Academic Year: 2021-2022 **Semester: VIII**
Subject: Cloud Computing Lab **Class / Branch / Division: BE/CMPN A**
Name: Nithin Menezes **Roll Number: 56**

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

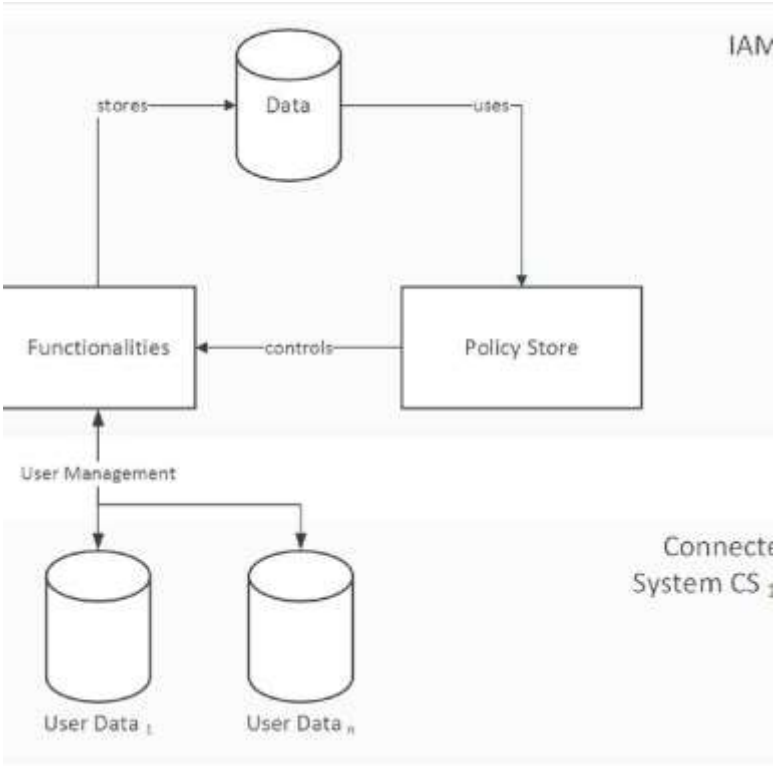
There are other basic components of IAM. First, we have the user; many users together form a group. Policies are the engines that allow or deny a connection based on policy. Roles are temporary credentials that can be assumed to an instance as needed. Users An IAM user is an identity with an associated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

