

## **Desafío 4 - Bootcamp Devops Engineer**

**Alumno: Ignacio Peretti**

### **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.

### **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 creado 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.

**Requisito número 1 - Crear un bucket en s3, recuerda asignar un nombre único.**

### 1.- Creación del bucket s3

```
ubuntu@devops: ~  
ionConstraint=us-west-2  
  
An error occurred (InvalidAccessKeyId) when calling the CreateBucket operation: The AWS Access Key Id you provided does not exist in our records.  
ubuntu@devops:~$ aws s3api create-bucket --bucket bucket-desafio4 --region us-east-1 --create-bucket-configuration  
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html  
  
usage: aws [options] <command> [<subcommand> ...] [parameters]  
To see help text, you can run:  
  
aws help  
aws <command> help  
aws <command> <subcommand> help  
aws: error: argument --create-bucket-configuration: expected one argument  
ubuntu@devops:~$ aws s3api create-bucket --bucket bucket-desafio4 --region us-east-1  
  
An error occurred (InvalidAccessKeyId) when calling the CreateBucket operation: The AWS Access Key Id you provided does not exist in our records.  
ubuntu@devops:~$ aws configure  
AWS Access Key ID [*****BL3S]: AKIA2UC3DQXX6F3I4UUB  
AWS Secret Access Key [*****WSV1]: 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  
Default region name [None]:  
Default output format [None]:  
ubuntu@devops:~$ aws s3api create-bucket --bucket bucket-desafio4 --region us-east-1  
{  
  "Location": "/bucket-desafio4"  
}
```

**Requisito número 2 - Crear un rol con una política que permita escribir en el bucket cerrado en el paso anterior.**

2.- Se crea un archivo JSON que contenga la política que permitirá escribir en el bucket S3

```
ubuntu@devops: ~  
GNU nano 6.2 s3-write-policy.json  
  
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:PutObject",  
        "s3:PutObjectAcl"  
      ],  
      "Resource": "arn:aws:s3:::bucket-desafio4/*"  
    }  
  ]  
}
```

[ Read 14 lines ]

^G Help    ^O Write Out    ^W Where Is    ^K Cut    ^T Execute    ^C Location    M-U Undo    M-A Set Mark  
^X Exit    ^R Read File    ^\ Replace    ^U Paste    ^J Justify    ^/\_ Go To Line    M-E Redo    M-6 Copy

**Requisito número 3 - Generar un usuario IAM llamado s3-support y crear una credenciales programáticas.**

### 3.- Creación del usuario s3-support

```
}
ubuntu@devops:~$ aws iam create-user --user-name s3-support
{
  "User": {
    "Path": "/",
    "UserName": "s3-support",
    "UserId": "AIDA2UC3DQXXQGM7JYGV7",
    "Arn": "arn:aws:iam::730335512047:user/s3-support",
    "CreateDate": "2024-05-28T00:02:00Z"
  }
}
```

