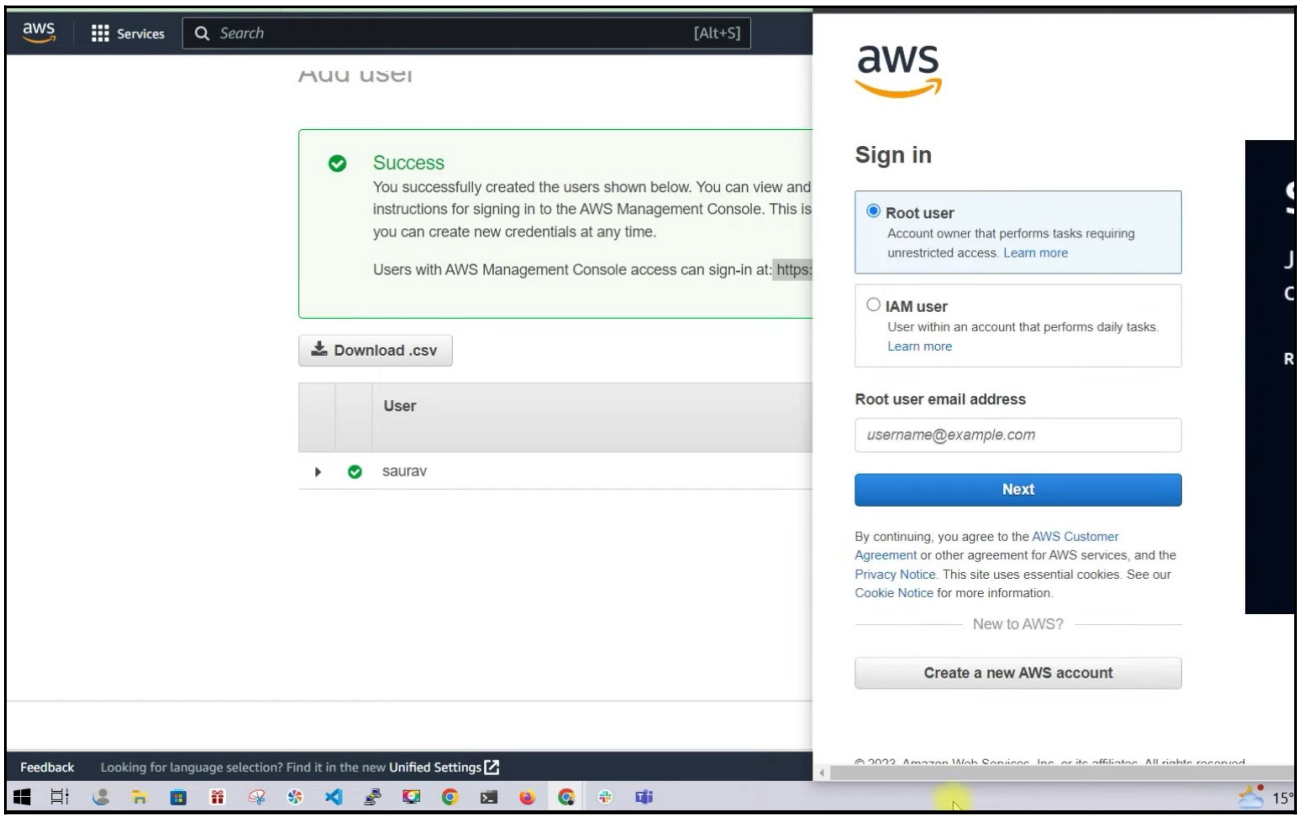
Experiment No. 8

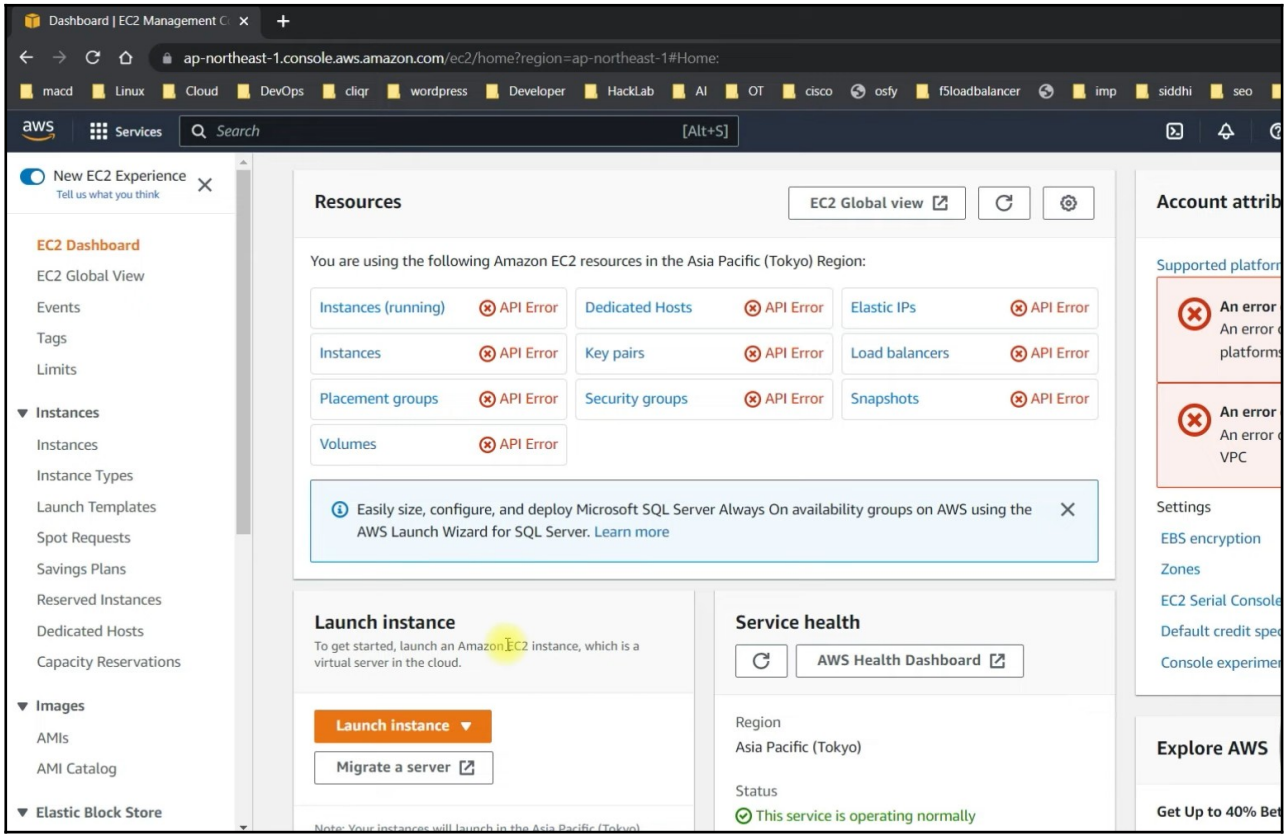
Aim: To study and implement Identity and Access Management (IAM) practices on AWS