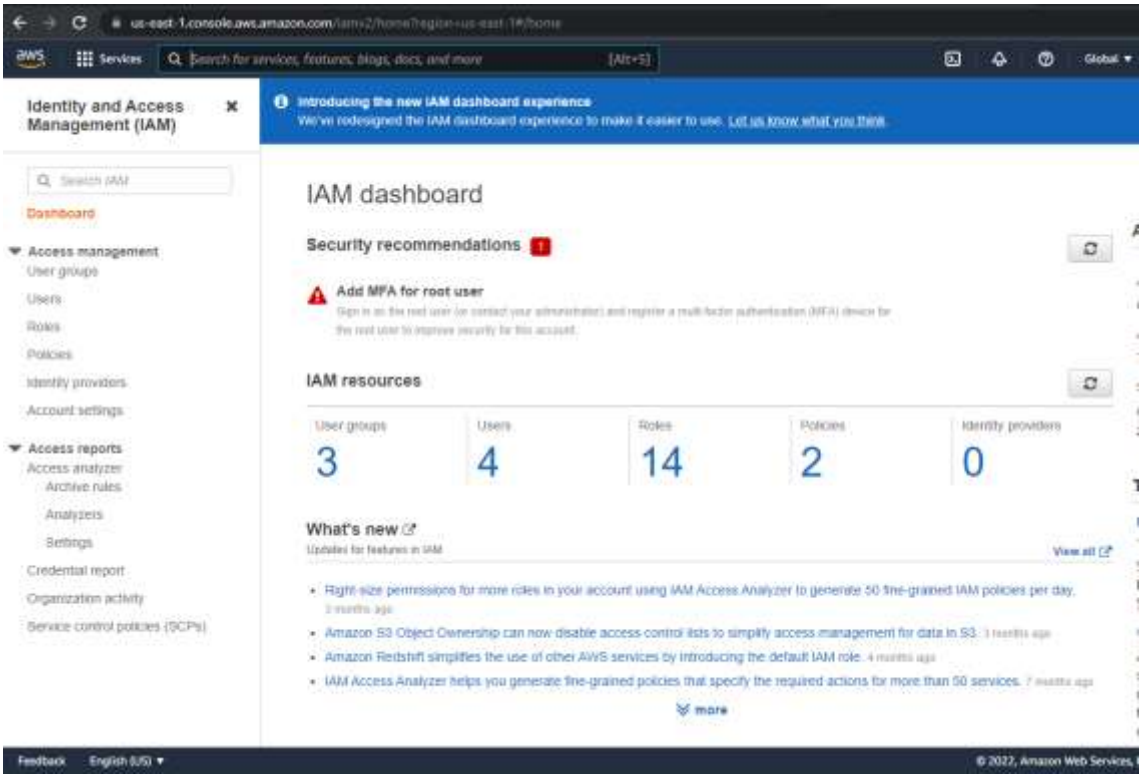
What actions that user can take

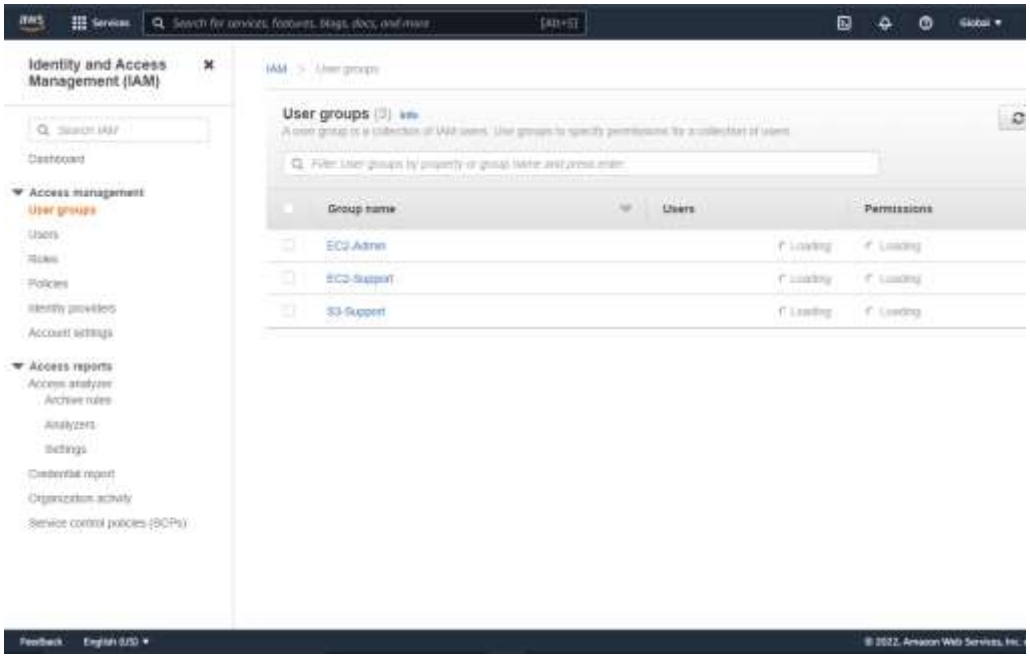
Which AWS resources that user can access

