

Desafío numero 4 Educacionit (devOps)

Hernán Andrés Acosta-993394

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.

Configuración CLI:

Una buena practica para encarar cualquier desafío seria realizar un esquema con los pasos a seguir para cumplir con el objetivo a realizar:

Orden de creación de objetos

- 1.Crear un usuario IAM.
- 2.Crear un role de IAM.
- 3.Attachar la política al role.
- 4.Crear una política inline sobre el usuario para permitir el uso del role.

Configuración de AWS CLI.

```
Aws configure --profile <nombre_del_perfil_usuario>
```

Asumir el rol con las credenciales del usuario.

```
Aws --profile <nombre_del_perfil_usuario> sts assume-role \  
--role-arn arn:aws:iam::<cta>:role/<role_name> \  
--role-session-name s3OperatorRole-session
```

configurar las credenciales del rol en el CLI

```
Aws configure --profile <nombre_del_perfil_role>
```

Verificar la configuración del CLI

```
Aws sts get-caller-identity --profile <nombre_del_perfil_role>
```

Listar los buckets de S3

```
Aws s3 ls --profile <nombre_del_perfil_role>
```

Esquema orientativo para encarar el desafío:



En primer lugar como indica nuestro diagrama vamos a crear un usuario con el el nombre de **s3-support**

User details

User name
s3-support

Console password type
None

Require password reset
No

Permissions summary < 1 >

Name ⓘ ▲

Type ▼

Used as ▼

No resources

Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

Key

owner

×

Use "educaloniit"

educaloniit

×

Remove

Users (2) Info

Delete

Create user

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Q

Search

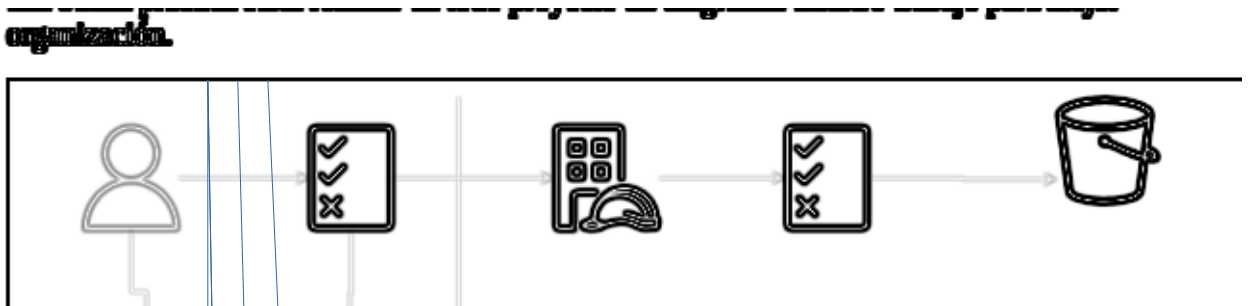
<

1

>

<input type="checkbox"/>	User name	Path	Group	Last activity	MFA	Password age
<input type="checkbox"/>	herman-admin	/	1	8 minutes ago	Virtual	1 hour
<input type="checkbox"/>	s3-support	/	0	-	-	-

como se puede observar solamente se creo el usuario por el momento no tiene relación con los demás componentes: como ser roles políticas ni servicios.



En el siguiente paso se procede a crear el rol:

Una de las ventajas que nos ofrece el rol es que podemos acceder a otra cuentas de aws, nos da opción de un identificador y de que nos solicite el MFA

AWS service

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

An AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

This account (207567791252)

Another AWS account

Options

seguidamente se procede a definir los permisos ya sea los creados por Amazon o creados por nosotros mismos, en este caso elegimos uno creado por Amazon.

Permissions


Trust relationships

Tags (1)

Last Accessed

Revoke sessions


Permissions policies (2) [Info](#)



 [Simulate](#) [Remove](#) [Add permissions](#)

You can attach up to 10 managed policies.

