

Desafio #3 - Brian Girod

Objetivo:

El objetivo de este ejercicio es aprender a configurar y utilizar roles de AWS IAM desde la línea de comandos (CLI) para permitir la escritura en un bucket de S3.

Escenario:

Eres un administrador de sistemas en una empresa que utiliza AWS para sus servicios en la nube. Te han asignado la tarea de configurar un rol de IAM que permita a los usuarios asumirlo desde la CLI para escribir archivos en un bucket de S3 específico.

Requisitos:

1. Crear un bucket en s3, recuerda asignar un nombre único.
2. Crear un rol con una política que permita escribir en el bucket cerrado en el paso anterior.
3. Generar un usuario IAM llamado s3-support y crear una credenciales programáticas.
4. Actualizar la política del rol para que permita al usuario s3-support asumir el rol.
5. Conecta el CLI con las credenciales del usuario s3-support.
6. Asume el rol de válido que puedas escribir en el bucket.

Documentación utilizada;

<https://docs.localstack.cloud/getting-started/installation/>

https://docs.aws.amazon.com/es_es/cli/latest/userguide/getting-started-install.html

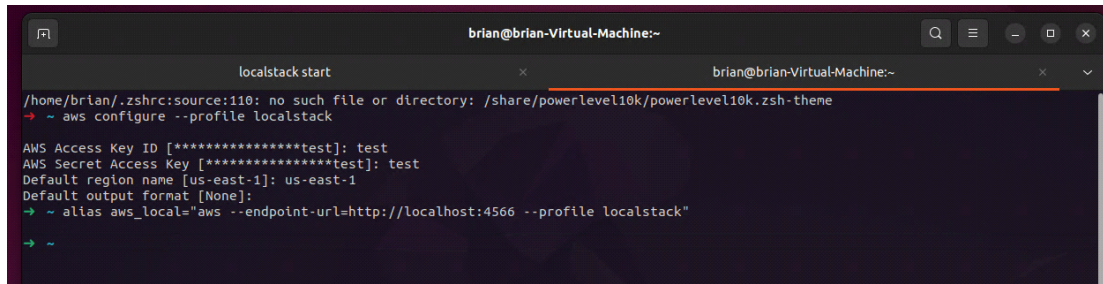
En este desafio utilizo LocalStack para emular AWS

Paso 1: Configuración de AWS CLI para LocalStack

Configuración de AWS CLI para conectar a Localstack con comando;

```
$ aws configure --profile localstack
```

Proporciono para Access Key y Secret Key valores ficticios; test y test, y utilizo la región us-east-1



```
brian@brian-Virtual-Machine:~  
localstack start  
/home/brian/.zshrc:source:110: no such file or directory: /share/powerlevel10k/powerlevel10k.zsh-theme  
→ ~ aws configure --profile localstack  
  
AWS Access Key ID [*****test]: test  
AWS Secret Access Key [*****test]: test  
Default region name [us-east-1]: us-east-1  
Default output format [None]:  
→ ~ alias aws_local="aws --endpoint-url=http://localhost:4566 --profile localstack"  
→ ~
```

(Opcional) genero un alias para facilitar los comandos con localstack;

```
$ alias aws_local="aws --endpoint-url=http://localhost:4566 --profile localstack"
```

