

Desafío #3

Objetivo: configurar y utilizar roles de AWS IAM desde la línea de comandos (CLI) para permitir la escritura en un bucket de S3.

Prerrequisito: `sudo apt install awscli -y` (instalar awscli en Ubuntu con apt)

```
* appconfig
j0rg3n@j0rg3n-OptiPlex-790:~$ aws configure
AWS Access Key ID [None]: AKIAQ3EGL4DDXI0BT5C
AWS Secret Access Key [None]: SUnX06/dCDZvWfxWRVxggcaqsj9PNSuSLsGgx7b
Default region name [None]: us-east-1
Default output format [None]:
j0rg3n@j0rg3n-OptiPlex-790:~$
```

`aws iam list-users` (solo para verificar que este conectado)

```
netp
j0rg3n@j0rg3n-OptiPlex-790:~$ aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "cloud_user",
      "UserId": "AIDAQ3EGL4DDAG42UMGV",
      "Arn": "arn:aws:iam::058264084230:user/cloud_user",
      "CreateDate": "2024-09-17T20:53:15Z",
      "PasswordLastUsed": "2024-09-17T22:37:53Z"
    }
  ]
}
j0rg3n@j0rg3n-OptiPlex-790:~$
```

1. Crear un bucket en s3, recuerda asignar un nombre único.

`aws s3api create-bucket --bucket devops2024jcavaiuolo`

```
j0rg3n@j0rg3n-OptiPlex-790:~$ aws s3api create-bucket --bucket devops2024jcavaiuolo
{
  "Location": "/devops2024jcavaiuolo"
}
```

`aws s3api list-buckets` >> para listar todos los buckets

```
j0rg3n@j0rg3n-OptiPlex-790:~$ aws s3 ls
2024-09-17 19:44:25 devops2024jcavaiuolo
```

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

desde

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_s3_rw-bucket.html

a. creo la política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PutObject",
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": ["arn:aws:s3:::devops2024jcavaiuolo/*"]
    }
  ]
}
```

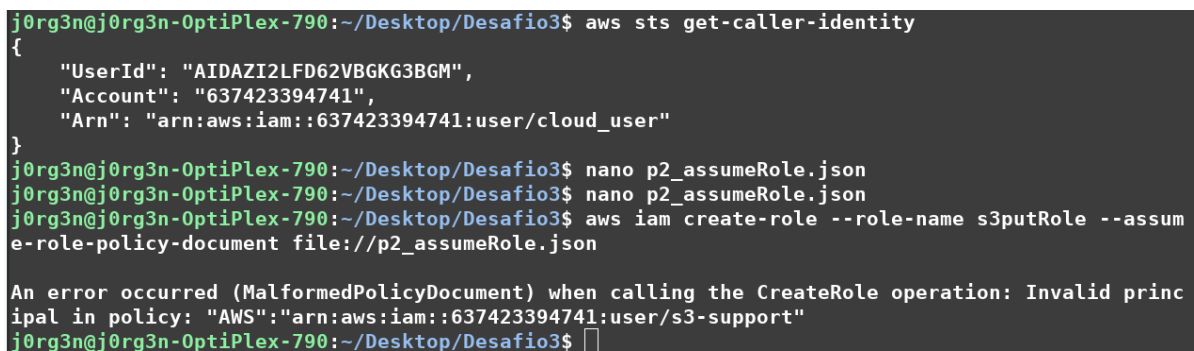
```
aws iam create-policy --policy-name S3WritePolicy --policy-document
file://p2_politica.json
```

```
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ nano p2_politica.json
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws iam create-policy --policy-name S3WritePolicy
--policy-document file://p2_politica.json
{
  "Policy": {
    "PolicyName": "S3WritePolicy",
    "PolicyId": "ANPAZI2LFD62YVG6LDN3K",
    "Arn": "arn:aws:iam::637423394741:policy/S3WritePolicy",
    "Path": "/",
    "DefaultVersionId": "v1",
    "AttachmentCount": 0,
    "PermissionsBoundaryUsageCount": 0,
    "IsAttachable": true,
    "CreateDate": "2024-09-18T22:43:07Z",
    "UpdateDate": "2024-09-18T22:43:07Z"
  }
}
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ cat p2
cat: p2: No such file or directory
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ cat p2_politica.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PutObject",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": ["arn:aws:s3:::devops2024jcavaiuolo/*"]
    }
  ]
}
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$
```

Crear el rol.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::637423394741:user/s3-support"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Creo el role con: `aws iam create-role --role-name s3putRole --assume-role-policy-document file://p2_assumeRole.json`