Filter by Type

All types

< 1 > 

<input type="checkbox"/>	Policy name ?	Type	Attached entities
<input type="checkbox"/>	 AmazonS3OutpostsReadO...	AWS managed	1
<input type="checkbox"/>	 AmazonS3ReadOnlyAccess	AWS managed	1

Permissions boundary (not set)

Role details

Role name

Enter a meaningful name to identify this role.

s3OperatorRole

Maximum 64 characters. Use alphanumeric and '+=, @-/_[]!#\$%^&*()~*' characters.

Description

Add a short explanation for this role.

Demo creacion de rol IAM

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, @-/_[]!#\$%^&*()~*'.

Step 1: Select trusted entities

Trust policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Principal": {
8         "AWS": "207567791252"
9       },
10      "Condition": {}
11    }
12  ]
13 }
```

con esto creamos el rol y esta conectado con la política



hasta este instante le usuario no tiene conexión con el rol, ni con el servicio



*El siguiente paso que vamos a realizar es conectar el usuario con el rol: -seleccionamos el usuario
-creamos una política inline para asumir un rol
seleccionamos STS

de policy

Policy editor Visualizar

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Action": [
8         "sts:AssumeRole"
9       ],
10      "Resource": ["arn:aws:iam::207567791252:role/s3operatorRole"]
11    }
12  ]
13 }
```

en este paso el usuario puede asumir el rol donde se copio la arn de rol para asignarlo a la política

Policy details

Policy name

Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+,=,@-_' characters.

ahora nuestro usuario s3Operator puede asumir el rol

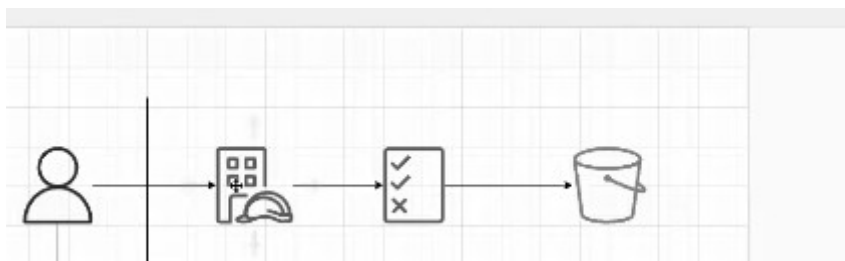
<input type="checkbox"/>	Policy name ?	Type	Attached via ?
<input type="checkbox"/>	s3OperatorAssumerol	Customer inline	Inline

s3OperatorAssumerol

[Copy JSON](#)

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Action": [
8         "sts:AssumeRole"
9       ],
10      "Resource": [
11        "arn:aws:iam::207567791252:role/s3operatorRole"
12      ]
13    }
14  ]
15 }
```

con esto logramos que a través de la política inline el usuario ` pueda asumir el rol



como este usuario no tiene acceso por consola debemos crear el access key 42:13 46:40

Access key best practices & alternatives [Info](#)

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

☒ Command Line Interface (CLI)

You plan to use this access key to enable the AWS CLI to access your AWS account.

comandos utiles para continuar con el dasafio

*****Asumir el rol con las credenciales del usuario.*****

```
Aws -profile <nombre_del_perfil_usuario> sts assume-role \  
--role-arn arn:aws:iam::<cta>:role/<role_name> \  
--role-session-name s3OperatorRole-session
```

*****configurar las credenciales del rol en el CLI*****

```
Aws configure -profile <nombre_del_perfil_role>
```

*****Verificar la configuracion del CLI*****