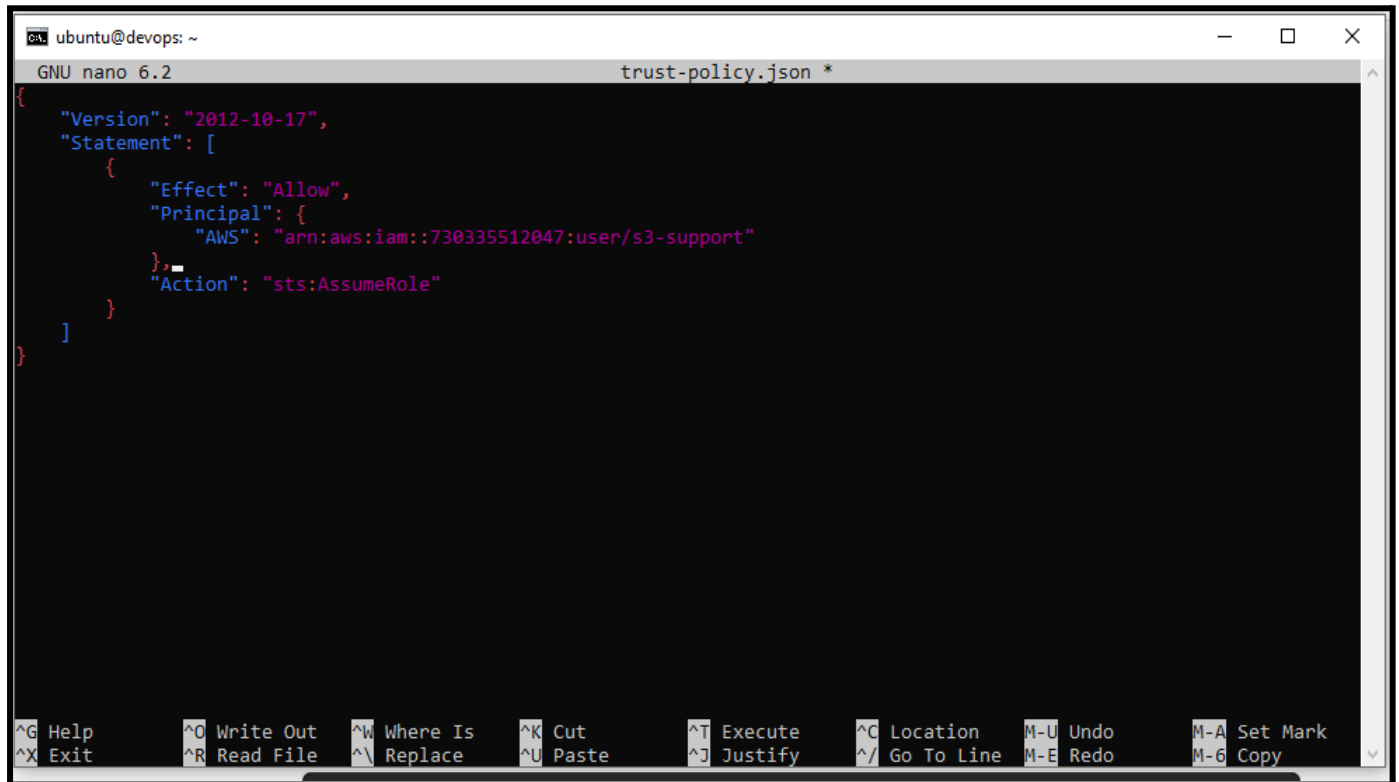
Comando: aws iam attach-user-policy

```
}
ubuntu@devops:~$ aws iam create-access-key --user-name s3-support
{
  "AccessKey": {
    "UserName": "s3-support",
    "AccessKeyId": "AKIA2UC3DQXXXPOGKBGJ",
    "Status": "Active",
    "SecretAccessKey": "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",
    "CreateDate": "2024-05-28T00:03:09Z"
  }
}
```

"AccessKey": {

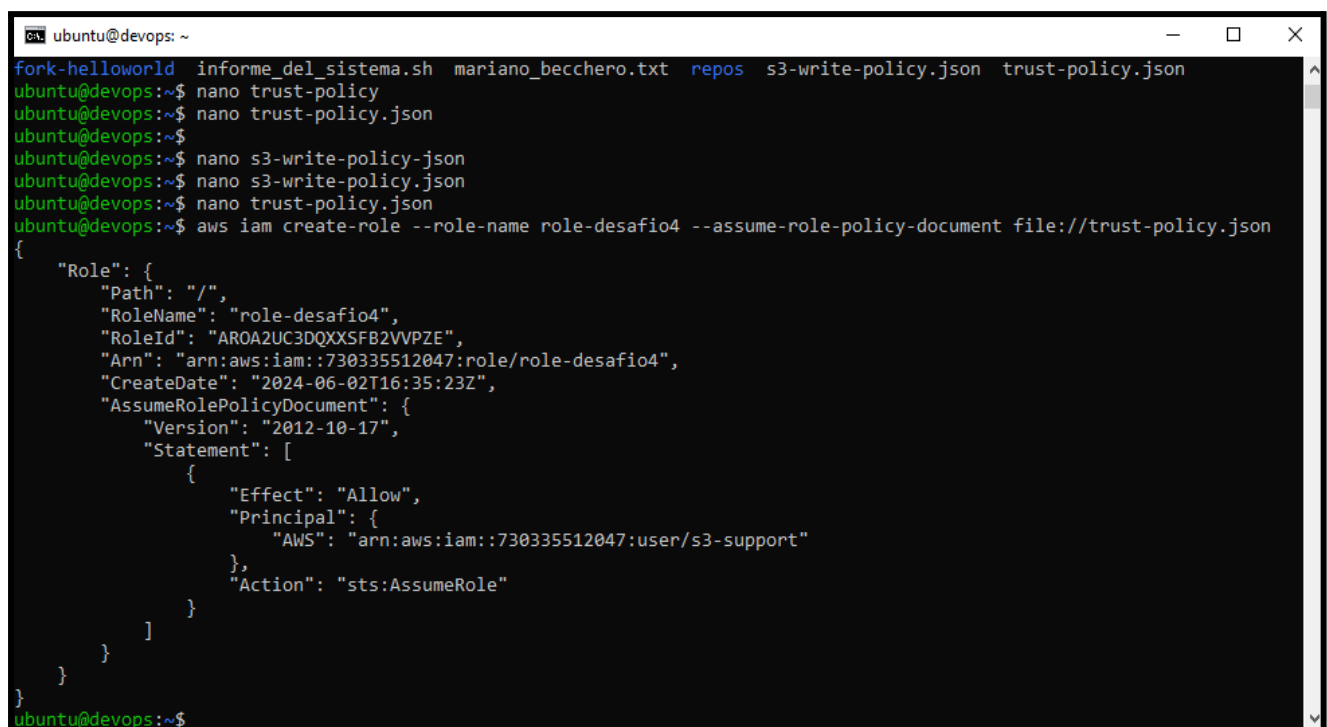
#### ***Requisito número 4 - Actualizar la política del rol para que permita al usuario s3-support asumir el rol.***