```
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws sts get-caller-identity
{
  "UserId": "AIDAZI2LFD62VBGKG3BGM",
  "Account": "637423394741",
  "Arn": "arn:aws:iam::637423394741:user/cloud_user"
}
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ nano p2_assumeRole.json
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ nano p2_assumeRole.json
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws iam create-role --role-name s3putRole --assume-role-policy-document file://p2_assumeRole.json

An error occurred (MalformedPolicyDocument) when calling the CreateRole operation: Invalid principal in policy: "AWS": "arn:aws:iam::637423394741:user/s3-support"
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$
```

Nota: acá estuve trabado un rato, primero tuve que ver como obtener el número de cuenta (`aws sts get-caller-identity`) y luego tenía un error muy raro. Después de investigar un rato concluí que el tema podía venir por el lado de que no existía el usuario.

Nota: esto está mal. Para ver la solución real [enlace](#)

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

```
aws iam create-user --user-name s3-support
aws iam create-access-key --user-name s3-support
```

```
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws iam create-user --user-name s3-support
{
  "User": {
    "Path": "/",
    "UserName": "s3-support",
    "UserId": "AIDAQ3EGPL4DDFJLFSV3H",
    "Arn": "arn:aws:iam::058264084230:user/s3-support",
    "CreateDate": "2024-09-17T23:21:50Z"
  }
}
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws iam create-access-key --user-name s3-support
{
  "AccessKey": {
    "UserName": "s3-support",
    "AccessKeyId": "AKIAQ3EGPL4DPBI5CXMH",
    "Status": "Active",
    "SecretAccessKey": "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",
    "CreateDate": "2024-09-17T23:23:00Z"
  }
}
```

Nota: con el usuario ya creado puede completar el punto 3

```
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws iam create-role --role-name s3putRole --assume-
role-policy-document file://p2_assumeRole.json
{
  "Role": {
    "Path": "/",
    "RoleName": "s3putRole",
    "RoleId": "AROAZI2LFD62RPBBUI5EJ",
    "Arn": "arn:aws:iam::637423394741:role/s3putRole",
    "CreateDate": "2024-09-18T22:54:06Z",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::637423394741:user/s3-support"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  }
}
```

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

Actualizo el usuario para asignarle la política s3WritePolicy

```
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws iam put-user-policy --user-name s3-support --
policy-name S3WritePolicy
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
aws: error: the following arguments are required: --policy-document
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws iam put-user-policy --user-name s3-support --
policy-name S3WritePolicy --policy-document file://p2_politica.json
```

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

```
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ cat s3-creds.txt
{
  "AccessKey": {
    "UserName": "s3-support",
    "AccessKeyId": "AKIAQ3EGPL4DPBI5CXMH",
    "Status": "Active",
    "SecretAccessKey": "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",
    "CreateDate": "2024-09-17T23:23:00Z"
  }
}
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws configure
AWS Access Key ID [*****BT5C]: AKIAQ3EGPL4DPBI5CXMH
AWS Secret Access Key [*****xC7b]: 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
Default region name [us-east-1]:
Default output format [None]:
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws sts assume-role S3WriteRole
```

6. Asume el rol de válido que puedas escribir en el bucket.

Asumo el rol: `aws sts assume-role --role-arn arn:aws:iam::637423394741:role/s3putRole --role-session-name S3WriteSession`

Copio un elemento al bucket para validar: `aws s3 cp identity.txt s3://devops2024jcavaiuolo`

