AWS Identity and Access Management

IAM - Identity and Access Management

- Serviço que controla acesso aos recursos na AWS
- Permite criar e controlar usuários, autenticação ou limitar acesso de usuários a recursos

IAM controla QUEM pode fazer O QUE na sua conta AWS

IAM - Identity and Access Management

Autenticação (Quem)

- AWS Management Console
  - Usuário e Senha
- AWS CLI ou SDK API
  - Access Key e Secret Key

Autorização (Permissões)

- Arquivo JSON
  - Permissões em detalhes
  - Users, Groups e Roles

IAM - Identity and Access Management

GROUPS

USERS

ROLES

POLICIES

IAM - Identity and Access Management

USERS

Pessoa ou Serviço que interage com a AWS

João

- Nome único
- Pode ter um conjunto de credenciais
  - Senha da Console da AWS
  - Access Key (Acesso via SDK ou CLI)
  - MFA - Multi Factor Authentication (Software, Hardware, SMS)
- Tem que estar associado a apenas uma conta da AWS
- Permite acesso de forma humana ou programada (API ou CLI)

IAM - Identity and Access Management

GROUPS

RH

Grupo de Usuários

- **Agrupa usuários por departamento, função, afinidades, etc**
- **Usuários compartilham as mesmas permissões (Policies)**
- **Facilitam o gerenciamento de Usuários**

IAM - Identity and Access Management

POLICIES

JSON

Definem QUEM tem acesso AO QUE e O QUE podem fazer

- São descritas no formato JSON
- Por padrão não dão acesso a nada
- Podem ser assinaladas para Users, Groups e Roles
- Define em detalhes as ações que podem ser executadas

IAM - Identity and Access Management

POLICIES

Definem QUEM tem acesso AO QUE e O QUE podem fazer

- **QUEM**
- **AÇÕES**
- **RECURSO**
- **QUANDO**
- **ONDE**

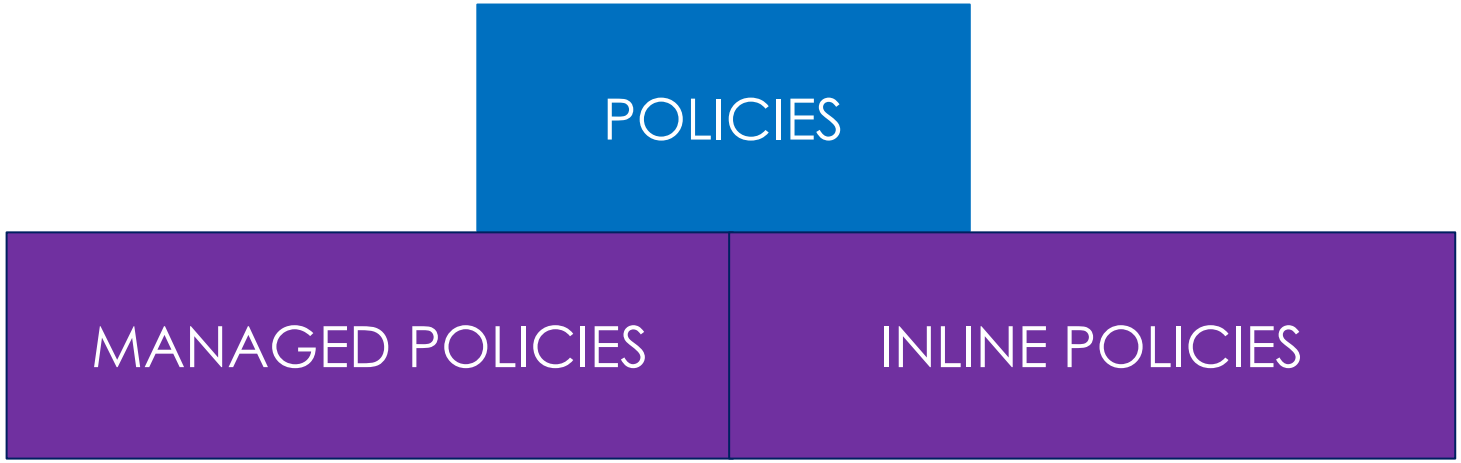
Rogerio
GET objetos no S3
Bucket = "*"
Até Dezembro 2021
A partir do IP 179.20.1.1

IAM - Identity and Access Management

POLICIES

```
{
  "Version": "2008-10-17",
  "Id": "example-ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:<region>:<account id>:<topic name>",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:*:*:<bucket name>"
        }
      }
    }
  ]
}
```

IAM - Identity and Access Management



- Criadas e Mantidas pela AWS
- Atualização Automática
- Gerenciamento de Mudança Centralizado
- Reutilizável

- Criadas pelos Clientes
- Permite maior definição e granularidade
- Pode ser apagada quando o "principal" for apagado

