LOGICLABS TECHNOLOGIES

www.logiclabstech.com

Amazon Web Services

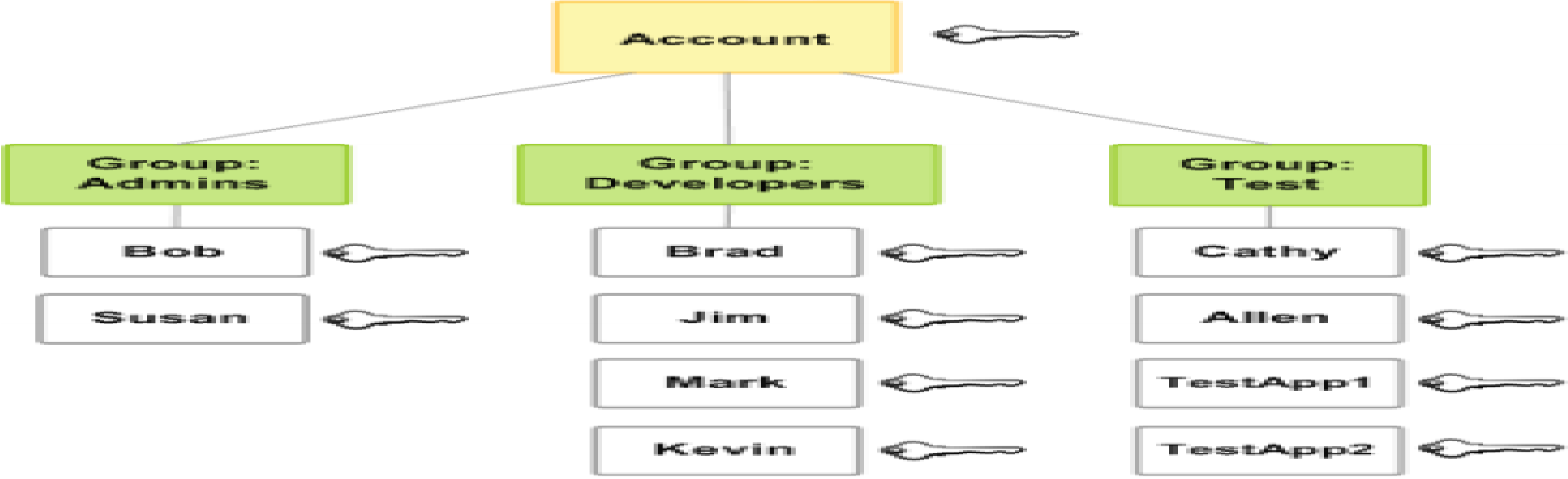
Identity & Access Management

ankitnarula1991@gmail.com

Identity & Access Management - IAM

- AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM can also keep our account credentials private.