4.1.- Se crea un archivo JSON que permitirá a una entidad asumir el rol



```
ubuntu@devops: ~  
GNU nano 6.2 trust-policy.json *  
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::730335512047:user/s3-support"  
      },  
      "Action": "sts:AssumeRole"  
    },  
  ]  
}
```

4.2.- Se crea el rol utilizando la política de confianza



```
ubuntu@devops: ~  
fork-helloworld informe_del_sistema.sh mariano_becchero.txt repos s3-write-policy.json trust-policy.json  
ubuntu@devops:~$ nano trust-policy  
ubuntu@devops:~$ nano trust-policy.json  
ubuntu@devops:~$  
ubuntu@devops:~$ nano s3-write-policy.json  
ubuntu@devops:~$ nano s3-write-policy.json  
ubuntu@devops:~$ nano trust-policy.json  
ubuntu@devops:~$ aws iam create-role --role-name role-desafio4 --assume-role-policy-document file:///trust-policy.json  
{  
  "Role": {  
    "Path": "/",  
    "RoleName": "role-desafio4",  
    "RoleId": "AROA2UC3DQXXSFB2VVPZE",  
    "Arn": "arn:aws:iam::730335512047:role/role-desafio4",  
    "CreateDate": "2024-06-02T16:35:23Z",  
    "AssumeRolePolicyDocument": {  
      "Version": "2012-10-17",  
      "Statement": [  
        {  
          "Effect": "Allow",  
          "Principal": {  
            "AWS": "arn:aws:iam::730335512047:user/s3-support"  
          },  
          "Action": "sts:AssumeRole"  
        },  
      ]  
    }  
  }  
}
```

#### 4.3.- Adjunto la política de S3 al rol

```
ubuntu@devops: ~  
ound.  
ubuntu@devops:~$ aws iam put-role-policy --role-name role-desafio4 policy-name S3WritePolicy --policy-document file://s3-write-policy.json  
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html  
  
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]  
To see help text, you can run:  
  
    aws help  
    aws <command> help  
    aws <command> <subcommand> help  
aws: error: the following arguments are required: --policy-name  
ubuntu@devops:~$ aws iam put-role-policy --role-name role-desafio4 policy-name S3WritePolicy --policy-document file://s3-write-policy.json  
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html  
  
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]  
To see help text, you can run:  
  
    aws help  
    aws <command> help  
    aws <command> <subcommand> help  
aws: error: the following arguments are required: --policy-name  
ubuntu@devops:~$ aws iam put-role-policy --role-name role-desafio4 --policy-name S3WritePolicy --policy-document file://s3-write-policy.json  
ubuntu@devops:~$
```