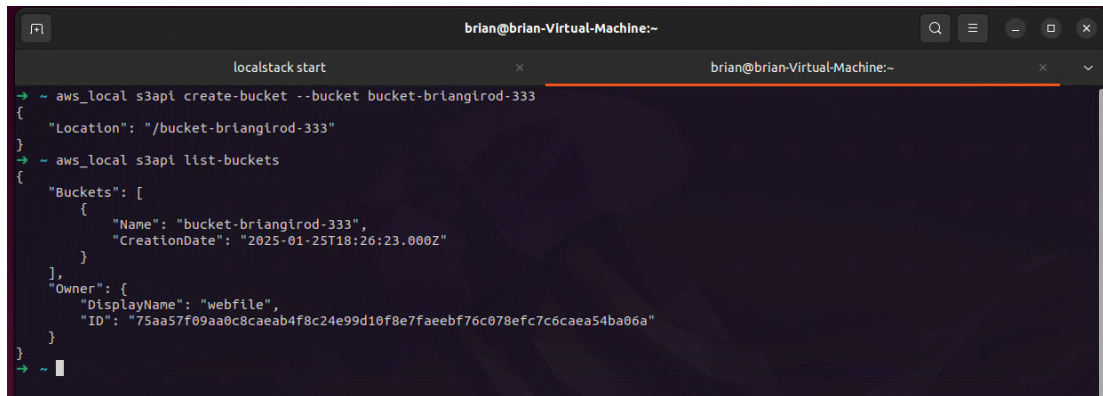
Paso 2: Creación de Bucket en S3

Comando para crear bucket;

```
$ aws_local s3api create-bucket --bucket bucket-briangirod-333
```

Verificar que el bucket se haya creado;

```
$ aws_local s3api list-buckets
```

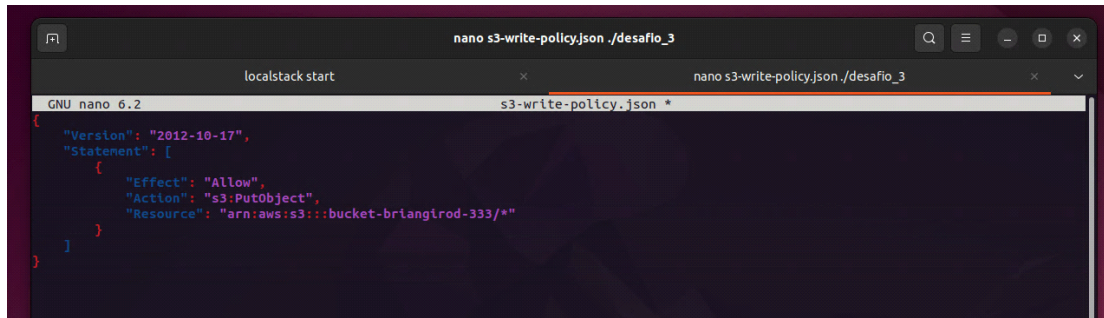


```
brian@brian-Virtual-Machine:~  
localstack start  
→ ~ aws_local s3api create-bucket --bucket bucket-briangirod-333  
{  
  "Location": "/bucket-briangirod-333"  
}  
→ ~ aws_local s3api list-buckets  
{  
  "Buckets": [  
    {  
      "Name": "bucket-briangirod-333",  
      "CreationDate": "2025-01-25T18:26:23.000Z"  
    }  
  ],  
  "Owner": {  
    "DisplayName": "webfile",  
    "ID": "75aa57f09aa0c8caeab4f8c24e99d10f8e7faeef76c078efc7c6caea54ba06a"  
  }  
}  
→ ~
```

Paso 3: Generación de rol con politica de escritura en el bucket

Genero con *"Nano"* el archivo Json con las politicas de escritura;

```
$ nano s3-write-policy.json
```



```
GNU nano 6.2 s3-write-policy.json *
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucket-briangirod-333/*"
    }
  ]
}
```

Creo el rol con el siguiente comando;

```
$ aws_local iam create-role --role-name S3WriteRole --assume-role-policy-document
file://s3-write-policy.json
```

