IAM

Manage User Access & Encryption Key

Agenda

Why do we need Access Management?

What is IAM?

Components of IAM

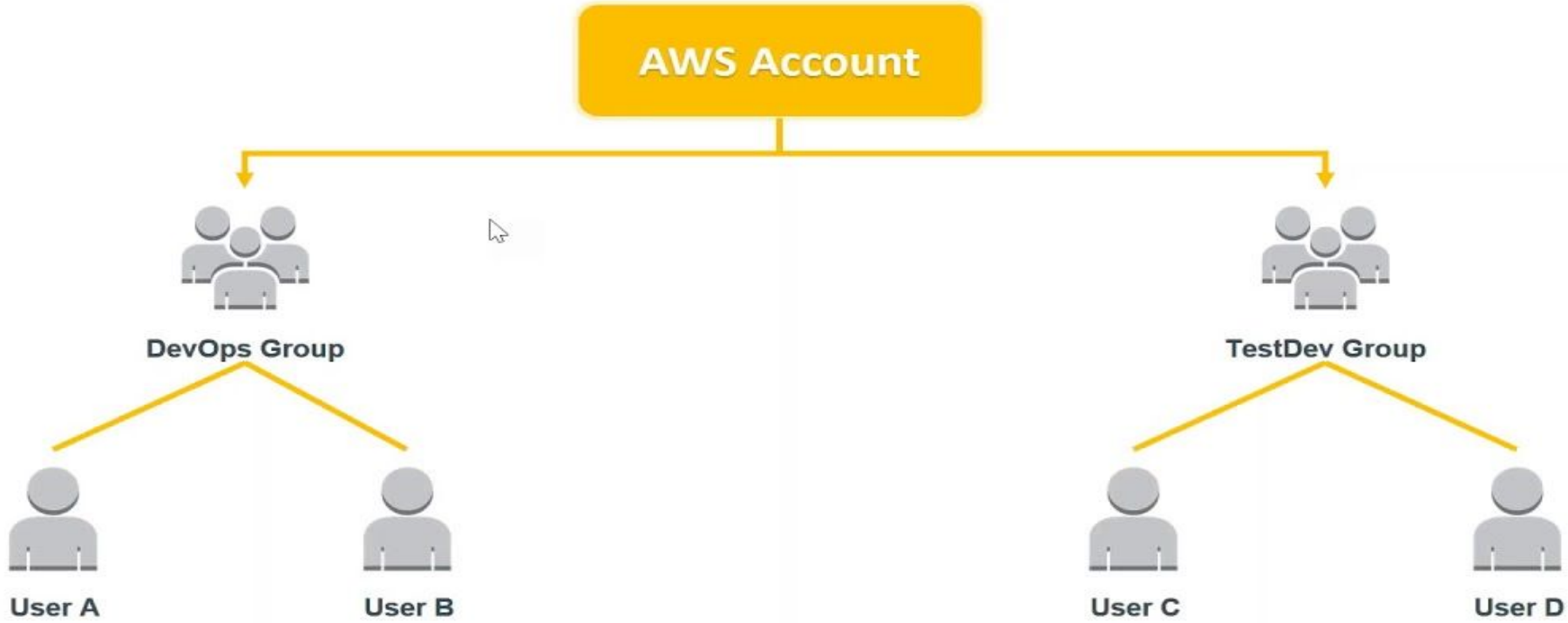
Multi Factor Authentication

Hands-on

IAM

- **AWS** Identity and Access Management (**IAM**) enables you to manage access to **AWS** services and resources securely
- **Securing Your AWS account using IAM**
- Using **IAM**, you can create and manage **AWS** users and groups, and use permissions to allow and deny their access to **AWS** resources.
- **IAM** is a feature of your **AWS** account offered at no additional charge.
- With IAM, Organizations can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.
- IAM enables the organization to create multiple users, each with its own security credentials, controlled and billed to a single aws account. IAM allows the user to do only what they need to do as a part of the user's job.

IAM: Groups


AWS Account
DevOps Group
TestDev Group
User A
User B
User C
User D

Features of IAM

Centralised control of your AWS account: You can control creation, rotation, and cancellation of each user's security credentials. You can also control what data in the aws system users can access and how they can access.

Shared Access to your AWS account: Users can share the resources for the collaborative projects.

Granular permissions: It is used to set a permission that user can use a particular service but not other services.