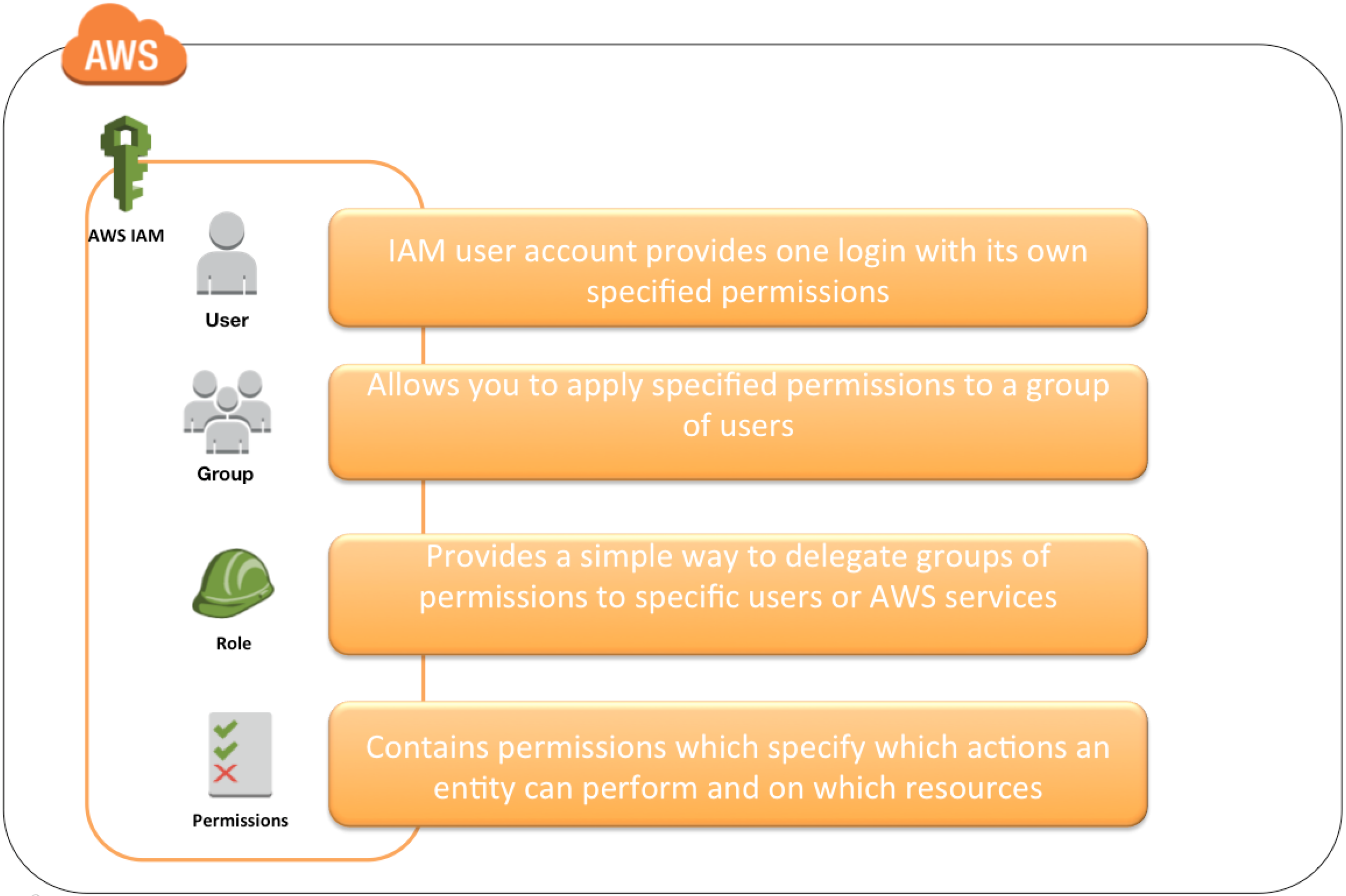
- When we first create an AWS account, it has complete access to all AWS services. This identity is called the AWS account root user



IAM - Features

- **Shared access to the AWS account**: The main feature of IAM is that it allows you to create separate usernames and passwords for individual users or resources and delegate access.
- **Multifactor authentication (MFA)**: IAM supports MFA, in which users provide their username and password plus a one-time password from their phone a randomly generated number used as an additional authentication factor.
- **Identity Federation**: If the user is already authenticated, such as through a Facebook or Google account, IAM can be made to trust that authentication method and then allow access based on it.
- **Free to use**: There is no additional charge for IAM security. There is no additional charge for creating additional users, groups or policies.
- **Password policy**: The IAM password policy allows you to reset a password or rotate passwords remotely.
- **Granular permissions**: Each user can be granted with different set granular permissions as required to perform their job

IAM - Important Terms



IAM user account provides one login with its own specified permissions

Allows you to apply specified permissions to a group of users

Provides a simple way to delegate groups of permissions to specific users or AWS services

Contains permissions which specify which actions an entity can perform and on which resources

IAM - Types of Account in AWS

- Root User
- IAM User

- **Root User**

- Root Account Credentials are the email address and password with which we sign in into the AWS account
- Root Credentials has full unrestricted access to AWS account including the account security credentials which include sensitive information
- An Administrator account can be created for all the activities which too has full access to the AWS account except the accounts security credentials, billing information and ability to change password

IAM - Types of Account in AWS

- IAM User

- IAM user represents the person or service who uses the access to interact with AWS.
- IAM user starts with no permissions and is not authorized to perform any AWS actions on any AWS resources and should be granted permissions as per the job function requirement.
- Each IAM user is associated with one and only one AWS account.
- IAM User cannot be renamed from AWS management console and has to be done from CLI or SDK tools.

IAM – Create

- Create Two IAM user.

- One user will access only EC2 Machines & Second user will access only S3 Buckets.

- Go to IAM

- Click on Users

- Click on Add Users

- Enter the user name

IAM – Create

- Select AWS Access Type.

- We can connect our AWS account with 2 ways.
- Console Access (Graphical Access)
- Command Line Interface (CLI)

- Select custom password & enter the password

- Uncheck require password reset

- Click on Next: Permissions

IAM – Create

- Click on Attach existing policies directly
- Search the EC2 full Access policy
- Select the policy
- Click on Next: Tags
- Click on Next: Review
- Click on Create user
- Create Another User Given S3 Full Access

IAM – Login

- Note down the console ID of your root user
- Go to the AWS URL
- Select IAM User
- Enter the Account ID (Console ID)
- Click on Next
- Enter IAM user name & password
- Click on Sign In
- Change the Password

ankitnarula1991@gmail.com