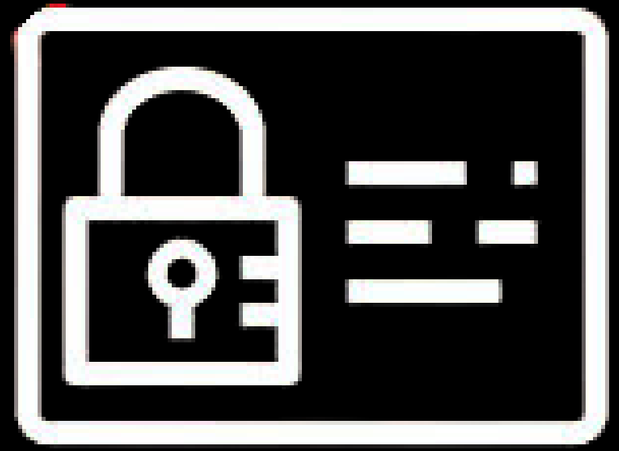
NARESH IT VEERA BABU BATCH

AWS IAM ROLE

BY TEAM SKYOPS

BATCH 10:30 AM

TABLE OF CONTENTS



WHAT IS IAM?

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources.

- It defines who (users, applications, or services) can access which resources, and what actions they can perform.
- IAM provides granular permissions through policies.
- It enables secure authentication (signing in) and authorization (granting permissions).

Why IAM is Needed?

Security
- Protects AWS resources from unauthorized access
- Prevents misuse of the root account

Granular Control
- Define who can access what
- Restrict actions (e.g., only read S3, not delete S3)

Centralized Access Management
- Manage permissions for all AWS services in one place
- Easy to add, update, or remove users

Scalability
- Works for a single user or large organizations
- Supports groups and roles to simplify permissions

Compliance & Auditing
- Enforce least privilege principle
- Track and log all access using CloudTrail

CONS OF IAM

Limited to AWS

- IAM manages AWS resources only
- For hybrid or multi-cloud, you need additional tools (like IAM Identity Center or external IdPs)

Access Key Management Issues

- If not rotated or secured, keys can be leaked
- Requires regular auditing

Global Service (No Region Isolation)

- IAM is global, so any misconfigured policy applies everywhere

IAM Component

Users
- Individual identities in AWS
- Have long-term credentials (username/password or access keys)

Groups
- Collection of users
- Permissions applied to group are inherited by all members

Roles
- Temporary access permissions
- Used by AWS services, applications, or external users

Policies
- Documents (in JSON) that define permissions
- Attached to users, groups, or roles

IAM POLICIES IN DETAIL

What is a Policy?
A JSON document that defines permissions in AWS
Controls what actions are allowed/denied and on which resources
Policies can be:

- AWS Managed (predefined by AWS)
- Customer Managed (created by you)
- Inline (attached directly to one identity)

DEMO

THANK YOU