



IAM Best Practices for Security



Faraz Sarwar

Senior Web Developer at Sudofy

I am a Full-Stack JavaScript and AWS
Certified Associate developer, having a 2+
years experience on AWS



Why Do We Need Access Management?

Why Do We Need Access Management?

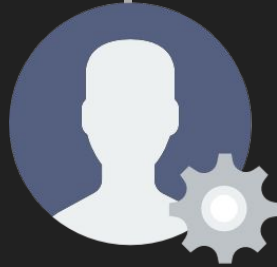


Web Portal

Why Do We Need Access Management?

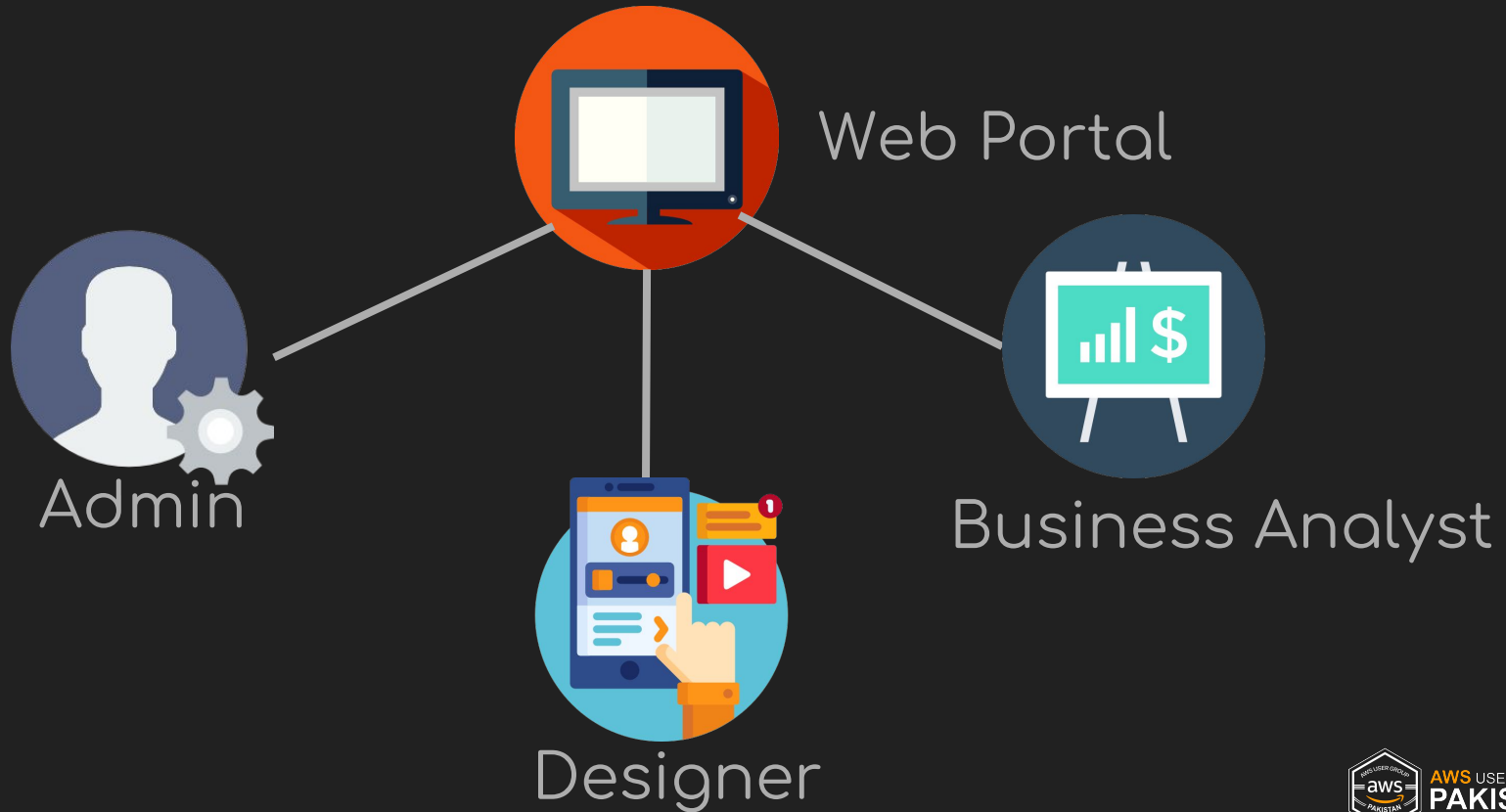


Web Portal



Super User

Why Do We Need Access Management?