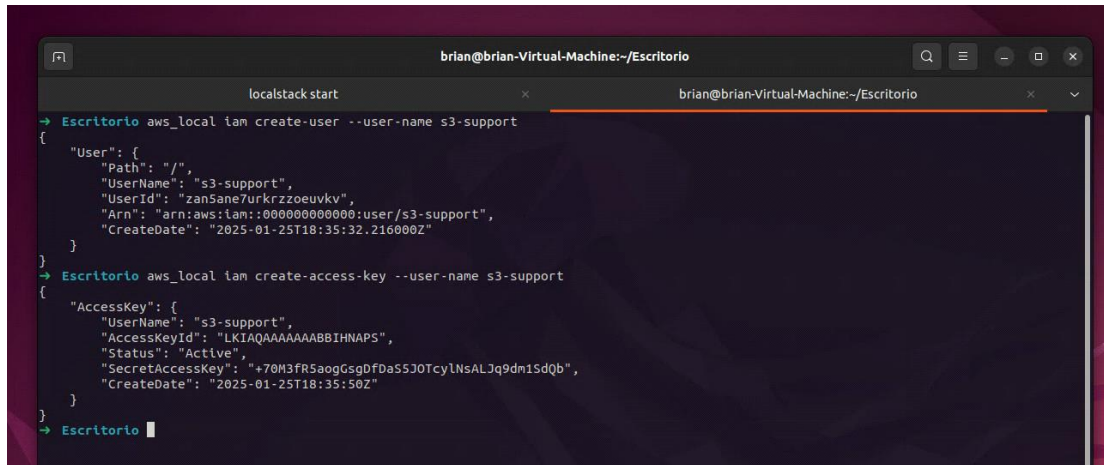
Paso 4: Crear usuario IAM

Comando para crear el usuario:

```
$ aws_local iam create-user --user-name s3-support
```

Generar credenciales programaticas;

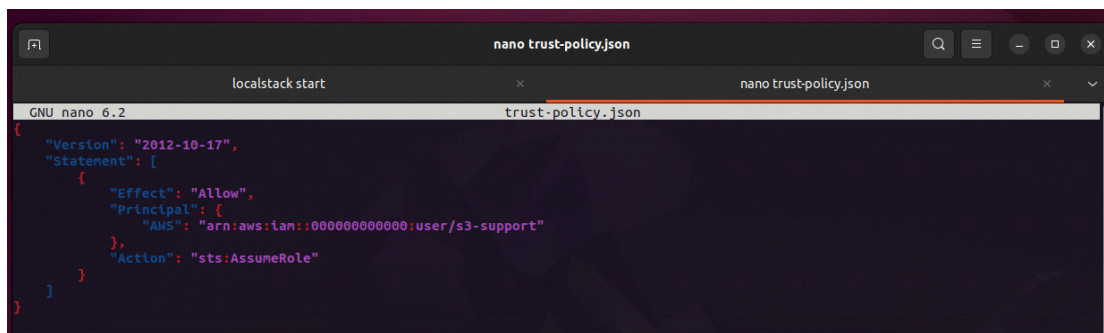
```
$ aws_local iam create-access-key --user-name s3-support
```



```
brian@brian-Virtual-Machine:~/Escritorio
localstack start
→ Escritorio aws_local iam create-user --user-name s3-support
{
  "User": {
    "Path": "/",
    "UserName": "s3-support",
    "UserId": "zanSane7urkrzz0euvkv",
    "Arn": "arn:aws:iam::000000000000:user/s3-support",
    "CreateDate": "2025-01-25T18:35:32.216000Z"
  }
}
→ Escritorio aws_local iam create-access-key --user-name s3-support
{
  "AccessKey": {
    "UserName": "s3-support",
    "AccessKeyId": "LKIAQAAAAAAB8IHNA5",
    "Status": "Active",
    "SecretAccessKey": "+70M3FR5aogGsgDfDaS5J0TcyLNsALJq9dm1SdQb",
    "CreateDate": "2025-01-25T18:35:50Z"
  }
}
→ Escritorio
```

Paso 5: Actualizar politica del rol y conectar al CLI con credenciales de S3-Support

Genero un archivo Json; *"trust-policy.json"* con el comando *"Nano"*



```
nano trust-policy.json
localstack start
GNU nano 6.2 trust-policy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::000000000000:user/s3-support"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Actualizo politicas de rol;

```
$ aws_local iam update-assume-role-policy --role-name S3WriteRole --policy-document file://trust-policy.json
```

Me conecto al CLI con las credenciales ya seteadas de s3-support;