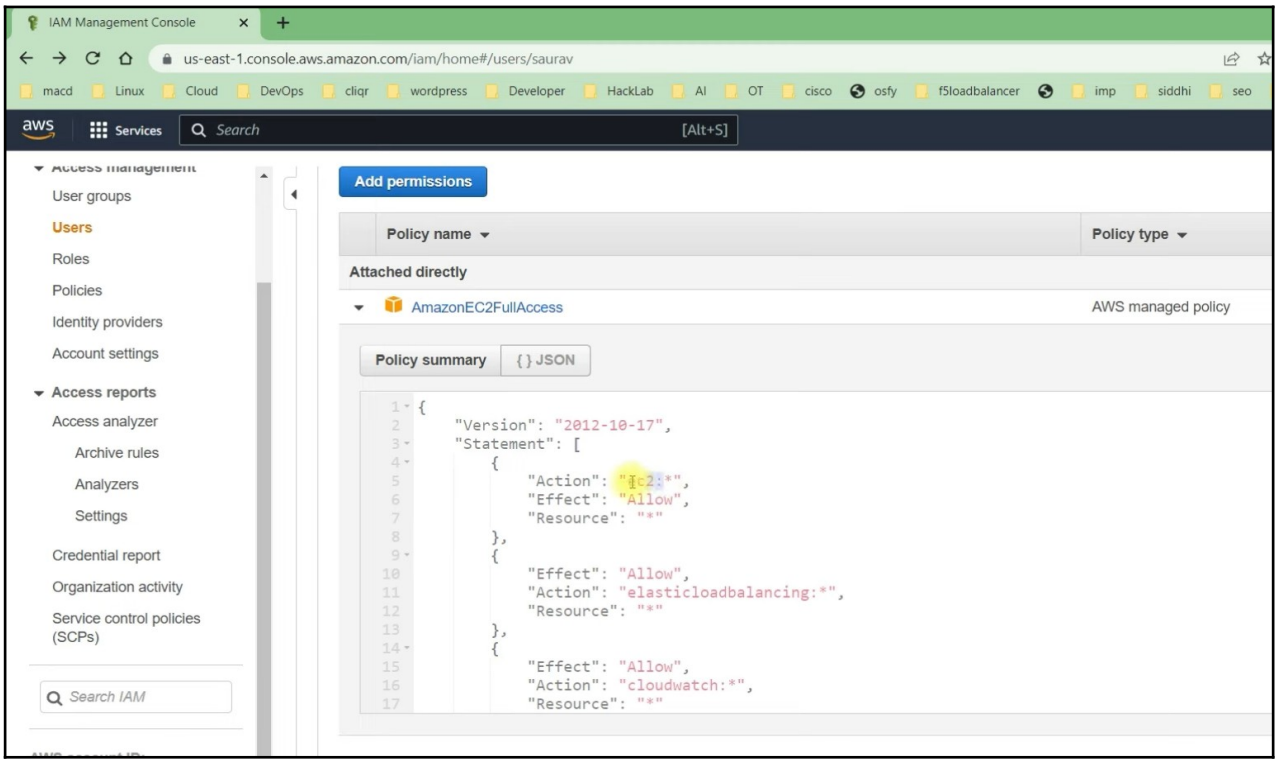
Theory:

