

IAM e controle de acesso.

1 – IAM Identity and Access Management

5.1.1) Password Policy

- Podemos definir na conta que os usuários tenham senhas fortes, com letras maiúsculas e minúsculas, 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 autenticação.

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) Simple

The screenshot shows the 'Create policy' interface in the AWS IAM console. The 'JSON' tab is selected, displaying the following policy document:

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "s3:ListAllMyBuckets",
7       "Resource": "arn:aws:s3:::confidential-data"
8     },
9     {
10      "Effect": "Allow",
11      "Action": "s3:GetObject",
12      "Resource": "arn:aws:s3:::confidential-data/*"
13    }
14  ]
15 }
```


Annotations on the screenshot:

- A vertical red dashed line on the left is labeled **IAM Policy**.
- A red bracket on the right groups the two statements, with labels **IAM Statement** and **IAM Statement**.

At the top right, there are two numbered tabs: 1 and 2. Below the tabs, a link 'Learn more' is visible. At the bottom right, there is a link 'Import managed policy'.

5.3.2) Completa

Sample Policy



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

```
“Sid”: “Stmt1505076701000”,
“Effect”: “Allow”,
“Action”: [
  “s3:DeleteObject”,
  “s3:GetObject”
],
“Condition”: {
  “IpAddress”: {
    “aws:SourceIP”: “10.14.8.0/24”
  }
},
“Resource”: [
  “arn:aws:s3:::billing-marketing”,
  “arn:aws:s3:::billing-sales”
]
```

Who/what is authorized

Which task(s) are allowed

Which condition(s) need to be met for authorization

Resources to which authorized tasks are performed

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 download 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.

Creation time 2020-05-27 17:28 UTC+0100

Permissions Groups (1) Tags (1) Security credentials Access Advisor

Access advisor shows the service permissions granted to this user and when those services were last accessed. You can use this information to revise your policies. [Learn More](#)

Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. [Learn More](#)

Q Search No Filter < 1 2 3 4 5 6 7 ... 23 >

Service name	Policies granting permissions	Last accessed
AWS Identity and Access Management	AdministratorAccess	Today
AWS Health APIs and Notifications	AdministratorAccess	Today

5.6) IAM best practices

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.

- Home
- Billing
- Bills**
- Payments
- Credits
- Purchase orders
- Cost & usage reports
- Cost categories
- Cost allocation tags
- Free tier
- Billing Conductor
- Cost Management
- Cost explorer
- Budgets
- Budgets reports
- Savings Plans
- Preferences
- Billing preferences
- Payment preferences
- Consolidated billing
- Tax settings

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

7) aws COSTS