

Crear un bucket S3. El nombre del bucket debe ser único a nivel global. Crear el usuario IAM s3-support. Obtener el ARN del usuario. Guardar el valor. Crear la política de permisos para el rol. Reemplazar el nombre del bucket por el utilizado.

```
aws CloudShell
us-east-1 +
~ $ aws s3api create-bucket --bucket desafio-03 --region us-east-1
{
  "Location": "/desafio-03"
}
~ $ aws iam create-user --user-name s3-support
An error occurred (EntityAlreadyExists) when calling the CreateUser operation: User with name s3-support
~ $ clear
~ $ clear
~ $ aws s3api create-bucket --bucket desafio-03 --region us-east-1
{
  "Location": "/desafio-03"
}
~ $ aws iam create-user --user-name s3-support
{
  "User": {
    "Path": "/",
    "UserName": "s3-support",
    "UserId": "AIDAMXP6DM7SOM3NT4WTE",
    "Arn": "arn:aws:iam::462728423396:user/s3-support",
    "CreateDate": "2025-05-28T21:34:23+00:00"
  }
}
~ $ nano s3-write-policy.json
~ $
```

```
aws CloudShell
us-east-1 +
GNU nano 8.3 s3-write-policy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::desafio-03/*"
    }
  ]
}
```

Crear la política de confianza del rol y Crear el archivo trust-policy.json con el siguiente contenido.

```
aws CloudShell
us-east-1 +
~ $ aws s3api create-bucket --bucket desafio-03 --region us-east-1
{
  "Location": "/desafio-03"
}
~ $ aws iam create-user --user-name s3-support
An error occurred (EntityAlreadyExists) when calling the CreateUser operation: User with name s3-support
~ $ clear
~ $ clear
~ $ aws s3api create-bucket --bucket desafio-03 --region us-east-1
{
  "Location": "/desafio-03"
}
~ $ aws iam create-user --user-name s3-support
{
  "User": {
    "Path": "/",
    "UserName": "s3-support",
    "UserId": "AIDAXPGDH7SON3NT4WTE",
    "Arn": "arn:aws:iam::462728423396:user/s3-support",
    "CreateDate": "2025-05-28T21:34:23+00:00"
  }
}
~ $ nano s3-write-policy.json
~ $ nano trust-policy.json
~ $
```

```
aws CloudShell
us-east-1 +
GNU nano 8.3 trust-policy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::462728423396:user/s3-support"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

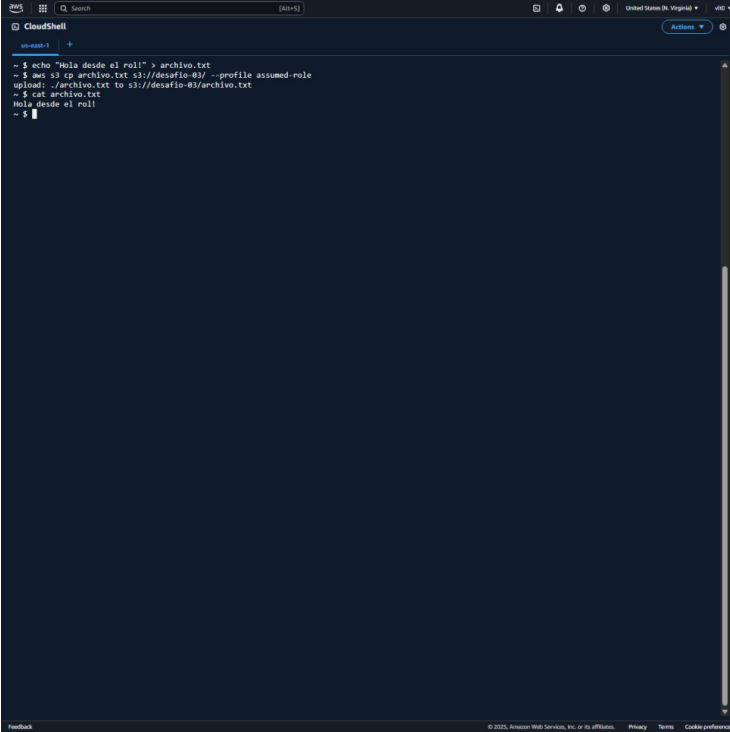
Crear el rol IAM. Asociar la política de permisos al rol. Crear credenciales para el usuario s3-support. Guardar el AccessKeyId y el SecretAccessKey.

