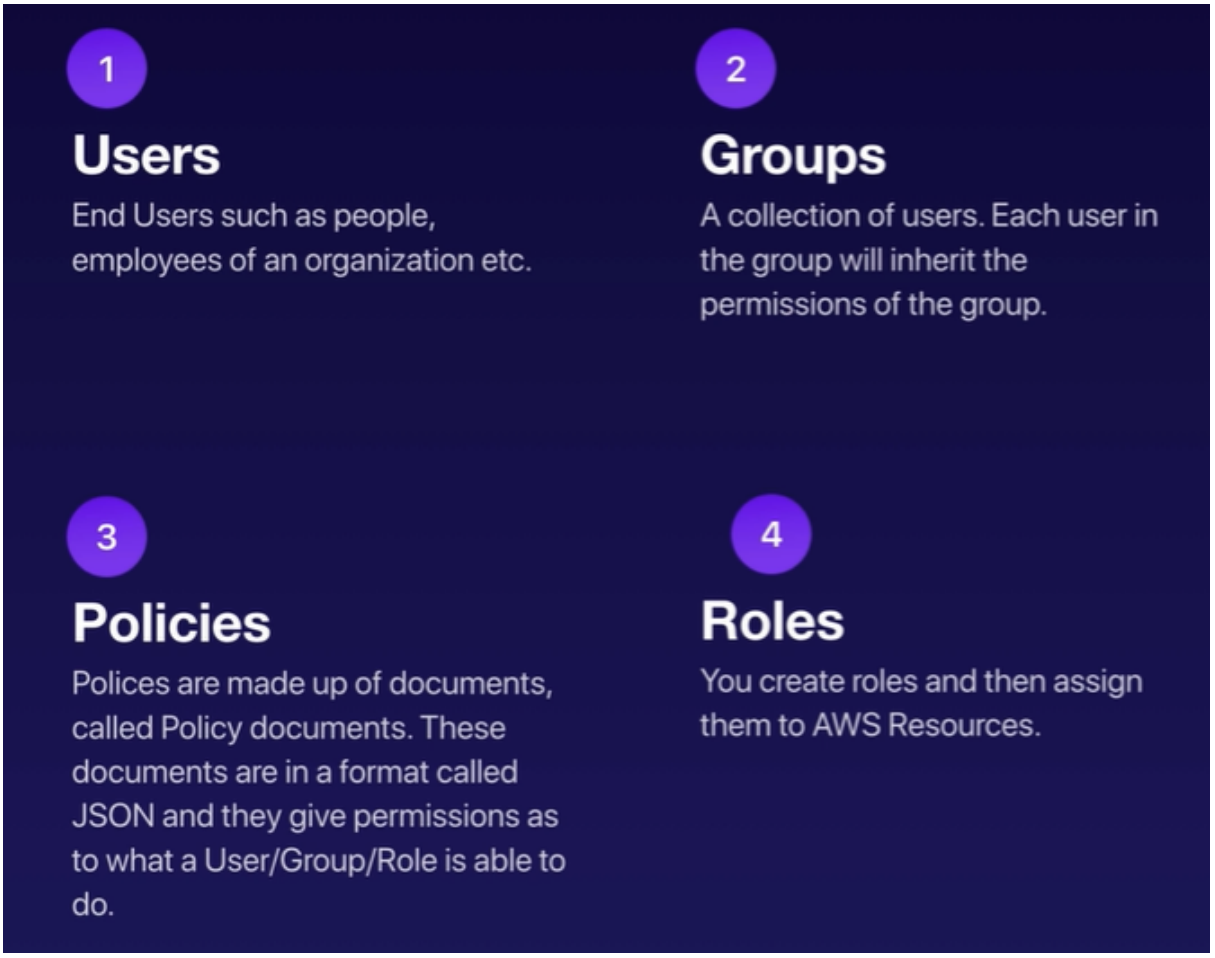
IAM

O que é o IAM?

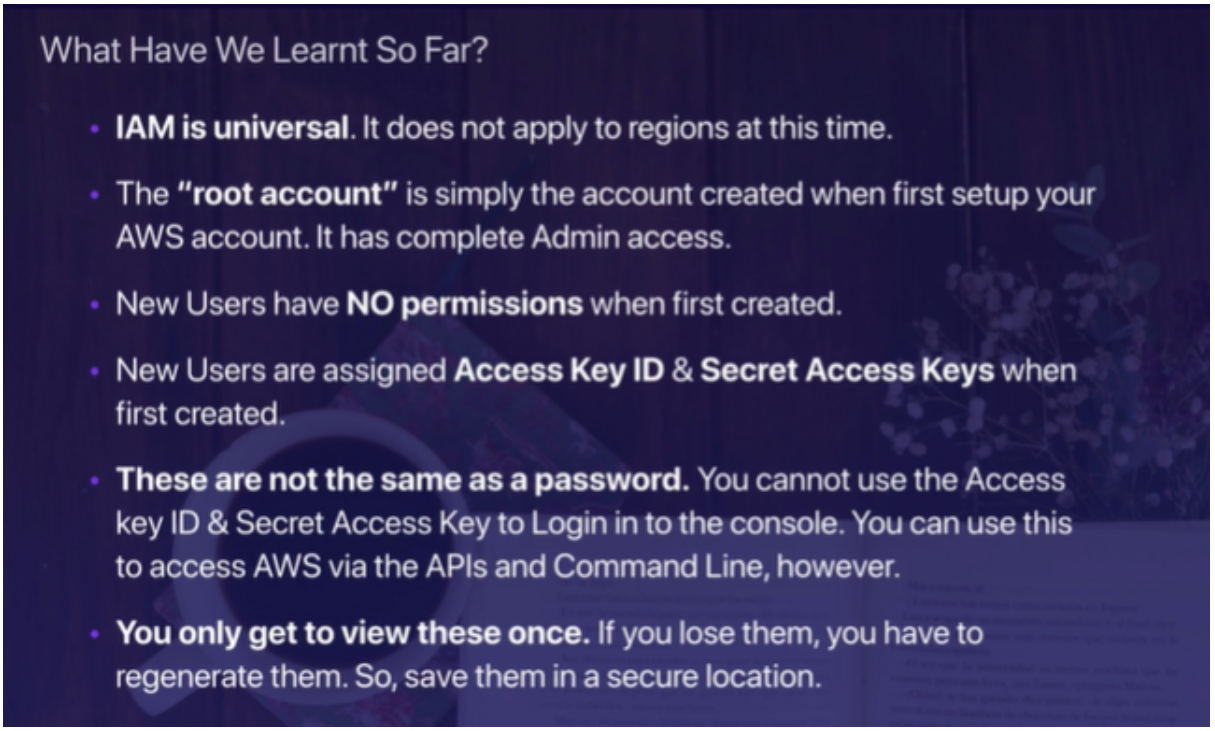
Identity Acess Management é o sistema utilizado para gerenciar os usuários da plataforma AWS e os seus privilégios, se quiser usar a AWS, tem que entender o IAM.

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



Job Functions (Cargos de usuários e suas permissões): https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html



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, dentr 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 **Secret Access Key ≠ Password**

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”.