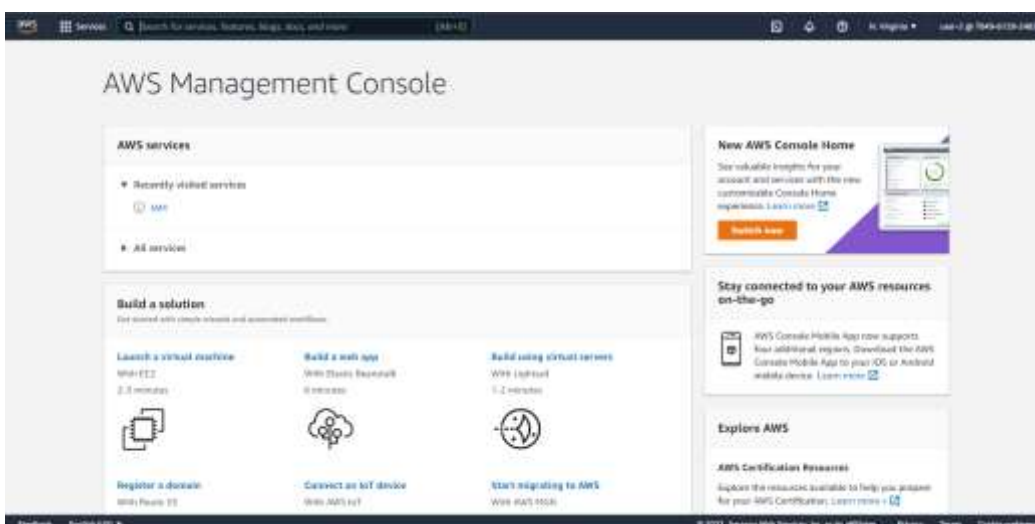
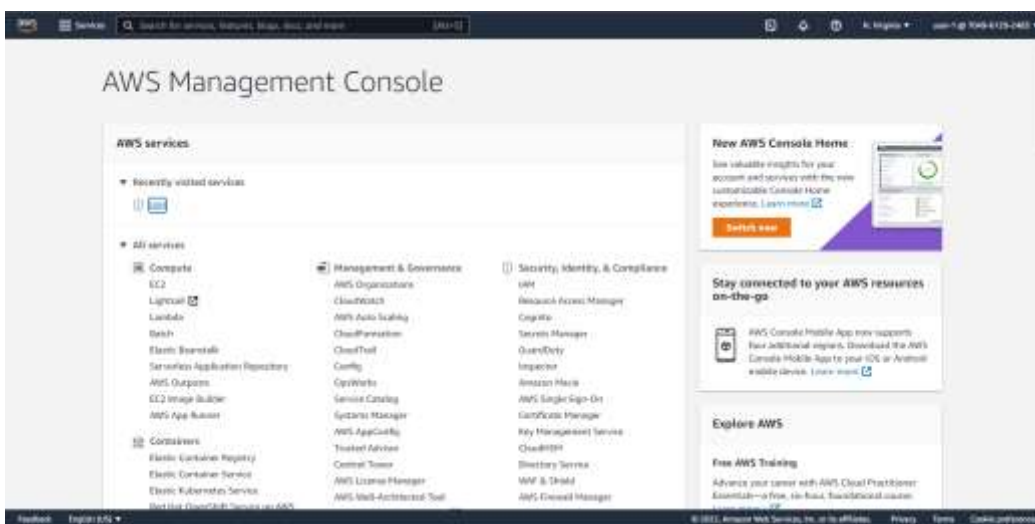
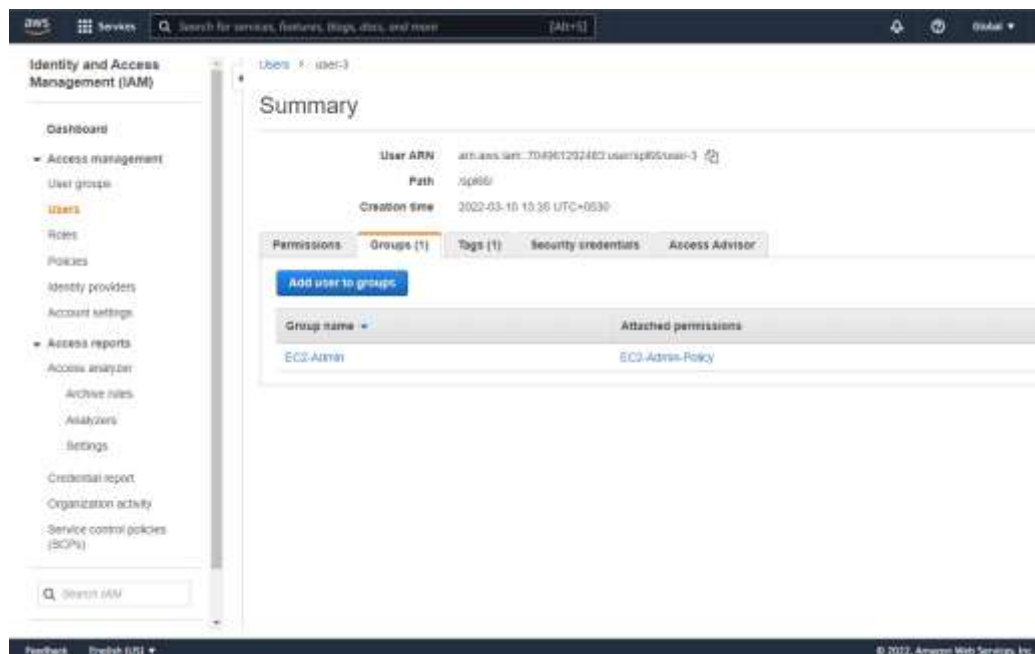
Add user to groups

Group name	Attached permissions
SS-Support	AmazonEC2ReadOnlyAccess

Feedback

English (US)

© 2022, Amazon Web Services, Inc. or its affiliates



## Conclusion:

In this experiment successfully completed Study and implement of Identity and Access Management (IAM)