IAM - Identity and Access Management

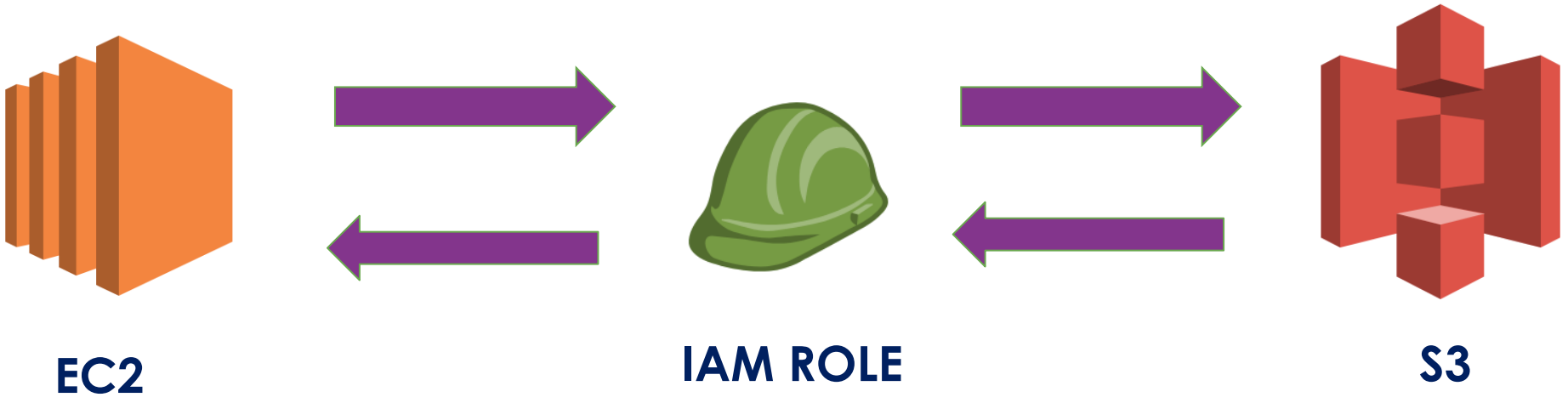
ROLE

Report Processor

Função/Papel que interage com a AWS

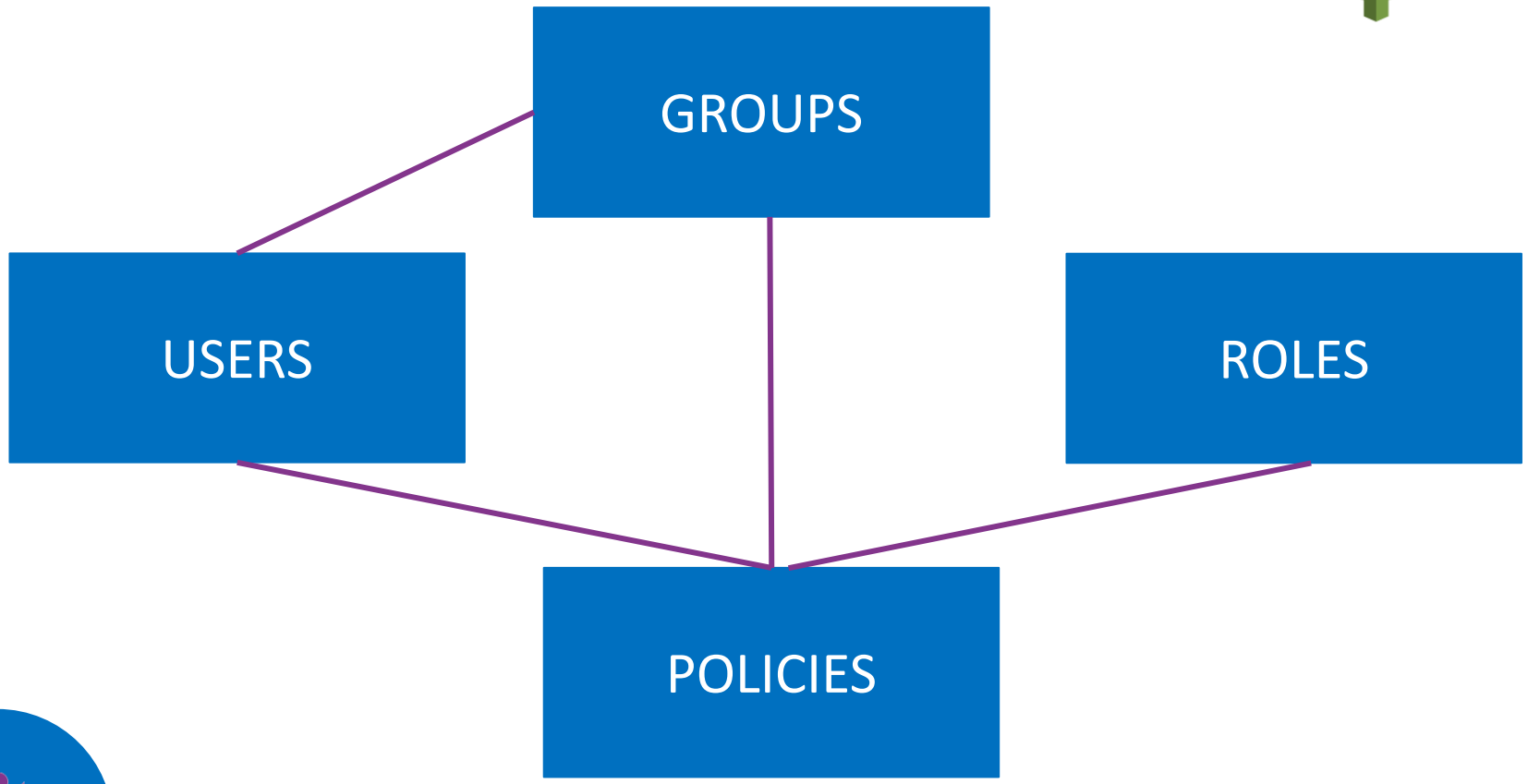
- **Usa as Policies**
- **Não possui credenciais.**
- **Chaves de Acesso são criadas dinamicamente**
- **Usuários, aplicações e serviços podem assumir IAM Roles**

IAM - Identity and Access Management



Exemplo: Uma máquina EC2 pode ter acesso a arquivos do S3 sem precisar de um usuário específico, apenas usando uma Role

IAM - Identity and Access Management




UniversidadeGlobal