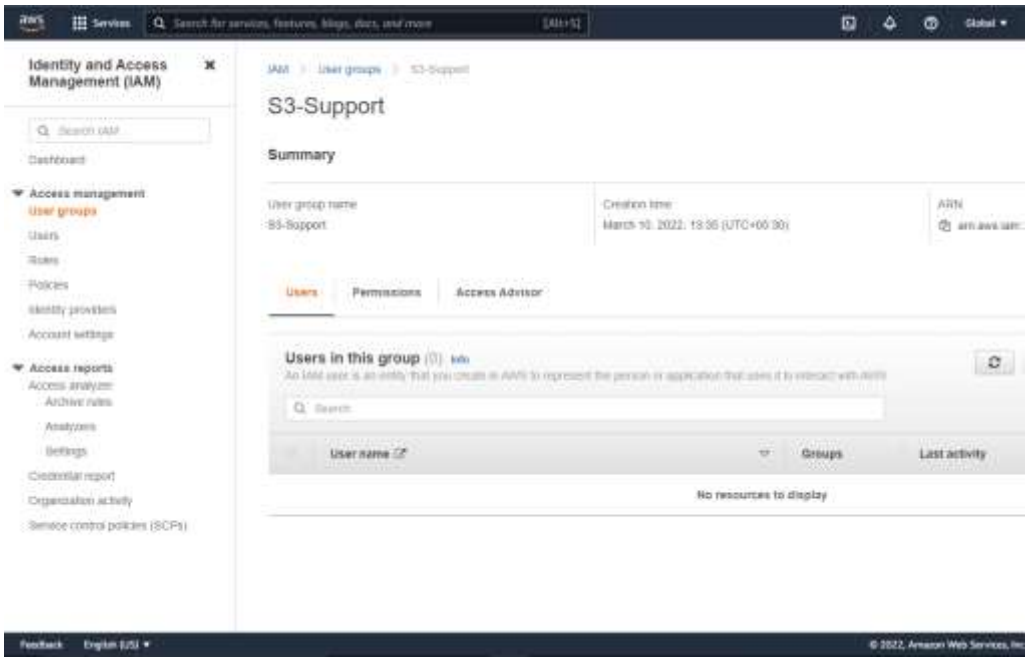
When they can be accessed

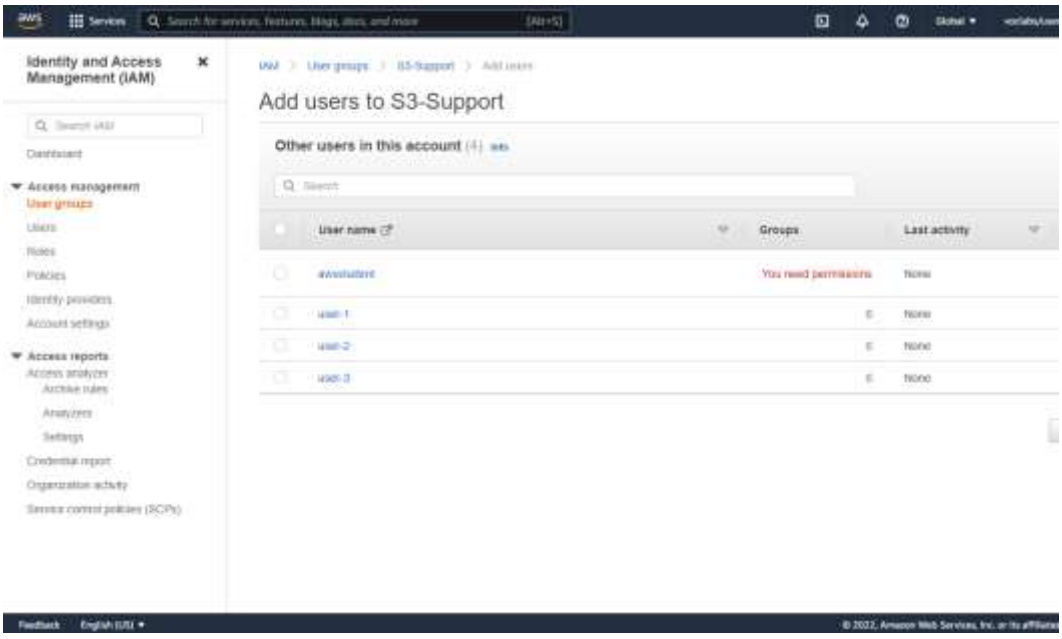


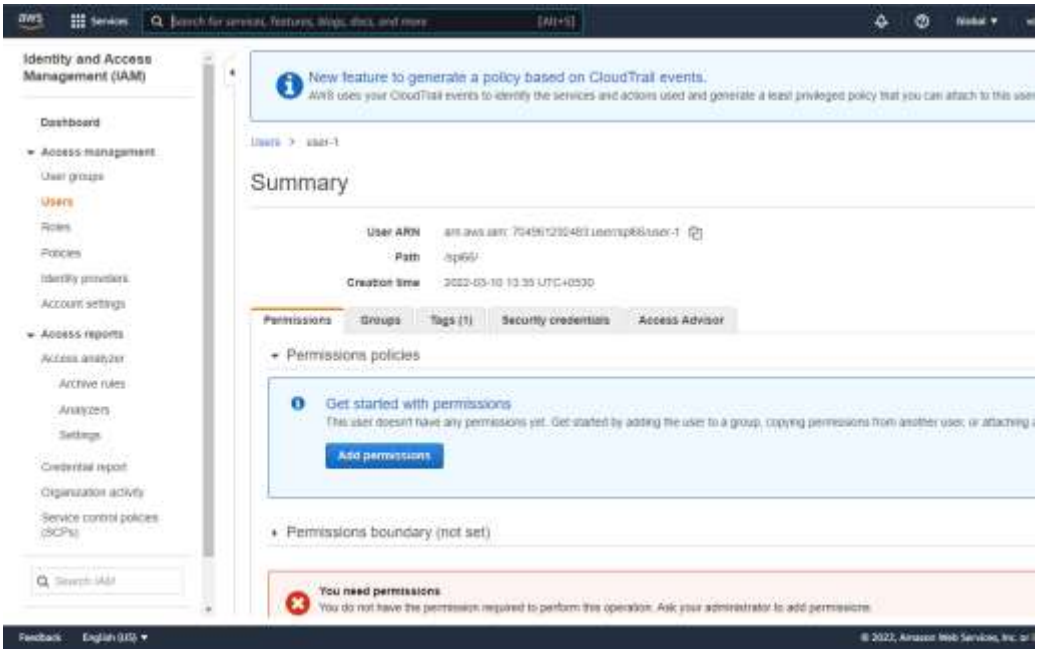
Implementation:

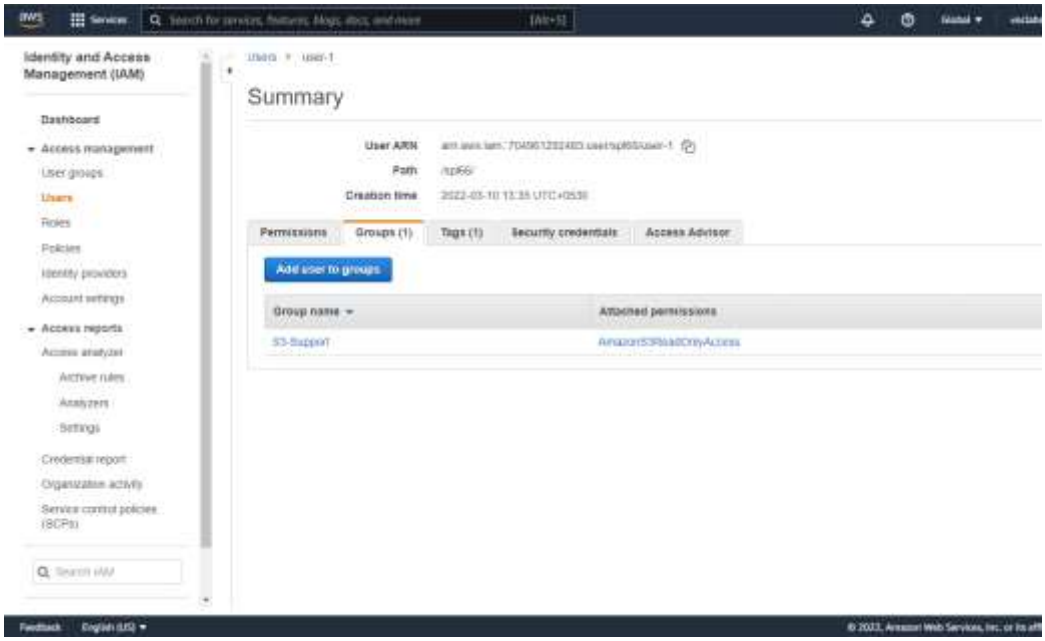


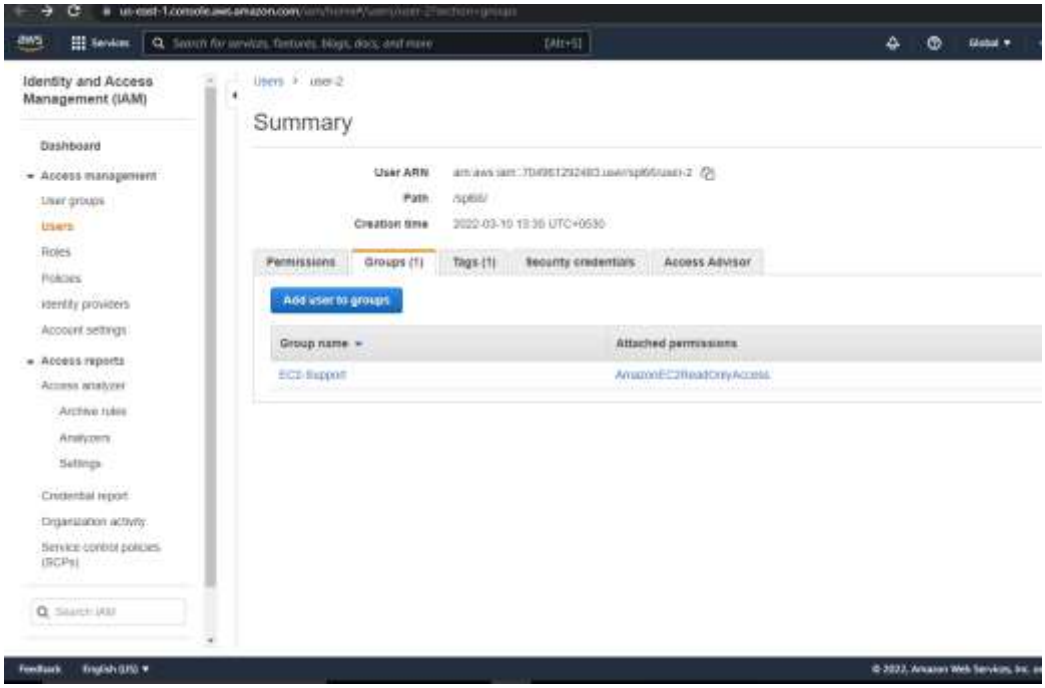

Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
User groups (3)
Group name
Users
Permissions
EC2-Admin
EC2-Support
S3-Support

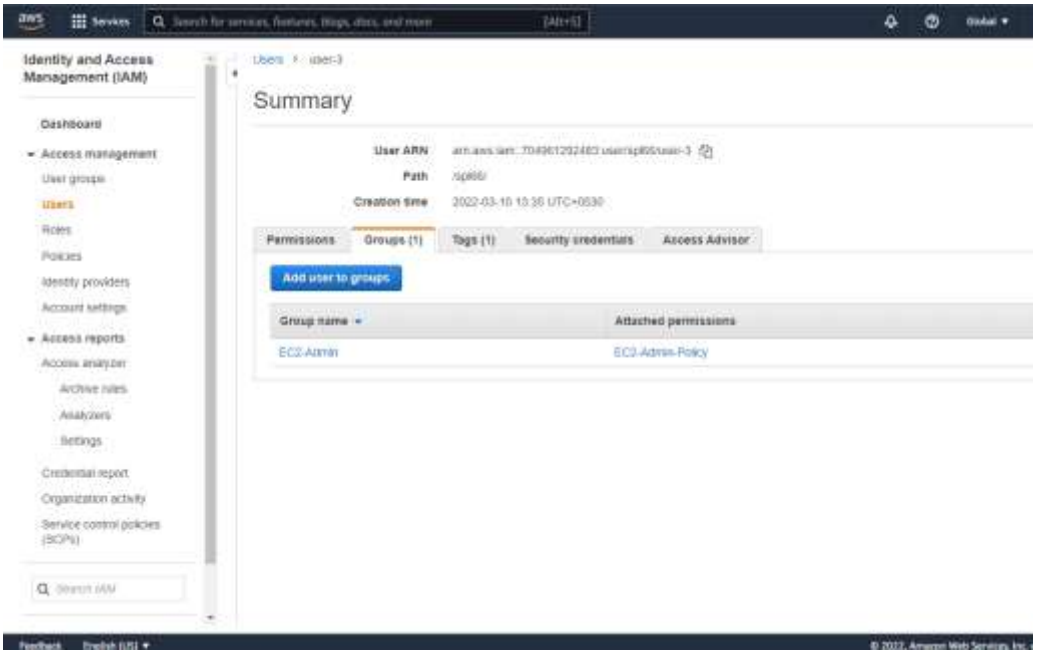

Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Credential report
Organization activity
Service control policies (SCPs)
S3-Support
Summary
User group name
S3-Support
Creation time
Permissions
Access Advisor
Users in this group (0)
User name
Groups
Last activity
No resources to display