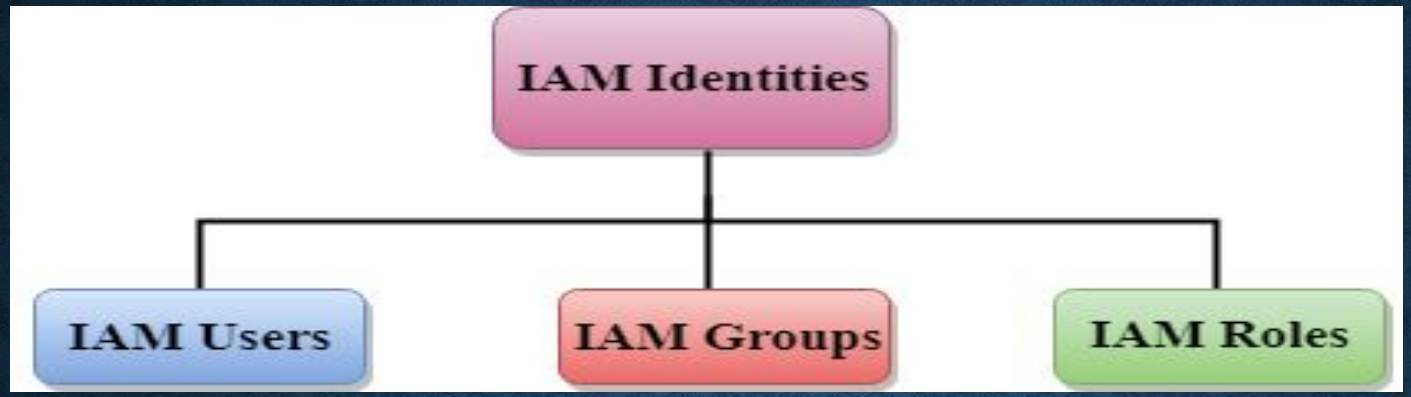
Multifactor Authentication: An AWS provides multifactor authentication as we need to enter the username, password, and security check code to log in to the AWS Management Console.

Permissions based on Organizational groups: Users can be restricted to the AWS access based on their job duties, for example, admin, developer, etc.

Networking controls: IAM also ensures that the users can access the AWS resources within the organization's corporate network.
Provide temporary access for users/devices and services where necessary: If you are using a mobile app and storing the data in AWS account, you can do this only when you are using temporary access.

Integrates with many different aws services: IAM is integrated with many different aws services.

IAM Identities



AWS Account Root User

When you first create an AWS account, you create an account as a root user identity which is used to sign in to AWS.

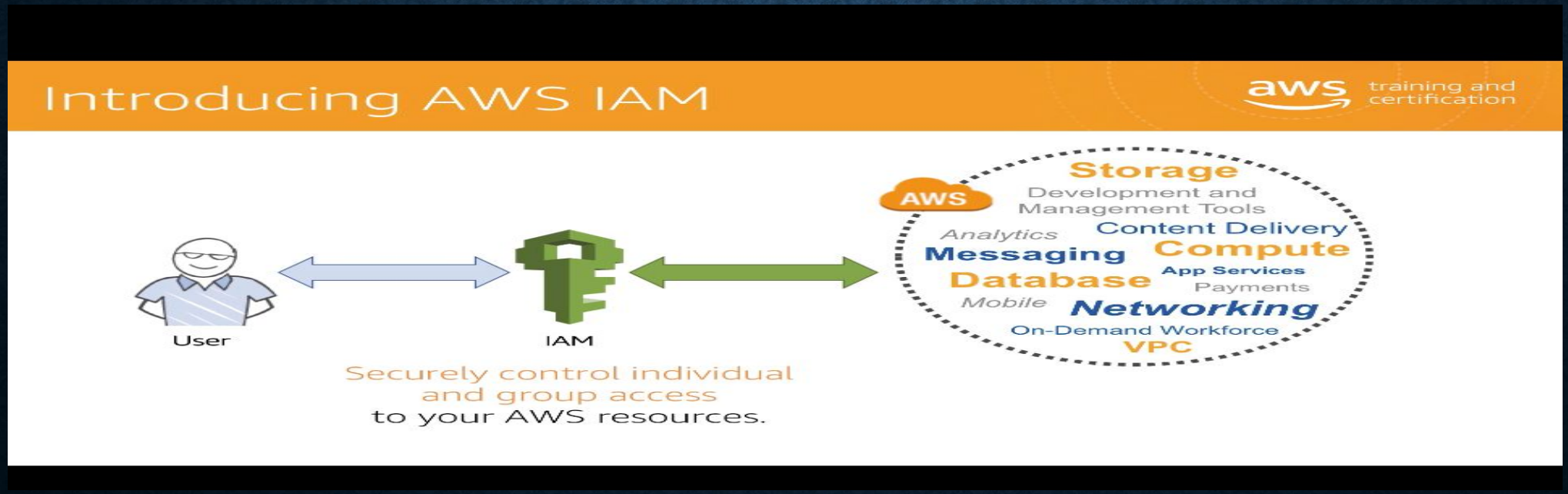
You can sign to the AWS Management Console by entering your email address and password. The combination of email address and password is known as **root user credentials**.

When you sign in to AWS account as a root user, you have unrestricted access to all the resources in AWS account.

The Root user can also access the billing information as well as can change the password also.

IAM Identities

User
Specific Individual , can receive personal logins.
Group
Collection of IAM users that you can manage as a unit.
Roles
Are a secure way to grant permissions to entities that you trust.
Policy
Set of Permissions



DEMO