IAM :- identity and Access management

Features :-

* Shared access and AWS account
* Granular permissions :- you can grant different permission to different people to access resources
* Secure access to AWS resources for application that run on amazon EC2.
* Multi-factor authentication (MFA) :- for two-factor authentication to your account and to individual uses for extra security.
* Identity federation :- you can allow users who already have password
* Free to use

TERMS OF IAM :-

* IAM resources :- the user, group, role, policy and id provider objects that are stored in AWS. As another resources you can add, edit and remove the resources from IAM
* IAM identity :- the IAM resource object that are to identify and group. You can attach policy to an IAM identity. This includes roles, users, group.
* IAM entities :- the IAM resource objects that AWS use for authentication. This include roles and users.
* Principals :- a person or application that uses the AWS account root user, an IAM user, or an IAM role to sign in and make request to AWS. Principal included federated users and assumed roles.

**HOW IAM WORKS** :-

**Contents :-**

1. **Terms**

* IAM resource :- role, users, policy, group, identity provider
* IAM identity :- it is for to identify and group. You can attach policy to an IAM identity. This included user, group, role
* IAM entity :- it is use for authentication
* Principal

1. **Principal**
2. **Request**

* Action or operation :- that the principal want to perform. it can be AWS CLI, AWS API
* Resources :- resource object upon which action or operation want to perform
* Principal
* Environment data :- information about IP, user agent, SSL enable status
* Resource data :- data related to resource that being requested e.g:- dynamodb, EC2

1. **Authentication**
2. **Authorization**
3. **Actions or operations**
4. **Resources**

**ABAC :- attribute based access control**

This is nothing but the tag. These ABAC policy can be design to allowed when the principal tags matches with the resources tags.

1. At a time we can create 10 users and maximum 5000
2. At a we can create 10 groups and maximum 300
3. We can create maximum roles 1000.
4. Maximum policies we can create 1000
5. One user we can add in 10 groups
6. You can attached 10 policies in one group
7. 20 policies we can attached in one IAM user
8. 10 policies we can attached in one IAM group