
amazon
S3

Segurança no Amazon S3

- Por padrão, **todos os recursos** do Amazon S3 — como buckets, objetos e sub-recursos relacionados (por exemplo, configuração de lifecycle e configuração de website) — **são PRIVADOS**. Somente o proprietário do recurso (uma conta da AWS que o criou).

- O Amazon S3 oferece opções de política de acesso do tipo:

    - **Políticas de usuário**

    - **Políticas de recursos**
        - Políticas de buckets
        - Listas de controles de acessos (ACL)

Importante: Recomenda-se que **TODOS** os buckets criados dentro do Amazon S3 sejam do tipo **PRIVADO**, salvo em casos explícitos como a utilização de Websites, onde o conteúdo deve estar público.

Segurança no Amazon S3

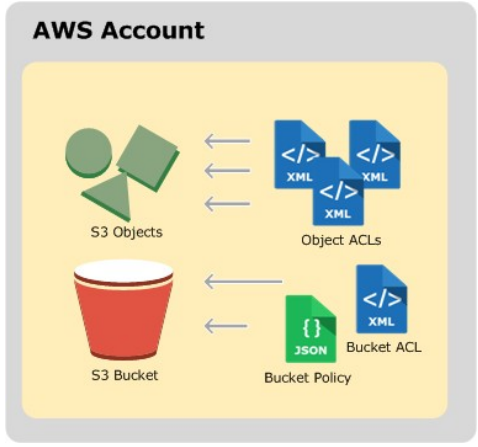
- No Amazon S3, **buckets** e **objetos** são os recursos, onde ambos possuem sub-recursos associados, como:
  - Lifecycle
  - Website
  - Policy e ACL
  - CORS
  - Logging

- Buckets e objetos são recursos do Amazon S3. Por padrão, **apenas o proprietário dos recursos** (conta root) pode acessá-los.

Importante: A AWS recomenda que você **NÃO** use credencias de acesso de usuário raíz da conta da AWS para fazer solicitações de autenticações. Em vez disso, crie u usuário do IAM e conceda acesso total a ele, tornando-os usuários adminitradores.

Políticas de recursos

- As políticas de bucket e listas de controle de acesso (ACLs) usam como base recursos, porque você as anexa aos recursos do Amazon S3.
  - **ACL:** cada bucket e cada objeto têm **uma ACL associada**. Uma ACL é uma **lista de concessões** que identifica o concessionário e a permissão concedida. Você usa ACLs para conceder permissões de leitura/gravação básicas a outras contas da AWS.
  - **Políticas de bucket:** você pode adicionar uma política de bucket para conceder a **outras contas da AWS** ou **usuários do IAM** permissões ao bucket e aos objetos contidos nele. As permissões de objeto **aplicam-se somente aos objetos criados pela proprietário do bucket**. As políticas do bucket suplementam e, em muitos casos, **substituem as políticas de acesso com base em ACL**.



Políticas de recursos

ACL

```xml
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>*** Owner-Canonical-User-ID ***</ID>
    <DisplayName>owner-display-name</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="Canonical User">
        <ID>*** Owner-Canonical-User-ID ***</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

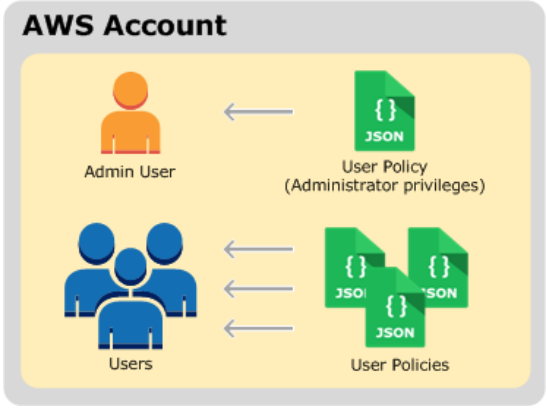
Políticas de bucket

```json
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect":"Allow",
            "Principal": "*",
            "Action":["s3:GetObject"],
            "Resource":["arn:aws:s3:::examplebucket/*"]
        }
    ]
}
```

Políticas de usuários (IAM)

- Você pode usar o IAM para gerenciar o **acesso a recursos do Amazon S3**. Você pode criar usuários, grupos e funções do IAM em sua conta e **anexar políticas de acesso** que concedem acesso a recursos da AWS, incluindo o Amazon S3. ACL.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExampleStatement1",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                 "arn:aws:s3:::examplebucket/*",
                 "arn:aws:s3:::examplebucket"
            ]
        },
        {
            "Sid": "ExampleStatement2",
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "*"
        }
    ]
}
```



Links para consulta

https://docs.aws.amazon.com/pt_br/AmazonS3/latest/dev/s3-access-control.html