```
usage: aws [options] <command> [<subcommand> ...] [parameters]
aws: error: the following arguments are required: --role-session-name
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws sts assume-role --role-arn arn:aws:iam::637423394741:role/s3putRole --role-session-name S3WriteSession
{
  "Credentials": {
    "AccessKeyId": "ASTAZI2LFD62YF5K7VW",
    "SecretAccessKey": "FfAT3L8dpv8/jVT/p55YnrMm67aGNCPrpknVbIL",
    "SessionToken": "Fw6GZlVYXdzEckaDhvx8TilSvBN2QBCKyATUqJ0NUHL1IC0B05M+L7pHDXPHW1LyrDGVXUAQKFF66pcHuJIGBYGmp41G7LI26xakU20oG4ii9K4+S0/6wa0sv3msqRm1UuUmBFhwczBmKYPQsk33QLr54f0/sISrws8KnB0LY119HSH9L1NrsYF80G2pu6qsUCbnU0EC1RFR+7YYU1ams1v8w4IXr+Y0UdrP0a8Gw9Bm02e-JVE2Ux1VtmFUX8o7E8hhsfmgko/00twYylsyzwqR218iffhAip1rSAVB8FT9+DWG1s3Hxud0w85zo2QALFRqLFPLmrZcQ==",
    "Expiration": "2024-09-19T08:27:59Z"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROAZI2LFD62RPPBU15E3:S3WriteSession",
    "Arn": "arn:aws:sts::637423394741:assumed-role/s3putRole/S3WriteSession"
  }
}
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ ll
total 68
drwxr-xr-x 2 j0rg3n j0rg3n 4096 Sep 18 19:53 ./
drwxr-xr-x 7 j0rg3n j0rg3n 4096 Sep 17 19:28 ../
-rw-rw-r-- 1 j0rg3n j0rg3n 44521 Sep 17 19:28 'AWS Uso de roles.pdf'
-rw-rw-r-- 1 j0rg3n j0rg3n 129 Sep 18 19:44 identity.txt
-rw-rw-r-- 1 j0rg3n j0rg3n 211 Sep 18 19:46 p2_assumeRole.json
-rw-rw-r-- 1 j0rg3n j0rg3n 214 Sep 18 19:42 p2_politica.json
-rw-rw-r-- 1 j0rg3n j0rg3n 254 Sep 18 19:48 p3-support-creds.txt
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws s3 cp identity.txt s3://devops2024jcavaiuolo
upload: ./identity.txt to s3://devops2024jcavaiuolo/identity.txt
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws s3 cp identity.txt s3://devops2024jcavaiuolo/
upload: ./identity.txt to s3://devops2024jcavaiuolo/identity.txt
```

Amazon S3

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3

> Buckets

> devops2024jcavaiuolo

devops2024jcavaiuolo info

< Objects Properties Permissions Metrics Management Accel >

Objects (1) info

Copy S3 URI Copy URL Download Open

Delete Actions Create folder Upload

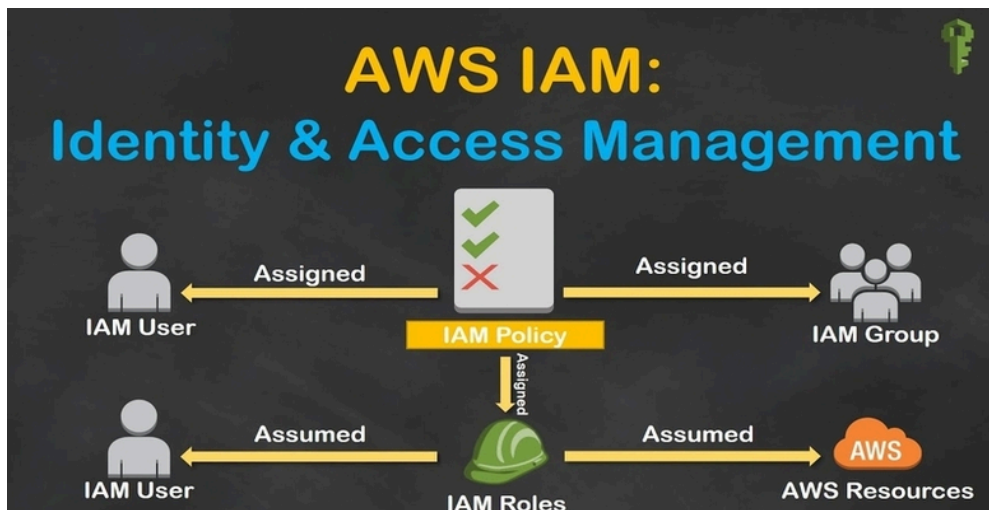
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	identity.txt	txt	September 18, 2024, 20:29:17 (UTC-03:00)	128.0 B	Standard

Llegado este punto me encontré con lo siguiente:

Revisando la relación entre users, roles y políticas, si bien funcionó, algo está mal.



Relación entre los tres:

- **Usuarios** pueden tener políticas directamente asociadas a ellos, que les permiten realizar ciertas acciones sobre los recursos.
- **Los roles** también tienen políticas asociadas, pero un rol no tiene un usuario específico: puede ser asumido temporalmente por varios usuarios o servicios. Las políticas de **confianza** controlan quién puede asumir el rol.
- **Políticas** controlan qué pueden hacer los usuarios o roles con los recursos de AWS.

Problema: Al menos como yo lo armé, el resultado final es que s3putRole no tiene una política asignada y me di cuenta que en el paso 4 le asigne la política directamente al usuario.

s3putRole

Summary

Creation date: September 18, 2024, 19:54 (UTC-03:00)

ARN: `arn:aws:iam::637423394741:role/s3putRole`

Link to switch roles in console: <https://signin.aws.amazon.com/switchrole?roleName=s3putRole&account=637423394741>

Maximum session duration: 1 hour

Permissions policies (0)

No resources to display

s3-support

Summary

ARN: `arn:aws:iam::637423394741:user/s3-support`

Console access: Disabled

Access key 1: AKIAZI2LFD626HU3ZD2U - Active
Used today. Created today.

Created: September 18, 2024, 19:48 (UTC-03:00)

Access key 2: [Create access key](#)

Permissions policies (1)

Policy name	Type	Attached via
S3WritePolicy	Customer inline	Inline

Por lo cual, no funcionó por haber asumido el rol correctamente, sino porque el usuario tenía una política asignada que le permite subir archivos en cualquier momento.

Solución 2:

1. eliminar la politica del usuario