```
$ aws configure --profile s3-support-localstack
```

```
$ user: test / password: test / region: us-east-1
```

```
brian@brian-Virtual-Machine:~/Escritorio
localstack start
→ Escritorio nano trust-policy.json
→ Escritorio aws local iam update-assume-role-policy --role-name S3WriteRole --policy-document file://trust-policy.json
→ Escritorio aws configure --profile s3-support-localstack
AWS Access Key ID [None]: test
AWS Secret Access Key [None]: test
Default region name [None]: us-east-1
Default output format [None]:
→ Escritorio
```

Paso 6: Asumir rol y escribir en Bucket

Asumo el rol con el siguiente comando;

```
$ aws_local sts assume-role --role-arn arn:aws:iam::000000000000:role/S3WriteRole
--role-session-name s3WriteSession
```

```
brian@brian-Virtual-Machine:~/Escritorio
localstack start
→ Escritorio aws_local sts assume-role --role-arn arn:aws:iam::000000000000:role/S3WriteRole --role-session-name s3WriteSession
{
  "Credentials": {
    "AccessKeyId": "LSIAQAAAAAAJGBWIDKQ",
    "SecretAccessKey": "TTTLyXu4FecSZ9FpEU2nS6/1SBOPDgvUTRJvh6vV/",
    "SessionToken": "FQoGZXiVYXZEBYadQDKsRrntpU00gz1XILyXKGUtpNgMB6scYWRBz8FAdWrcAgWLS0ebPo4ai+H0fmMbddt467WLB2KjGwt5FpIN5q0pq/VYIa5Gp0ASi87y+baspgIG03RfscmJTfcWRp0Pb8Q5zQ03CNDPr9a1rnxMlICQlYkY4lB0jzGrFHhgeIEbl6a6KFuIF2z21U560P8hhpIts+7rVvk0sI0X1Tu1pyM2jq+EkDeTY26KadM4ftP7m951wrjuYmkKqEy7Brcru0bnMQGQ37BWJFkxTuu6MSXOam214Vw5SNfk1BQyoLtk1Ban2MAzmzqcALhpvSHV0D1b1Q2v9y2fSFsh4=",
    "Expiration": "2025-01-25T19:38:36.395000Z"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROAQAAAAAALVZLFY7R2:s3WriteSession",
    "Arn": "arn:aws:sts::000000000000:assumed-role/S3WriteRole/s3WriteSession"
  },
  "PackedPolicySize": 6
}
→ Escritorio
```

Genero un archivo .txt y lo subo al bucket;

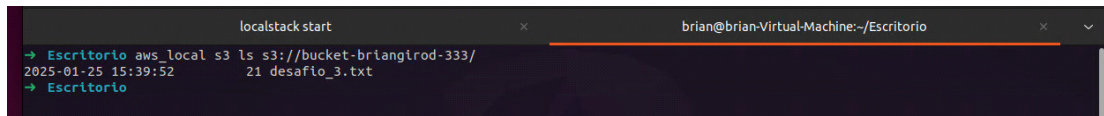
```
$ echo "Este es el desafio 3" > desafio_3.txt
```

```
$ aws_local s3 cp desafio_3.txt s3://bucket-briangirod-333/
```

```
brian@brian-Virtual-Machine:~/Escritorio
localstack start
→ Escritorio echo "Este es el desafio 3" > desafio_3.txt
→ Escritorio aws_local s3 cp desafio_3.txt s3://bucket-briangirod-333/
upload: ./desafio_3.txt to s3://bucket-briangirod-333/desafio_3.txt
→ Escritorio
```

Verifico que los archivos se hayan subido correctamente;

`$ aws_local s3 ls s3://bucket-briangirod-333/`



```
localstack start x brian@brian-Virtual-Machine:~/Escritorio x v
→ Escritorio aws_local s3 ls s3://bucket-briangirod-333/
2025-01-25 15:39:52 21 desafio_3.txt
→ Escritorio
```