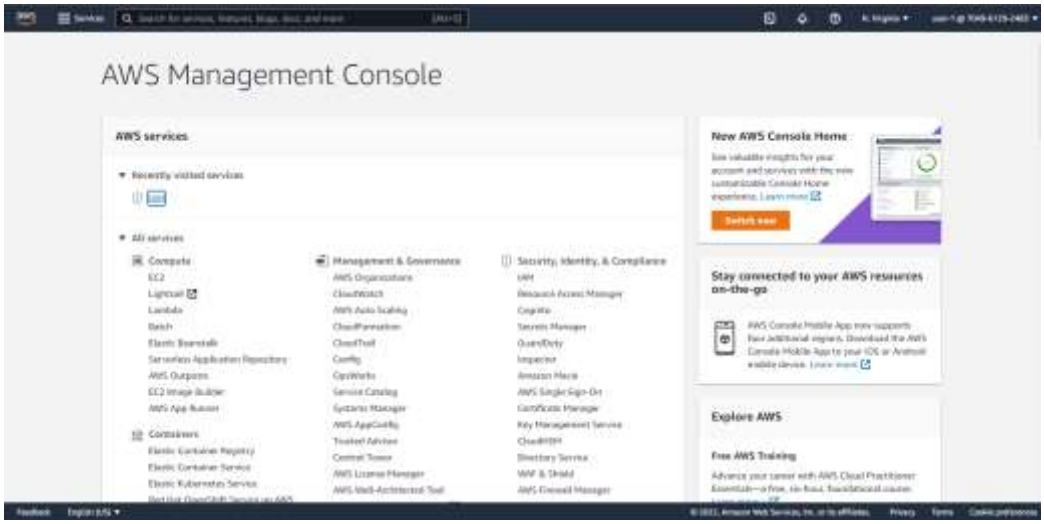

Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Credential report
Organization activity
Service control policies (SCPs)
Add users to S3-Support
Other users in this account (4)
User name
Groups
Last activity
awsstudent
You need permissions
None
user-1
user-2
user-3

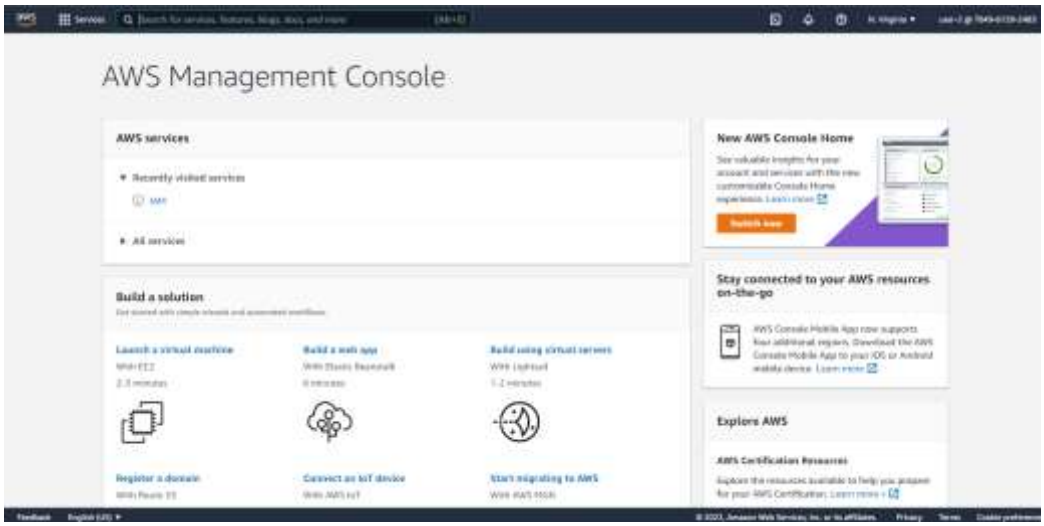

Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
New feature to generate a policy based on CloudTrail events.
Users > user-1
Summary
User ARN
Path
Creation time
Permissions
Groups
Tags (1)
Security credentials
Access Advisor
Permissions policies
Get started with permissions
Add permissions
Permissions boundary (not set)
You need permissions
Feedback
English (US)


Identity and Access Management (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
Service control policies (SCPs)
Users > user-1
Summary
User ARN
Path
Creation time
Permissions
Groups (1)
Tags (1)
Security credentials
Access Advisor
Add user to groups
Group name
Attached permissions
S3-Support
Feedback
English (US)


Identity and Access Management (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
Service control policies (SCPs)
Users > user-2
Summary
User ARN
Path
Creation time
Permissions
Groups (1)
Tags (1)
Security credentials
Access Advisor
Add user to groups
Group name
Attached permissions
EC2-Support
Feedback
English (US)







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