```
aws iam detach-user-policy --user-name s3-support --policy-arn  
arn:aws:iam::637423394741:policy/S3WritePolicy
```

2. attachar la politica al rol

```
aws iam attach-role-policy --role-name s3putRole --policy-arn  
arn:aws:iam::637423394741:policy/S3WritePolicy
```

3. asumo el rol:

```
aws sts assume-role --role-arn  
arn:aws:iam::637423394741:role/s3putRole --role-session-name  
S3WriteSession
```

```
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws sts assume-role --role-arn arn:aws:iam::637423394741:role/s3putRole --role-session-name testSession  
{  
  "Credentials": {  
    "AccessKeyId": "ASIAZI2LFD622KLIVW7C",  
    "SecretAccessKey": "lTgRohs/E0A7xPhLeTpdH2YpHRIHzhGp6XXcYLLB",  
    "SessionToken": "FwoGZXIvYXZlCoaDiVldGbFlKoUsDosSKvAYLr3yovmy93n0J+hRRnWqrqNV6dR+3+/I0D/7AKy7MwAqhScDHAVZaCre/WidKwmLa5BmcFV3w6Bo/vHrW5t6/RU8b6jkgPeqPXem1hjSDUguv9PAaZ1dr6yfTDwMuItpxSmLqiZ5ROZD0vxEjhTJK5PEiywvZ007Vu67/6dffYKjY3RSJhhixi+hQDSSZ0A2zWKyWFXuy2VmWszuy7foU3qeFiC2We0NRtgSljB48oq9ittwYyLVP2qmge1GG+9ai5audSateMRtCd/pA0wvblvlCpQqq2NkkdpxG583qagbXtZW==",  
    "Expiration": "2024-09-19T01:11:23Z"  
  },  
  "AssumedRoleUser": {  
    "AssumedRoleId": "AR0AZI2LFD62RPBBUI5EJ:testSession",  
    "Arn": "arn:aws:sts::637423394741:assumed-role/s3putRole/testSession"  
  }  
}
```

4. exporto las credenciales temporales

```
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ export AWS_ACCESS_KEY_ID=ASIAZI2LFD62QZEYK67Q  
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ export AWS_SECRET_ACCESS_KEY=yEHFeCNyI0TYZkBfm6vfVVq4SME2wvdhqIRktYab  
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ export AWS_SESSION_TOKEN=FwoGZXIvYXZlCoaDB/0Q+YzS8JynT8vTSKvAcfmset4ngHEant0ISCtmsgKzmHDFZ+5wg+gbMj/e6HJzvDZzMDr1jEzXr+DrM3w+TsZd8Y/7k4IXBixi+2W3sRHaq/q/u2DePvo3lopenlB5R4hWST10UC1fvjPMtVS9QFmTY5RT4V004DJx46g60ScSkb4BK/U5s9X95qNlKocorNR/yCmub2/VB52f/V05A0SUG6v/Kb6VIw+7V27YQRkBMlym0ykh3QLVr+2WYo19ettwYyLfztTtDtqHMgq79rpU9b0tF/LpLrTKUkAoUxCvcBaPwZKdE0d51dkTNWIwnxg==
```

5. Y ahora si intento subir un archivo, con las credenciales generadas a raíz de asumir el rol s3putRole:

```
aws s3 cp p2_politica.json s3://devops2024jcavaiuolo/
```

```
W3sRHaq/q/u2DePvo3lopenlB5R4hWST10UC1fvjPMtVS9QFmTY5RT4V004DJx46g60ScSkb4BK/U5s9X95qNlKocorNR/yCmub2/VB52f/V05A0SUG6v/Kb6VIw+7V27YQRkBMlym0ykh3QLVr+2WYo19ettwYyLfztTtDtqHMgq79rpU9b0tF/LpLrTKUkAoUxCvcBaPwZKdE0d51dkTNWIwnxg==  
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$ aws s3 cp p2_politica.json s3://devops2024jcavaiuolo/  
upload: ./p2_politica.json to s3://devops2024jcavaiuolo/p2_politica.json  
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$  
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$  
j0rg3n@j0rg3n-OptiPlex-790:~/Desktop/Desafio3$
```

Feature spotlight				
AWS Marketplace for S3				
<input type="checkbox"/>	 Identity.txt	txt	September 18, 2024, 20:28:17 (UTC-03:00)	129.0 B Standard
<input type="checkbox"/>	 p2_politica.json	json	September 18, 2024, 21:12:08 (UTC-03:00)	214.0 B Standard

