



# IAM

## O que é o IAM?

**Identity Access Management** é o sistema utilizado para gerenciar os usuários da plataforma AWS e os seus privilégios, se quiser usar a AWS, tem que entender o IAM.

## Features

- Controle centralizado da conta.
- Acesso compartilhado da sua conta
- Permissões granulares
- Identity Federation (Logar com a conta do Facebook, LinkedIn, Active Directory (Windows) etc.).
- Autenticação multi-fator
- Acesso temporário para usuários/dispositivos quando necessário
- Definição de uma política de senha rotacional

1

## Users

End Users such as people, employees of an organization etc.

2

## Groups

A collection of users. Each user in the group will inherit the permissions of the group.

3

## Policies

Policies are made up of documents, called Policy documents. These documents are in a format called JSON and they give permissions as to what a User/Group/Role is able to do.

4

## Roles

You create roles and then assign them to AWS Resources.

Job Functions (Cargos de usuários e suas permissões):

[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_job-functions.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html)

## What Have We Learnt So Far?

- **IAM is universal.** It does not apply to regions at this time.
- The **"root account"** is simply the account created when first setup your AWS account. It has complete Admin access.
- New Users have **NO permissions** when first created.
- New Users are assigned **Access Key ID & Secret Access Keys** when first created.
- **These are not the same as a password.** You cannot use the Access key ID & Secret Access Key to Login in to the console. You can use this to access AWS via the APIs and Command Line, however.
- **You only get to view these once.** If you lose them, you have to regenerate them. So, save them in a secure location.

## Criando Um Alarme de Gastos

É possível definir um aviso de gastos dentro do painel da **CloudWatch**

- O aviso pode ser definido de acordo com uma métrica da sua escolha, por exemplo: valor gasto em dólar, quantidade de chamados na API, uso de recurso da instância, dentre outros parâmetros.
- O alarme de gastos utiliza o SNS (Simple notification service) para alertar o cliente sobre a métrica.

## Os Acessos à AWS

Para acessar a AWS, temos 3 opções:

- **AWS Management Console** (Painel de gerenciamento da web) ⇒ **senha + MFA**
- **AWS Comand Line Interface** (CLI) ⇒ **access key**
- **AWS Software Developer Kit** (SDK - Utilizado em chamadas da API) ⇒ **access key**

Access keys são secretas, como senhas. **NÃO AS COMPARTILHE!**

Access Key ID ≠ Username  
Password

Secret Access Key ≠

## Anotações

- Quando você cria uma conta AWS, você cria apenas o usuário raiz, o qual deve ter seu uso evitado. Para criar usuários na conta, basta acessar o painel do IAM e criar os usuários, dessa forma você também pode definir os privilégios deles.
- Um usuário pode pertencer a vários grupos
- Os roles (funções) são permissões que são atribuídas para os serviços da AWS, por exemplo: dar permissão para uma EC2 ter acesso a uma opção da plataforma AWS.
- Através do IAM, é possível gerar um relatório das credenciais dos usuários na opção **Credencial Report**
- Ao clicar nos detalhes do usuário, você pode ir no painel **Access Advisor** para visualizar quais serviços o usuário acessou, qual período ele acessou pela última vez e qual política deu a ele esse direito, bem utiu para gerenciar acesso.
- **As políticas IAM são definidas em formato JSON.**
  - As permissões são definidas de fato no valor de "Statement".