```
aws CloudShell
us-east-1 +
~ $ aws iam create-role \
> --role-name S3WriteRole \
> --assume-role-policy-document file://trust-policy.json
{
  "Role": {
    "Path": "/",
    "RoleName": "S3WriteRole",
    "RoleId": "AROAWXPGDM7SPLRKNQN26",
    "Arn": "arn:aws:iam::462728423396:role/S3WriteRole",
    "CreateDate": "2025-05-28T22:17:47+00:00",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::462728423396:user/s3-support"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  }
}
~ $ aws iam put-role-policy \
> --role-name S3WriteRole \
> --policy-name S3WriteAccess \
> --policy-document file://s3-write-policy.json
~ $ aws iam create-access-key --user-name s3-support
{
  "AccessKey": {
    "UserName": "s3-support",
    "AccessKeyId": "AKIAWXP6DM7SHCAZGMCU",
    "Status": "Active",
    "SecretAccessKey": "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",
    "CreateDate": "2025-05-28T22:18:10+00:00"
  }
}
~ $
```

Configurar AWS CLI con el perfil s3support. Completar con los datos. Asumir el rol desde la CLI. Configurar un perfil temporal con las credenciales del rol. Ingresar los valores.

```
aws CloudShell
us-east-1 +
~ $ aws configure --profile s3support
AWS Access Key ID [None]: AKIAWXP6DM7SHCAZGMCU
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
~ $ aws sts assume-role \
> --role-arn arn:aws:iam::462728423396:role/S3WriteRole \
> --role-session-name pruebaSesion \
> --profile s3support
{
  "Credentials": {
    "AccessKeyId": "ASTIAWXP6DM7SCQ5VMV5",
    "SecretAccessKey": "kRQa7hID513y/F1sN3N2m9ahbwVe/H1/OA3HpPj3",
    "SessionToken": "IQoJb3JpZ2luX2VlEj////////wEaCXzLWVhc3QtMSJ1MEYCIQCR0wHmbaChI21ja0ZVPacF61Hs
r3mrnx5W7ZdHRkyKpkCCH8QA80MDVynZi4NDIzMzk2IGx3+X3vTI3yIi3j/XQq9gH2b1SGKQIzRZUePrdLcCqGNTPTdjcc6GZxNwgn
rm508WwQU5IgvZa7X7vh8Vh4z1mFegBkh6J1u0TbWgD7C8U8quuncIEgLEYdvh3XPUq6luVBpx1o1mJV1NUwvI2y//b3VeDd2dnPj/+F
I9qW3InIQ021jcZkCT1TxV+3jIDmc6k0tG8e12VosLEagkzmhUuevVM4t6qvRdtqua93HxoQFqWABmLEu1zrfd8v3owk5jewQY6nAGef0t
zj444wUm52fuEWHIuAw/PsHKFT5mPhnhJwF1jeCBZ8sz+xUnsU8UwZeHgqko0e/Rp6doyRP12M40BRcn/j60FqA42e4xbP13h2V3mJ6
1wE=",
    "Expiration": "2025-05-28T23:20:03+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROAWXPGDM7SPLRKNQN26:pruebaSesion",
    "Arn": "arn:aws:sts::462728423396:assumed-role/S3WriteRole/pruebaSesion"
  }
}
~ $ aws configure --profile assumed-role
AWS Access Key ID [None]: ASTIAWXP6DM7SCQ5VMV5
AWS Secret Access Key [None]: kRQa7hID513y/F1sN3N2m9ahbwVe/H1/OA3HpPj3
Default region name [None]: us-east-1
Default output format [None]: json
~ $
```

11. Subir un archivo a S3 usando el perfil temporal. Crear un archivo de prueba y Subir el archivo:.



```
CloudShell [root@i-0a1e1e1e]
~$ echo "Hola desde el rol" > archivo.txt
~$ aws s3 cp archivo.txt s3://desafio-03/ --profile assumed-role
upload: ./archivo.txt to s3://desafio-03/archivo.txt
~$ cat archivo.txt
Hola desde el rol
~$
```