IAM e controle de acesso.

1 - IAM Idendity and Access Management

5.1.1) Password Policy

- Podemos definir na conta que os usuários tenham senhas fortes, com letras maiusculas e minusculas, caracteres especiais. Podemos definir que o usuário mude sua senha com um determinado tempo e que não repita a senha.

5.1.2) MFA (Multi factor)

Podemos solicitar que os usuários usem MFA, para ter dupla autentificação.

5.2) Users and Groups

Usuários: são os usuários da sua organização eles podem ser agrupados em grupos ou não ou podem até fazer parte de diversos grupos.

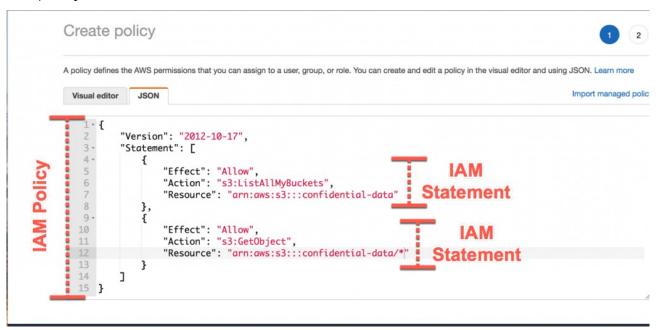


5.3) Policies (Permissions)

As polices são políticas que definem o que cada usuário tem acesso.

É Importante que você leve em conta o least privilege principle. No caso de o acesso mínimo, não de mais permissão que o usuário necessita.

5.3.1) Simples



Sample Policy



IAM Policies are JSON documents used to describe permissions within AWS.

```
"Sid": "Stmt1505076701000",
                                                  Who/what is authorized
"Effect": "Allow",
"Action": [
    "s3:DeleteObject",
                                                  Which task(s) are allowed
   "s3:GetObject"
"Condition": {
    "IpAddress": {
                                                  Which condition(s) need to be met for
        "aws:SourceIP": "10.14.8.0/24"
                                                  authorization
                                                  Resources to which authorized tasks
"Resource": [
    "arn:aws:s3:::billing-marketing",
                                                  are performed
    "arn:aws:s3:::billing-sales"
]
```

5.4) Roles

- Roles são como usuários. Porém, é usado por outros recursos da AWS. Um exemplo é você colocar uma Role em uma EC2 que tenha acesso de escrita a um S3. Então quando o ec2 fizer uma requisição para alterar algo no S3 ele conseguirá.
- Podemos usar assume roles de outras contas para outras contas da AWS.

5.5) IAM security Tool

5.5.1) Credentials reports

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

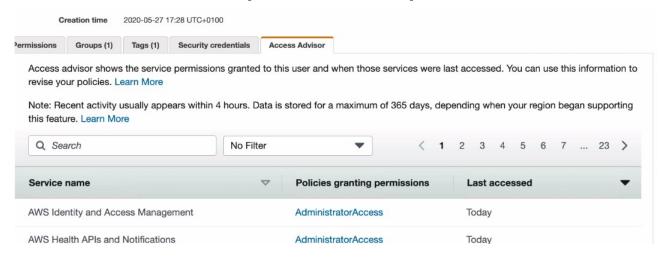
Organization activity

Service control policies (SCPs)

Você pode fazer donload para verificar se o MFA tá ativado do usuário se ele tem rotacionado a senha.

5.5.2) Access Advisor

- Podemos entrar no usuário e ver o que ele tem acessado e o que não tem acessado.

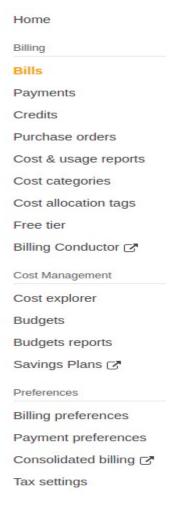


5.6) IAM best pratices

ler depois: https://docs.aws.amazon.com/pt br/IAM/latest/UserGuide/best-practices.html

6) AWS Budget

na categoria Billing da AWS, você consegue ver quais serviços mais estão gastando, a previsão pro final do mês.



Na aba Budgets você também criar alertas para quando sua conta estiver chegando em um valor, você possa ser acionado.

7) aws COSTS