```
Aws sts get-caller-identity -profile <nombre_del_perfil_role>
```

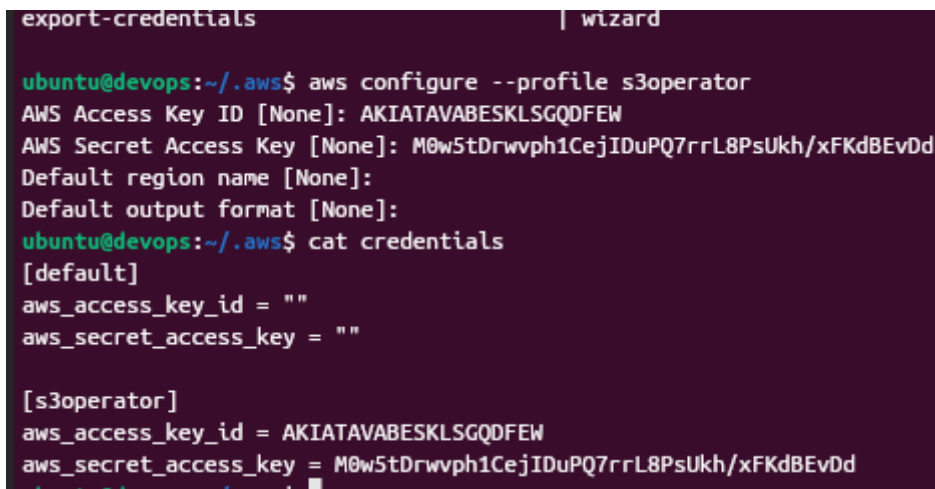
*****Listar los buckets de S3*****

```
Aws -profile <nombre_del_perfil_role> s3 ls
```

seguidamente procedemos a crear un nuevo perfil en AWS CLI : llamado

s3operator

--creamos un nuevo perfil en la consola



```
export-credentials | wizard  
  
ubuntu@devops:~/aws$ aws configure --profile s3operator  
AWS Access Key ID [None]: AKIATAVABESKLSGQDFEW  
AWS Secret Access Key [None]: M0w5tDrwvph1CejiDuPQ7rrL8PsUkh/xFKdBvDd  
Default region name [None]:  
Default output format [None]:  
ubuntu@devops:~/aws$ cat credentials  
[default]  
aws_access_key_id = ""  
aws_secret_access_key = ""  
  
[s3operator]  
aws_access_key_id = AKIATAVABESKLSGQDFEW  
aws_secret_access_key = M0w5tDrwvph1CejiDuPQ7rrL8PsUkh/xFKdBvDd
```

ejecutamos el comando para lista los s3 y nos indica que no tiene permisos para dicha acción

```
ubuntu@devops:~/aws$ aws -profile s3operator s3 ls
```

An error occurred (AccessDenied) when calling the ListBuckets operation: User:

arn:aws:iam::207567791252:user/s3-support is not authorized to perform: s3:ListAllMyBuckets

because no identity-based policy allows the s3:ListAllMyBuckets action

```
history
help
ubuntu@devops:~/.aws$ aws --profile s3operator s3 ls
The config profile (s3operator) could not be found
ubuntu@devops:~/.aws$ aws --profile s3operator s3 ls
An error occurred (AccessDenied) when calling the ListBuckets operation: User: arn:aws:iam::207567791252:user/s3-support is not authorized to perform: s3:ListAllMyBuckets because no identity-based policy allows the s3:ListAllMyBuckets action
ubuntu@devops:~/.aws$
```

*El siguiente paso es asumir el rol en aws CLI

Para asumir el rol debemos:

- 1* conocer el ARN DEL ROL
- 2* podríamos dar un nombre de sesión para identificarlo

Comandos para asumir el rol:

Acá nos otorga un nuevo accessKeyId, SecretAccessKey, y una sesión de token con expiración