What is AWS IAM?



What is AWS IAM?

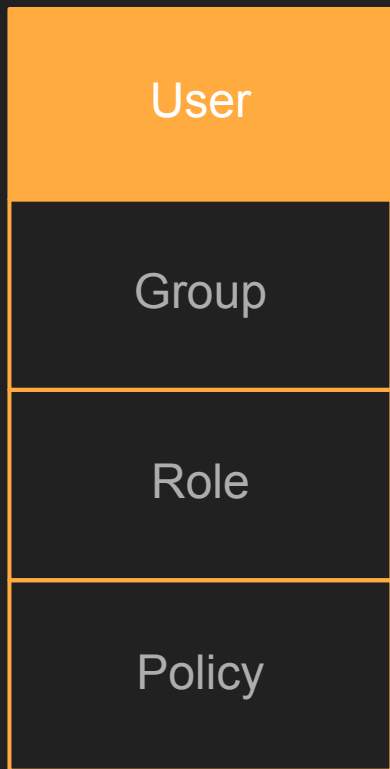
AWS Identity and Access Management (IAM) is a service that helps you securely control access to AWS resources for your users. It is used to create accounts and manage authorization on AWS resources.

Components of AWS IAM

There are four main components of AWS IAM

- USER
- GROUP
- ROLE
- POLICY

Components of IAM



WHO IS THAT USER?

Components of IAM

User

Group

Role

Policy

Using IAM, you can create and manage AWS users, and their permissions to allow and deny their access to AWS resources.

Components of IAM

User

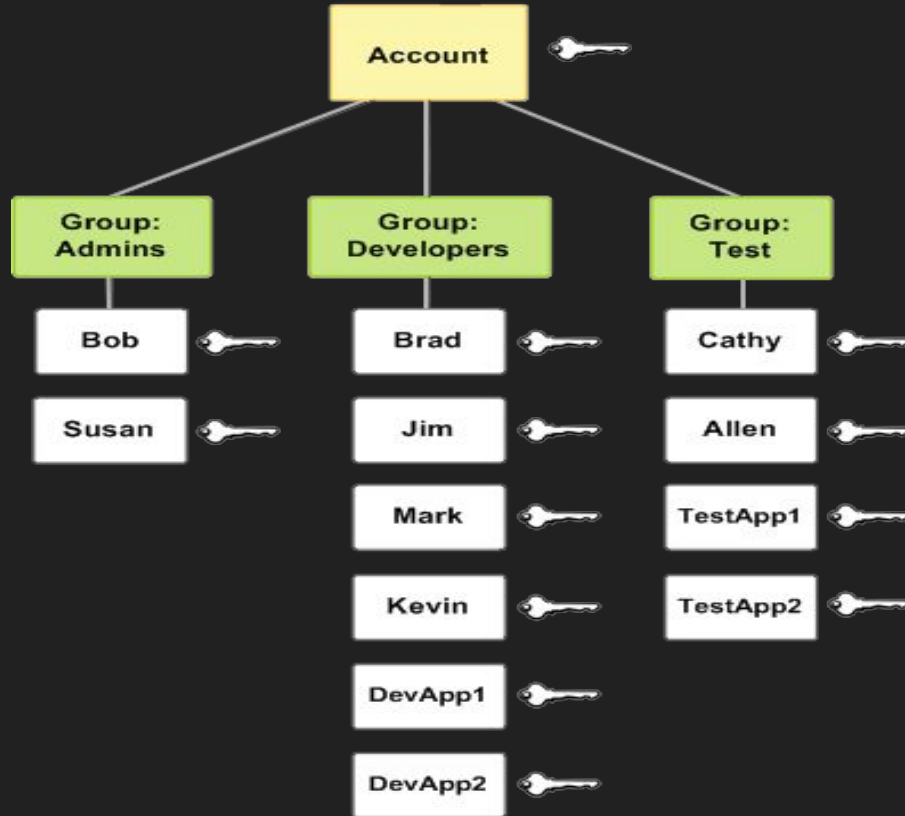
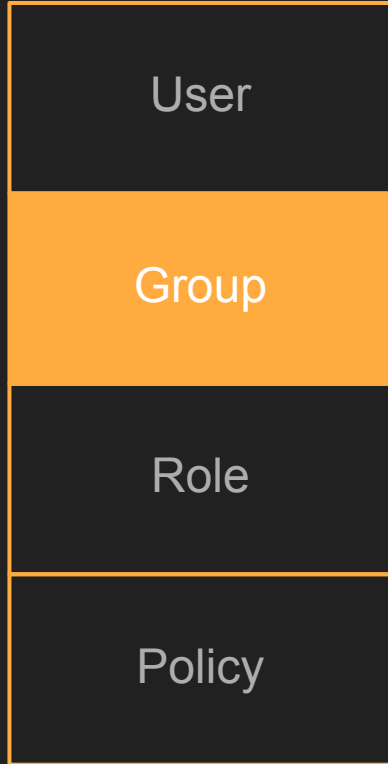
Group