#### 4.4.- Creo un archivo JSON con la política de asignación del rol al usuario

```
GNU nano 6.2 assume-role-policy.json  
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "sts:AssumeRole",  
      "Resource": "arn:aws:iam::730335512047:role/role-desafio4"  
    }  
  ]  
}
```

[ Wrote 11 lines ]

<b>^G</b> Help	<b>^O</b> Write Out	<b>^W</b> Where Is	<b>^K</b> Cut	<b>^T</b> Execute	<b>^C</b> Location	<b>M-U</b> Undo	<b>M-A</b> Set Mark
<b>^X</b> Exit	<b>^R</b> Read File	<b>^N</b> Replace	<b>^U</b> Paste	<b>^J</b> Justify	<b>^_</b> Go To Line	<b>M-E</b> Redo	<b>M-6</b> Copy

#### 4.5 .- Adjunto la política de asumir el rol al usuario

```
ubuntu@devops: ~  
ubuntu@devops:~$ aws iam put-role-policy --role-name role-desafio4 policy-name S3WritePolicy --policy-document file:///s3-write-policy.json  
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html  
  
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]  
To see help text, you can run:  
  
aws help  
aws <command> help  
aws <command> <subcommand> help  
aws: error: the following arguments are required: --policy-name  
ubuntu@devops:~$ aws iam put-role-policy --role-name role-desafio4 --policy-name S3WritePolicy --policy-document file:///s3-write-policy.json  
ubuntu@devops:~$ ls  
fork-helloworld  informe_del_sistema.sh  mariano_becchero.txt  repos  s3-write-policy.json  trust-policy.json  
ubuntu@devops:~$ nano assume-role-policy.json  
ubuntu@devops:~$ aws iam put-user-policy --user-name nombre-del-usuario --policy-name AssumeRolePolicy --policy-document file:///assume-role-policy.json  
^[[D^[[D  
An error occurred (NoSuchEntity) when calling the PutUserPolicy operation: The user with name nombre-del-usuario cannot be found.  
^[[Dubuntu@devops:~$ aws iam put-user-policy --user-name nombre-del-usuario --policy-name AssumeRolePolicy --policy-document file:///assume-role-policy.json^C  
ubuntu@devops:~$ aws iam put-user-policy --user-name nombre-del-usuario --policy-name AssumeRolePolicy --policy-document file:///assume-role-policy.js^C  
ubuntu@devops:~$ aws iam put-user-policy --user-name s3-support --policy-name AssumeRolePolicy --policy-document file:///assume-role-policy.json  
ubuntu@devops:~$
```

#### Requisito número 5 - Conecta el CLI con las credenciales del usuario s3-support.

5 - Me autentico con las credenciales del usuario s3-support y asumo el rol. También obtengo las credenciales temporales para escribir en el bucket

```
ubuntu@devops: ~  
An error occurred (AccessDenied) when calling the AssumeRole operation: User: arn:aws:iam::730335512047:user/user-desafio4 is not authorized to perform: sts:AssumeRole on resource: arn:aws:iam::123456789012:role/MyS3WriteRole  
ubuntu@devops:~$ aws sts assume-role --role-arn arn:aws:iam::730335512047:role/role-desafio4 --role-session-name S3WriteSession  
An error occurred (AccessDenied) when calling the AssumeRole operation: User: arn:aws:iam::730335512047:user/user-desafio4 is not authorized to perform: sts:AssumeRole on resource: arn:aws:iam::730335512047:role/role-desafio4  
ubuntu@devops:~$ aws configure  
AWS Access Key ID [*****4UUB]: AKIA2UC3DQXXR45MQHP  
AWS Secret Access Key [*****5qpr]: XlWHaPnLXAhLe6fkcRdovwhLLZfcar/dFzCTjrKF  
Default region name [None]:  
Default output format [None]:  
ubuntu@devops:~$ aws sts assume-role --role-arn arn:aws:iam::730335512047:role/role-desafio4 --role-session-name S3WriteSession  
{  
  "Credentials": {  
    "AccessKeyId": "ASIA2UC3DQXXQ3A4RBK4",  
    "SecretAccessKey": "vwh2ufKNa/tc07YQyR17aBXrMPNUVzStRuTRKZQg",  
    "SessionToken": "FwoGZXIvYXZlEDQaDEibh7biirK+J0dD2SKyAfKzaMBwR/cKix51stt0zzJUgou4KD/XeXszn16oRdvd7RZYnrhL1N261Iz8j7fywpgpy+iZcju5k563nND5I0npZ74FwA0t1a9lbpFDuC2j7Qimb23IVXq3+7eiWAMK2v48acxeMutOvQS3yt/pzDSEzKgsOQSDn11Hidtu13qjNvmAJFX7hljy2YuJfH+vpShR5fC+/+qqrJI0jLn9yEbb/tjhco45eesBUGQiUD/Eer1pYosrv9sgYyLcehBZNQQATb/s14bqBJRIxMClw6iJDZbG6i2iFR2+EqjZYmfxm1S0roC1fvw==",  
    "Expiration": "2024-06-04T19:32:18Z"  
  },  
  "AssumedRoleUser": {  
    "AssumedRoleId": "AROA2UC3DQXXQXE4YNFR:S3WriteSession",  
    "Arn": "arn:aws:sts::730335512047:assumed-role/role-desafio4/S3WriteSession"  
  }  
}
```

