AWS Identity and Access Management (IAM)

O **AWS Identity and Access Management (IAM)** permite que você gerencie o acesso aos serviços e recursos da AWS com segurança.

O IAM oferece a flexibilidade de configurar o acesso com base nas necessidades operacionais e de segurança específicas da sua empresa. Você pode fazer isso usando uma combinação dos recursos do IAM, que vamos conhecer melhor nesta lição:

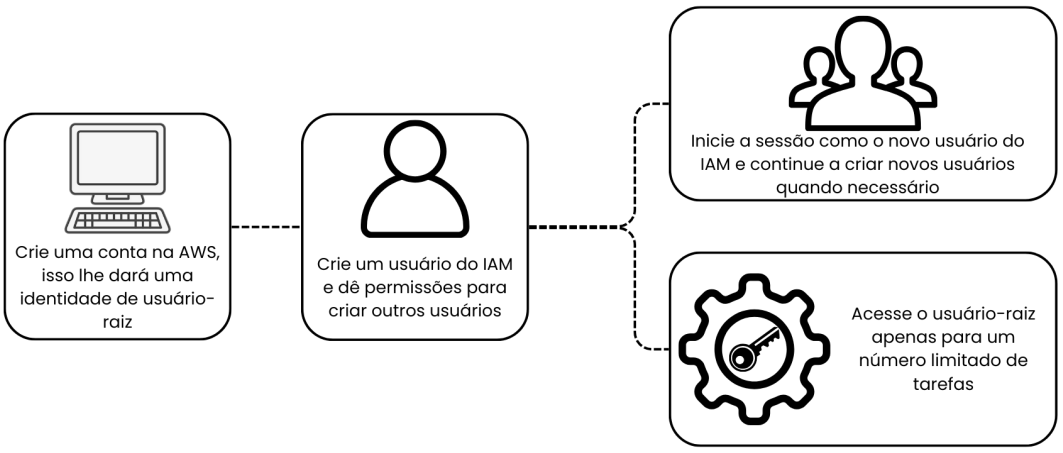
- Usuários, grupos e perfis do IAM
- Políticas do IAM
- Autenticação multifator

Você também conhecerá as práticas recomendadas para cada um desses recursos.

Usuário-raiz da conta AWS

Ao criar uma conta AWS, você inicia com uma identidade chamada usuário-raiz, que é acessada com o endereço de e-mail e a senha usados para criar a conta. O usuário-raiz tem acesso completo a todos os serviços e recursos AWS na conta.

Na gestão de identidade e acesso da AWS (IAM), a prática recomendada é não usar o usuário-raiz para tarefas cotidianas. Em vez disso, crie um usuário IAM com permissões para criar outros usuários. Use o usuário-raiz apenas para tarefas específicas, como alterar o endereço de e-mail do usuário-raiz ou o plano de suporte da AWS.



Usuários do IAM

Um usuário do IAM é uma identidade criada na AWS, que não possui permissões associadas por padrão. Para permitir ações específicas, é necessário conceder as permissões necessárias ao usuário. A prática recomendada é criar usuários individuais do IAM para cada pessoa que precisa acessar a AWS, mesmo que necessitem do mesmo nível de acesso, proporcionando segurança adicional através de um conjunto exclusivo de credenciais de segurança.

Políticas do IAM

As políticas do IAM (AWS Identity and Access Management) permitem personalizar os níveis de acesso dos usuários aos recursos AWS. A prática recomendada é seguir o princípio de segurança de menor privilégio, concedendo apenas as permissões necessárias para executar tarefas, ajudando a prevenir o acesso excessivo.

Exemplo: política do IAM

Veja um exemplo de como as políticas do IAM funcionam. Suponha que o proprietário da cafeteria tenha criado um usuário do IAM para um operador de

caixa recém-contratado. Esse funcionário precisa acessar os recibos mantidos em um bucket do Amazon S3 com o ID: AWSDOC-EXAMPLE-BUCKET.

Esse exemplo de política do IAM concede a permissão para acessar os objetos no bucket do Amazon S3 com o ID: *AWSDOC-EXAMPLE-BUCKET*.

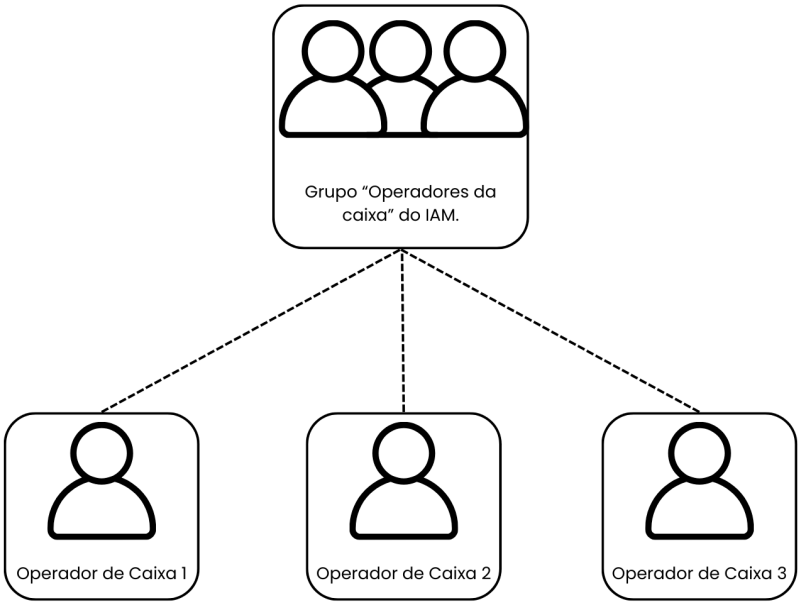
```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "s3:ListObject",
    "Resource": "arn:aws:s3:::AWSDOC-EXAMPLE-BUCKET"
  }
}
```

A política do IAM permite ações específicas, como ListObject no Amazon S3, em um bucket específico. Para permitir que um usuário acesse outros serviços e execute outras ações na AWS, o proprietário deve anexar políticas adicionais. Se houver vários usuários, como operadores de caixa, o proprietário pode colocá-los em um grupo do IAM para gerenciar permissões.

Grupos do IAM

Um grupo do IAM (AWS Identity and Access Management) é um conjunto de usuários do IAM. As políticas do IAM atribuídas a um grupo concedem permissões especificadas a todos os usuários desse grupo, semelhante a como um proprietário de cafeteria pode criar um grupo "operadores de caixa" e atribuir permissões no nível do grupo.

A atribuição de políticas do IAM facilita o ajuste de permissões quando um funcionário muda de função. Se um funcionário revezar em diferentes estações de trabalho, ele pode ter o acesso necessário através dos perfis do IAM.



Perfis do IAM

Os perfis do IAM na AWS funcionam como estações de trabalho em uma cafeteria, onde um funcionário alterna entre diferentes tarefas, abandonando e assumindo acessos conforme necessário. Os perfis do IAM são identidades temporárias com permissões específicas, ideais para situações onde o acesso a serviços ou recursos precisa ser concedido temporariamente.

Fonte: https://explore.skillbuilder.aws/learn (AWS Skill Builder)