```
--profile: command not found
ubuntu@devops:~/.aws$ aws --profile s3operator sts assume-role --role-arn arn:aws:iam::207567791252:role/s3operatorRole
{
  "Credentials": {
    "AccessKeyId": "ASIATAVABESKCU6WIRTY",
    "SecretAccessKey": "xXpoSqHJTcJPEWBqhSJrOE7pW4L+xSCeMwyIaaMG",
    "SessionToken": "FwoGZXIvYXZlePL////////wEaDPHabUz41dkqMg9ETyK6AZn8otLaqSTJX40F2FZw27fiW3Fwnf05+pzvm0h0eUpX5ebl1Mi96xArpwMVg2yWbUkvaZIYUFNG1svBSX0gxyELRK9pRFPg7bovgV9H9LTmU0/n9Hw7dfqV6oXR/jaRqhD",
    "Expiration": "2025-01-22T17:54:55+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROATAVABESKPBSWwGAL7:s3operatorRole-session",
    "Arn": "arn:aws:sts::207567791252:assumed-role/s3operatorRole/s3operatorRole-session"
  }
}
```

para configurar esto debemos llevarlo al perfil:

- ya sea editando el mismo perfil que tengo
- o bien crear otro profile:

s3operator

edito las credenciales de mi usuario
como se observa en las ilustraciones
con las nuevas credenciales antes obtenidas.


```
GNU nano 7.2                                credentials
[default]
aws_access_key_id = ""
aws_secret_access_key = ""
[s3operator]
aws_access_key_id = ASIATAVABESKFQ6K2HT3
aws_secret_access_key = PmBmabKH/Ye7cZSR2jJ4zv37WlgjGZzF4CBxGqLV
aws_session_token = FwoGZXIvYXZlECUaDPphPn9JCJWf9Tet4iK6AUB6qxQy/BL8kaEyFM3azKYIDBPM0PuVrmcPt7nEpA4tXIOLzzFeYs3orK8ZNPqrgd84nF
```

```
2025-01-24 15:05:37 s3-hernan-eduit
hernan@andres:~/aws$ cat credentials
[default]
aws_access_key_id = ""
aws_secret_access_key = ""
[s3operator]
aws_access_key_id = ASIATAVABESKFQ6K2HT3
aws_secret_access_key = PmBmabKH/Ye7cZSR2jJ4zv37WlgjGZzF4CBxGqLV
aws_session_token = FwoGZXIvYXZlECUaDPphPn9JCJWf9Tet4iK6AUB6qxQy/BL8kaEyFM3azKYIDBPM0PuVrmcPt7nEpA4tXIOLzzFeYs3orK8ZNPqrgd84nF
IPhMKPlc61tyPwwawTmIJrgTNVa0kgF6v9vtPyNELjgUpTuKsyclyF6yo0MSgw40qEMUIhp0wAk3ngLO+RfCDRb3BoIWdAnRMh/pE
e9jTPFJHlv1h80xnWekdYJZ9Gi8nIeml2KSAGN3NesFu9T6HgCiUyM+8BjItfy1TAHBbLsVPHY10xfFdc4Bj1gAoYIX5gZyEzbovy
hernan@andres:~/aws$
```

ejecutamos el siguiente comando
 aws --profile s3operator sts get-caller-identity
 Para verificar que se asumió el rol.

```
hernan@andres:~/aws$ aws --profile s3operator sts get-caller-identity
{
  "UserId": "AROATAVABESKMDOW2FG4U:s3operatorRole-session",
  "Account": "207567791252",
  "Arn": "arn:aws:sts::207567791252:assumed-role/s3operatorRole/s3operatorRole-session"
}
hernan@andres:~/aws$
```

Luego verifico que puede listar los bucket
 aws --profile s3operator s3 ls

```
already buckets - bucket
hernan@andres:~/aws$ aws --profile s3operator s3 ls
2025-01-24 15:05:37 s3-hernan-eduit
hernan@andres:~/aws$
```

Nombre	Región de AWS	Analizador de acceso IAM	Fecha de creación
<input type="radio"/> s3-hernan-eduit	Este de EE. UU. (Norte de Virginia) us-east-1	Ver analizador para us-east-1	24 de enero de 2025, 15:05:37 (UTC-03:00)

dando como resultado el acceso a lista de s3.