Autenticação e Autorização
IAM

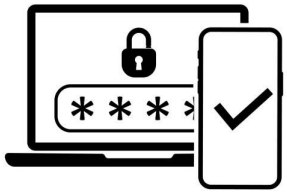
Prof. Raphael Rodrigues Pereira

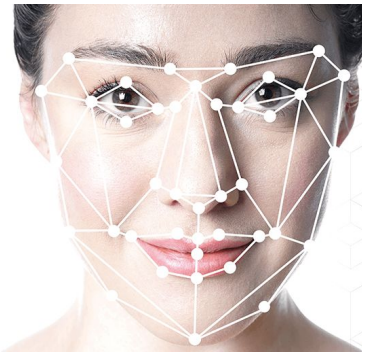
O que é Autenticação

- **Autenticação** é a confirmação da identidade de um usuário para ter acesso a algo.

Como pode ser feita a autenticação?

- Algo que eu saiba: Login e senha
- Algo que eu possua: Dispositivo móvel / Carteirinha / RG, CNH
- Algo que eu sou: Biometria Digital / Facial





Autorização

Controle de **permissões** sobre **o que o usuário pode acessar** depois de autenticado.

- Políticas de segurança
- Perfis
- Atributos e papéis.

IAM - Gerenciamento de Identidade e Acesso /

Identity and Access Management

Serviço da AWS responsável por **gerenciar identidades e controlar o acesso aos recursos**. Ele responde a duas perguntas fundamentais:

Quem você é?
Autenticação

O que você pode fazer?
Autorização

IAM = Acesso a um prédio corporativo

GROUP

USER

USER

USER

ROLE

POLICY

IAM - Gerenciamento de Identidade e Acesso / *Identity and Access Management*

Pilares fundamentais do IAM

IAM Users - Usuários

Conceito: Representam pessoas ou aplicações individuais que precisam acessar recursos AWS.

Analogia: Pense nos funcionários de uma empresa. Cada pessoa tem um crachá único com seu nome e foto - isso é o usuário no IAM.

Na prática:

- João Silva (desenvolvedor)
- Maria Santos (administradora de sistemas)
- Sistema de backup automatizado

IAM Users - Usuários

Características

- Possuem credenciais de longo prazo, como **nome de usuário e senha** para acesso ao **console AWS**, ou **chaves de acesso (Access Key ID e Secret Access Key)** para interações programáticas **via API ou CLI**.

- Por padrão, um novo usuário não tem permissão para fazer absolutamente nada na AWS. É como um funcionário novo no primeiro dia, sem crachá e sem acesso a nenhuma sala.

IAM Groups *(Grupos)*

Conceito: Coleções de usuários que compartilham as mesmas necessidades de acesso.

Analogia: Os departamentos da empresa. Todos do departamento de TI têm acesso à sala de servidores, todos do RH acessam o sistema de folha de pagamento.

Na prática:

- Grupo "Desenvolvedores"
- Grupo "Administradores"
- Grupo "Estagiários"

IAM Groups *(Grupos)*

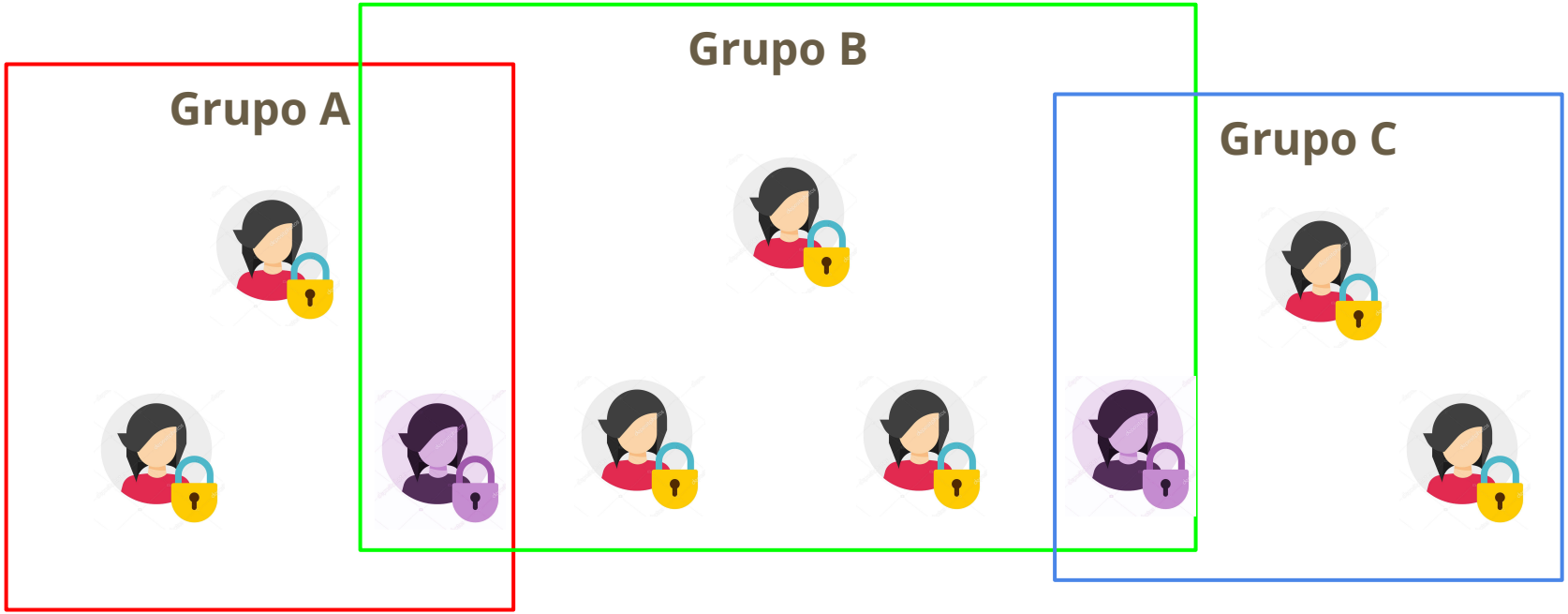
Características:

- Um usuário pode pertencer a **múltiplos grupos**.

