**What Is IAM?**

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users.

You use IAM to control who can use your AWS resources (authentication) and what resources they can use and in what ways (authorization).

## IAM Users

you can create individual IAM users within your account that correspond to users in your organization. IAM users are not separate accounts; they are users within your account. Each user can have its own password for access to the AWS Management Console.   
  
By default, a brand new IAM user has no [permissions](http://docs.aws.amazon.com/IAM/latest/UserGuide/access.html) to do anything. The user is not authorized to perform any AWS actions or to access any AWS resources, you provide the appropriate permissions after creating user.  
  
You can set a password policy on your AWS account to specify complexity:

* Set a minimum password length.
* Prevent reusing same password.
* change their password after a specified period of time

## Access keys (access key ID and secret access key)

Access keys consist of an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY).

You use access keys to **sign programmatic requests** that you make to AWS

Access keys are generated separately for a IAM user. You can have a **maximum of two** access keys (active or inactive) at a time.  
  
If you or your IAM users forget or **lose the secret access** key, you **can create a new access** key pair, but you **can’t recover** the previous lost one.

# IAM Groups

An IAM [group](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html) is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users.

A group can contain many users, and a user can belong to multiple groups. But group cant be a part of another group.

It is simply a way to attach policies to multiple users at one time.so that all the users in one group share the same permissions.

# IAM Roles

An IAM role is an IAM entity that defines a set of [permissions](https://aws.amazon.com/iam/details/manage-permissions/) for making AWS service requests.  
  
IAM roles for EC2 instances enables your applications running on EC2 to make requests to AWS services , without you having to copy AWS access keys to every instance.

**Note**: - You can only **associate one IAM role** with an EC2 instance at this time. you **cannot change the IAM role** on a running EC2 instance.   
Also You can only associate an IAM role **while launching** an EC2 instance.

# IAM Policies

To assign permissions to a user, group, role, or resource, you create a policy, which is a document that explicitly lists permissions.  
  
You can add up to 10 managed policies to a user, role, or group.

**AWS account alias**

The account alias is a name you define to make it more convenient to identify your account.

You can have one alias per AWS account.

# MFA Devices With Your IAM Sign-in Page

IAM users who are configured with multi-factor authentication (MFA) devices must use their MFA devices to sign in to the AWS Management Console.  
After the user types the user name and password, AWS checks the user's account to see if MFA is required for that user. If so, a second sign-in page appears with an **MFA code** box to enter the numeric code provided by an MFA .

To install MFA, we can install a app like “ Google Authenticator” in our smartphone & sync the MFA generated for the respective user.

Questions

+++++++++++++++++++++++++++++++++++++

how to create Users? what is secret & access keys?

what is the process to recover secret key?

What is a group?

Can I define a password policy for my user’s passwords?

what is IAM role? Can I associate more than one IAM role with an EC2 instance? Can I associate an IAM role with an already running EC2 instance?

Can I change the IAM role on a running EC2 instance?

what is policies? how many policies can we attached to a user max?

What is an AWS account alias?

how to enable MFA security to user?

+++++++++++++++++++++++++++++++++++++