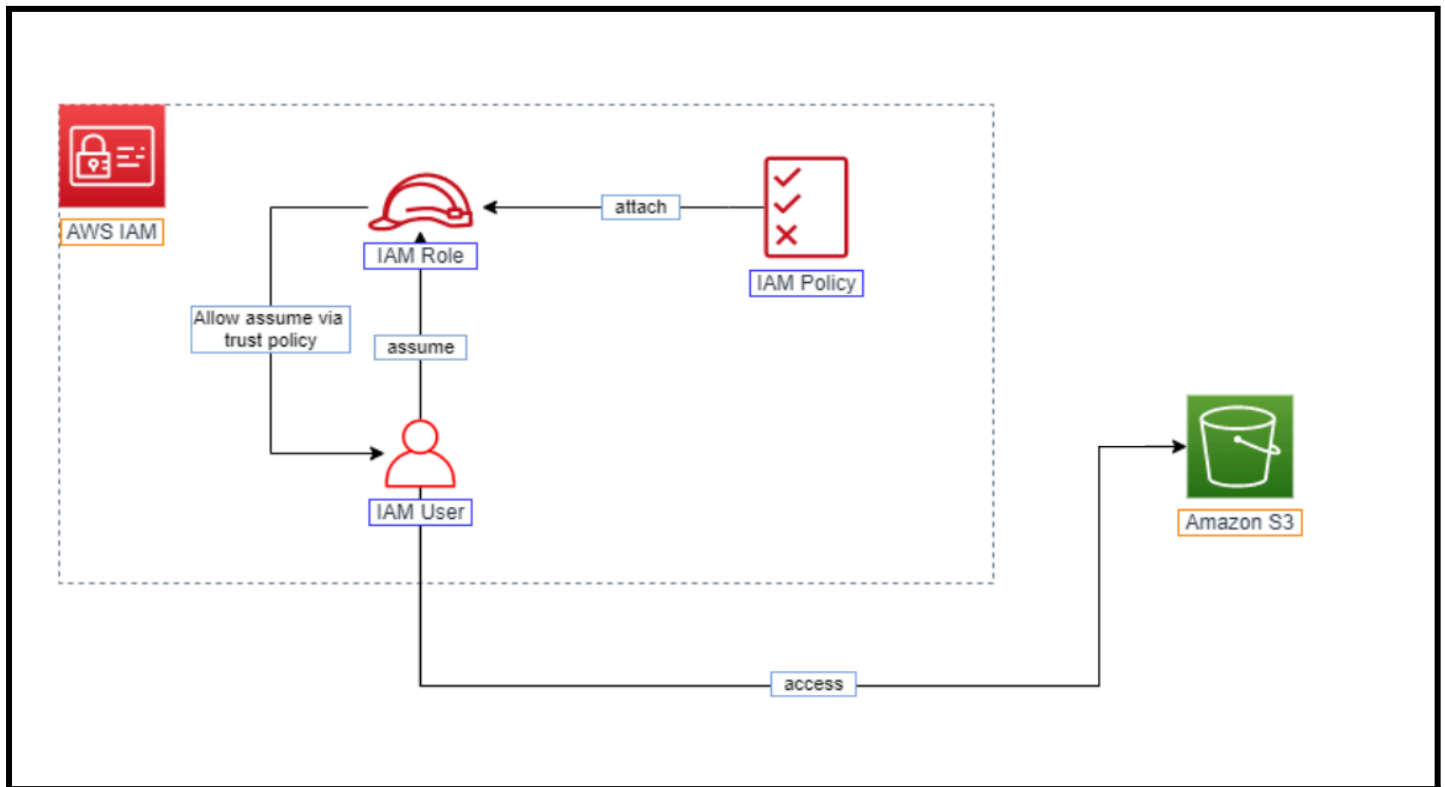
#### Requisito número 6 - Asume el rol de válido que puedas escribir en el bucket.