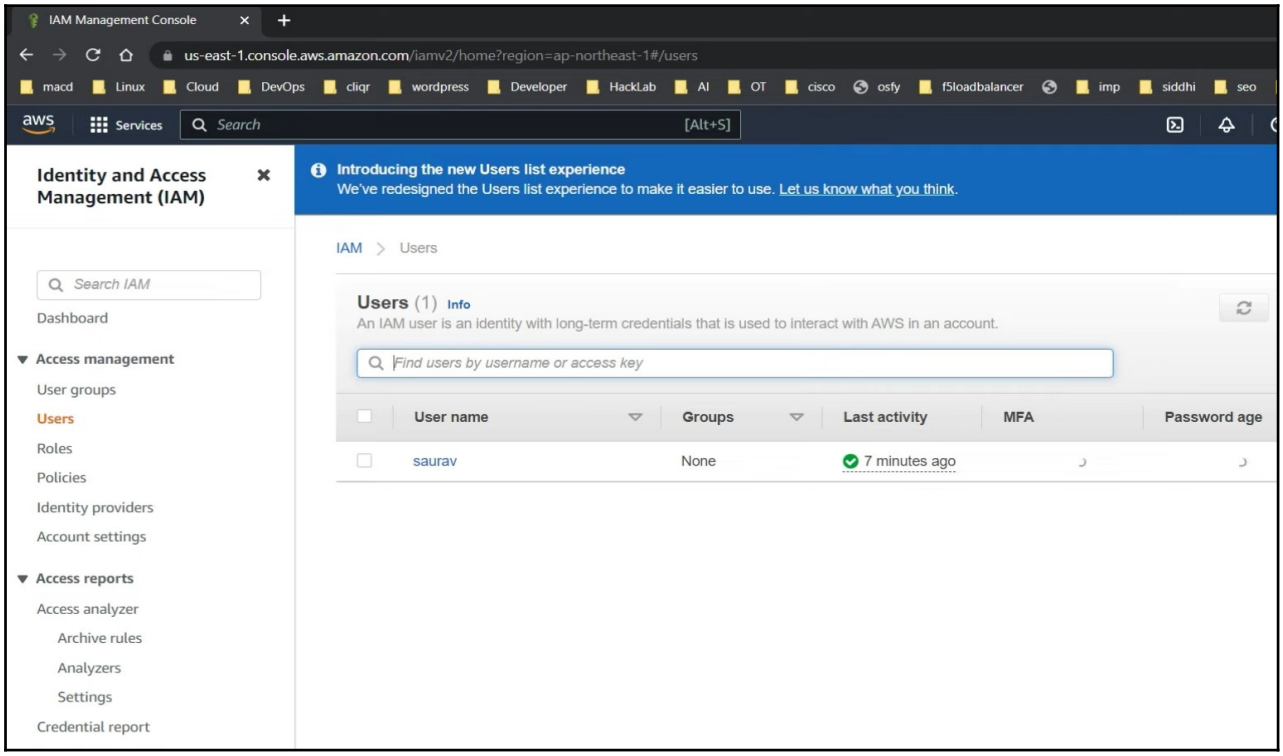
- Identity Management is a set of business processes, and a supporting infrastructure, for the creation, maintenance and use of digital identities.
- IAM is an essential function for protecting the privacy of information, enhancing user experience, enabling accountability, and controlling access to an organization's assets.
- IAM is the collection of processes and technology used to manage digital identities and the resource access provided through them.
- Components of access management
  - Establishing unique identities and associated authentication credentials.
  - Authoritative source is maintained as a central repository for storage.
  - Providing capability to identities to request entitlements
  - Assigning roles or entitlements to identities.
  - Managing off boarding and other business work processes by workflows
  - Providing capability to approve, revoke, review or certify entitlements or roles assigned to users.

Output:




Dashboard | EC2 Management C
ap-northeast-1.console.aws.amazon.com/ec2/home?region=ap-northeast-1#Home:
Services
Search
[Alt+S]
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Resources
EC2 Global view
You are using the following Amazon EC2 resources in the Asia Pacific (Tokyo) Region:
Instances (running) API Error
Dedicated Hosts API Error
Elastic IPs API Error
Instances API Error
Key pairs API Error
Load balancers API Error
Placement groups API Error
Security groups API Error
Snapshots API Error
Volumes API Error
Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more
Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
Migrate a server
Service health
AWS Health Dashboard
Region
Asia Pacific (Tokyo)
Status
This service is operating normally
Account attrib
Settings
EBS encryption
Zones
Explore AWS


IAM Management Console
us-east-1.console.aws.amazon.com/iam/home#/users/saurav
Services
Search
[Alt+S]
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)
Search IAM
Add permissions
Policy name
Policy type
Attached directly
AmazonEC2FullAccess
AWS managed policy
Policy summary
{ } JSON
{
"Version": "2012-10-17",
"Statement": [
{
"Action": "ec2:*",
"Effect": "Allow",
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "elasticloadbalancing:*",
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "cloudwatch:*",
"Resource": "*"



Conclusion: In AWS IAM (Identity and Access Management), users are entities that represent individuals or services interacting with AWS resources. Users are granted permissions through IAM policies, which specify what actions they can perform on which AWS resources. IAM allows you to create, manage, and delete users, enabling you to control access to your AWS environment securely. Users can have unique credentials (such as username and password) or use temporary security credentials for programmatic access. By managing users and their permissions, IAM helps organizations enforce the principle of least privilege, ensuring that users have only the access they need to perform their tasks.