**AWS Identity and Access Management (IAM) Global**

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

IAM has a global view.

Policies are written in Json

Your whole AWS security is there:

* + Users Phy person
  + Groups Grp of users
  + Roles Its for machine [only for internal usage within aws resources]

[One IAM Role per application]

IAM Features

* You can grant other people permission to administer and use resources in your AWS account without having to share your password or access key.
* You can grant different permissions to different people for different resources.
* Multi-factor authentication (MFA)
* Identity federation

You can allow users who already have passwords elsewhere—for example, in your corporate network

Accessing IAM

* AWS Management Console
* AWS Command Line Tools
* AWS SDKs
* IAM HTTPS API

AWS POLICY SIMULATOR

Used to test the policies

Admin Policies

**{**

**"Version": "2012-10-17",**

**"Statement": [**

**{**

**"Effect": "Allow",**

**"Action": "\*",**

**"Resource": "\*"**

**}**

**]**

**}**