Gerenciamento de Identidade e Acessos (IAM)

Termos de Uso

Propriedade Growdev

Todo o conteúdo deste documento é propriedade da Growdev. O mesmo pode ser utilizado livremente para estudo pessoal.

É proibida qualquer utilização desse material que não se enquadre nas condições acima sem o prévio consentimento formal, por escrito, da Growdev. O uso indevido está sujeito às medidas legais cabíveis.

Segurança

O que é IAM (Identity and Access Management)?

IAM (Gerenciamento de Identidade e Acessos) é um conjunto de práticas e tecnologias para gerenciar o acesso a recursos e dados, garantindo que cada usuário tenha permissões adequadas para realizar suas tarefas.

Por que é importante?

- Controla quem pode acessar quais recursos.
- Melhora a segurança limitando o acesso a dados e sistemas sensíveis.

Segurança

Como o IAM Funciona na AWS

Na AWS, o IAM permite criar e gerenciar usuários, grupos e políticas de acesso para controlar quem pode acessar os recursos.

- **Usuários e Grupos**: Criam-se identidades individuais ou em grupo para conceder permissões.
- **Políticas**: Documentos JSON que definem permissões específicas para usuários e grupos.
- **Exemplo**: Configuração de um usuário com permissões restritas para um bucket específico no S3.

Segurança

Como o IAM Funciona no Azure

O Azure usa uma combinação de Azure Active Directory e RBAC (Role-Based Access Control) para gerenciar identidades e acessos.

- **Azure Active Directory**: Gerenciamento de identidades para acessar recursos na nuvem e na rede corporativa.
- **RBAC (Controle de Acesso Baseado em Papéis)**: Define permissões com base em papéis predefinidos para usuários e grupos.
- **Exemplo**: Configuração de papéis para diferentes níveis de acesso a uma conta de armazenamento.

Segurança

Como o IAM Funciona no Google Cloud

O IAM no Google Cloud permite definir papéis e permissões para controlar o acesso a recursos de forma granular.

- **Papéis e Políticas**: Gerenciamento de acessos com base em papéis atribuídos a usuários, grupos e contas de serviço.
- **Contas de Serviço**: Identidades atribuídas a aplicativos e máquinas virtuais para autenticação e acesso seguro.
- **Exemplo**: Configuração de uma conta de serviço para acessar uma instância de Cloud Storage com permissões específicas.

Segurança

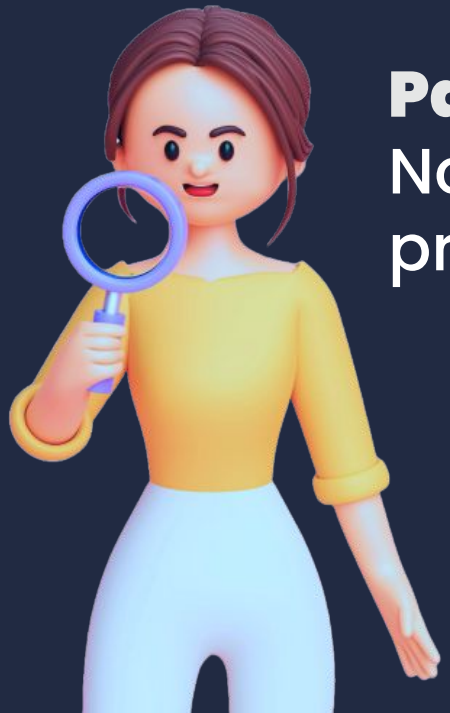
Boas Práticas para Gerenciar Identidades e Permissões

Para garantir uma implementação segura de IAM, siga estas práticas:

- **Princípio do Menor Privilégio**: Conceda apenas as permissões necessárias para cada função.
- **Revisão Regular de Permissões**: Verifique periodicamente quem tem acesso e se as permissões ainda são necessárias.
- **Uso de Autenticação Multifator (MFA)**: Adicione uma camada extra de segurança para acessos críticos.
- **Segregação de Funções**: Separe permissões administrativas e operacionais para reduzir riscos.

Resumo da ópera

- **Conceito de IAM**
  - Controle de acesso a recursos e dados para segurança e conformidade.
- **IAM na AWS**
  - Usuários, grupos e políticas para gerenciar acesso.
- **IAM no Azure**
  - Azure Active Directory e RBAC para controle de acesso com base em papéis.
- **IAM no Google Cloud**
  - Papéis, políticas e contas de serviço para acesso seguro.
- **Boas práticas**
  - Menor privilégio, revisão de permissões, MFA e segregação de funções.



Parabéns!
Nos vemos na próxima etapa!