- As **permissões** concedidas a um grupo são automaticamente herdadas por **todos os usuários membros desse grupo**.

- Não é possível "logar" como um grupo. Ele é apenas um contêiner para organizar usuários e gerenciar permissões de forma centralizada.

IAM - Usuários e Grupos de Usuários



IAM Roles *(Funções)*

Conceito: Conjunto de permissões que podem ser "assumidas" temporariamente por usuários, grupos ou serviços.

Analogia: É como um "crachá" temporário com acessos especiais. Um funcionário normal pode "utilizar o crachá" de gerente temporariamente para executar uma tarefa específica, como aprovar uma compra emergencial. Um técnico de manutenção pode utilizar um crachá temporário para acessar a sala de servidores e revisar o ar-condicionado.

Na prática:

- Role para aplicações EC2 acessarem S3
- Role para desenvolvedores assumirem privilégios de produção temporariamente
- Role para integração entre serviços AWS
- **Role para Lambda Function gravar dados no DynamoDB**

IAM Roles *(Funções)*

Quem pode assumir uma role?

- **Usuários IAM** na mesma conta ou em contas diferentes.
- **Serviços AWS** (por exemplo, uma instância EC2 precisa acessar um bucket S3).
- **Usuários federados** (por exemplo, usuários autenticados através de um provedor de identidade corporativo como Active Directory, Aws Cognito).

IAM Policy *(Políticas)*

Conceito: Documentos JSON que definem exatamente quais ações são permitidas ou negadas em quais recursos.

Analogia: É o "manual de regras" da empresa. Define que o pessoal do financeiro pode acessar a conta bancária, mas não pode deletar dados do servidor, ou que estagiários podem ler documentos, mas não podem modificá-los.

A policy diz **"quem"** (usuário, grupo, role) **pode fazer "o quê"** (ações como **s3:GetObject, ec2:StartInstances**) **em "quais recursos"** (por exemplo, um bucket S3 específico, todas as instâncias EC2 com uma determinada tag).

IAM Policy *(Políticas)*

Na prática:

- Política que **permite leitura e escrita** em um bucket S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AcessoLeituraEscritaBucketEspecifico",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::meu-bucket-da-aplicacao",
                "arn:aws:s3:::meu-bucket-da-aplicacao/*"
            ]
        }
    ]
}
```

IAM Policy *(Políticas)* - *Estrutura básica de uma policy:*

- **Version**: A versão da linguagem da política (geralmente "2012-10-17").
- **Statement**: Contém uma ou mais declarações individuais. Cada declaração inclui:
  - **Sid** (Statement ID): Um identificador opcional para a declaração.
  - **Effect**: Pode ser Allow (permitir) ou Deny (negar). Importante: Um Deny explícito sempre sobrescreve um Allow.
  - **Principal** (em resource-based policies): Especifica o usuário, conta, serviço ou outra entidade que tem permissão ou é negada.
  - **Action**: Lista as ações de serviço permitidas ou negadas (ex: s3:ListBucket, ec2:Describe*). O * atua como um curinga.
  - **Resource**: Lista os recursos aos quais a ação se aplica (ex: arn:aws:s3:::meu-bucket-secreto/*). O ARN (Amazon Resource Name) identifica unicamente os recursos.
  - **Condition** (opcional): Especifica as circunstâncias sob as quais a política concede ou nega permissão (ex: apenas se o acesso for feito de um IP específico, ou durante um certo horário).

IAM Policy *(Políticas)* - *Tipos de políticas*

- **Identity-based policies:** Anexadas a usuários, grupos ou roles. Elas definem o que aquela identidade pode fazer.
- **Resource-based policies:** Anexadas diretamente a recursos (ex: a um bucket S3). Elas definem quem tem permissão para acessar aquele recurso. Um exemplo comum é a **"Bucket Policy" do S3.**

Resumindo...

Característica	Usuário IAM	Grupo IAM	Role IAM	Policy IAM
Quem / O que é?	Pessoa ou aplicação	Coleção de usuários	Identidade temporária assumível	Documento JSON que define permissões
Credenciais?	Longo prazo (senha, chaves de acesso)	N/A	Curto prazo (obtidas ao assumir a role)	N/A (define o que as credenciais podem fazer)
Principal Uso?	Identificar quem está fazendo uma solicitação	Organizar usuários e gerenciar permissões	Delegar acesso, permitir que serviços AWS atuem em seu nome	Especificar permissões (o que pode ser feito, por quem, em quais recursos)
Login direto?	Sim	Não	Não (é assumida por uma entidade já autenticada)	Não

Princípio da Menor Permissão

Sempre conceda apenas as permissões mínimas necessárias.

É melhor começar restritivo e ir liberando conforme necessário.

1. **EXPLICIT DENY** → Nega imediatamente
2. **EXPLICIT ALLOW** → Permite (se não houver DENY)
3. **IMPLICIT DENY** → Nega por padrão

Se qualquer política contém um `"Effect": "Deny"` para a ação solicitada, **a requisição é negada imediatamente**, **independente de quantas outras políticas permitam**.


#01
AMAZON
IAM
IDENTITY AND ACCESS MANAGEMENT
CLOUDCAST
DESCOMPLICANDO CLOUD