6.- Me autentico con las credenciales temporales, edito el archivo credentials de aws para agregar el sessionToken y escribo en el bucket

```
ubuntu@devops: ~  
{  
  "Credentials": {  
    "AccessKeyId": "ASIA2UC3DQXXQ3A4RBK4",  
    "SecretAccessKey": "vwh2uFKNa/tc07YQyR17aBXrMPNUVzStRutRKZQg",  
    "SessionToken": "FwoGZXIvYXdzEDQaDEibh7biirK+J0dD2SKyAfKzaMBwR/cKix51sttOzzJUgou4KD/XeXsxn16oRdvd7RZYNrhL1N261Iz  
8j7fywgpy+iZcju5k563nND5I0npZ74FwA0t1a91bPfDuC2j7Qimb23IVXq3+7eiWAMK2v48acxeMut0vQS3yt/pzDSEzKgsOQ5dn11Hidtu13qjNvmAJFX7  
hljy2YuJfh+vpShR5fC+/+qrJI0jLn9yEbb/tjhco45eesBUGQiUD/Eer1pYosrv9sgYyLcehBZNQQATb/s14bq8JRIxMClw6ijDZbGJ6i2iFR2+EqjZYmfX  
m150roC1fvw==",  
    "Expiration": "2024-06-04T19:32:18Z"  
  },  
  "AssumedRoleUser": {  
    "AssumedRoleId": "AROA2UC3DQXXQXE4YNFR:S3WriteSession",  
    "Arn": "arn:aws:sts::730335512047:assumed-role/role-desafio4/S3WriteSession"  
  }  
}  
ubuntu@devops:~$ aws configure  
AWS Access Key ID [*****MQHP]: ASIA2UC3DQXXQ3A4RBK4  
AWS Secret Access Key [*****jrKF]: vwh2uFKNa/tc07YQyR17aBXrMPNUVzStRutRKZQg  
Default region name [None]:  
Default output format [None]:  
ubuntu@devops:~$ cd .aws  
ubuntu@devops:~/.aws$ nano credentials  
ubuntu@devops:~/.aws$ nano credentials  
ubuntu@devops:~/.aws$ cd ..  
ubuntu@devops:~$ aws s3 cp localfile.txt s3://my-example-bucket/remote-file.txt  
  
The user-provided path localfile.txt does not exist.  
ubuntu@devops:~$ aws s3 cp prueba.txt s3://bucket-desafio4/prueba.txt  
upload: ./prueba.txt to s3://bucket-desafio4/prueba.txt  
ubuntu@devops:~$
```

**Fin del documento.**

**DIAGRAMA** - Como trabajan los objetos IAM para asumir el rol.



El **ROL** de IAM es una característica que mejora la seguridad en AWS. Se puede asignar temporalmente una función de IAM a usuarios de IAM y recursos de AWS.

Cuando un usuario de IAM asume una función de IAM, ese usuario de IAM adquiere temporalmente los derechos de esa función de IAM.

Debe utilizar la función de IAM cuando desee proporcionar acceso a corto plazo a un usuario de IAM o a un recurso de AWS.

Para que un usuario de IAM acepte una función de IAM, la propia función de IAM debe permitir que el usuario ejecute una política de confianza.

Una característica importante es que la función IAM no tiene credenciales, por lo que no podrá iniciar sesión en su cuenta de AWS directamente utilizando la función IAM.

#### **Fuentes de información utilizadas.**

##### [IAM Role](#)

[How IAM works - AWS Identity and Access Management](#)

[assume-role — AWS CLI 1.33.0 Command Reference](#)

[Assume role credential provider - AWS SDKs and Tools](#)