Role

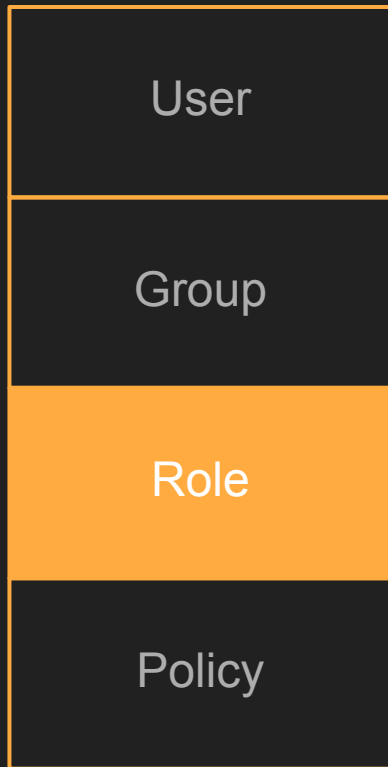
Policy

An IAM group is a collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users

Components of IAM

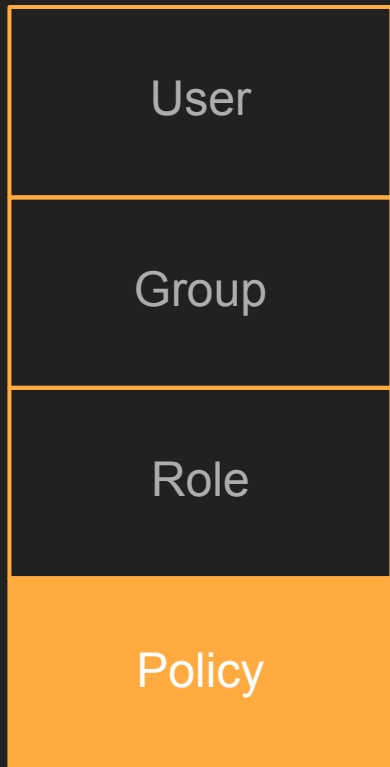


Components of IAM



An IAM role is an IAM entity that defines the set of permissions for making AWS service request. It determine what the identity can and cannot do in AWS.

Components of IAM



To assign permissions to a user, group, role or resource you create a policy which is a document that lists permissions.

Best Practices For Security

RULE 1

Never use your root account for day to day tasks instead creating an admin user for yourself

According to the Identity Theft Resource Center

1,093

Breaches occurred last year

According to the Identity Theft Resource Center

40%

Increase from 2016

RULE 2

Lock away your AWS account root
user access keys

RULE 3

Grant least privileges

RULE 4

Use roles to delegate permissions

RULE 5

Use roles for applications that run
on Amazon EC2 instances

RULE 6

Rotate Credentials Regularly

RULE 7

Monitor Activity in Your AWS Account



Thank you