

Desafío 4

AWS Uso de roles

Profesores: Ezequiel Gonzalez Rodriguez, Facundo Miglio

Alumno: Pedro Jonas Alandia Rios

Institución: Educación IT

Fecha de entrega: 09/06/2024

Índice:

1 Creación de bucket s3, p3.

2 Creación de rol, p5.

3 Creación de usuario IAM, p7.

4 Actualización de política de IAM, p9.

5 Conexión mediante cli del usuario, p12.

6 Asunción de rol específico y pruebas, p14.

Lista de comandos utilizados, p16.

Diagrama de servicios Aws, p17.

Bibliografía, p18.

1. Creación de bucket S3

En esta primera etapa, con nuestro usuario Admin crearemos los recursos solicitados. Primero nos logeamos al CLI con nuestro usuario “Admin1” que es el de los permisos para llevar a cabo las primeras tareas del enunciado:

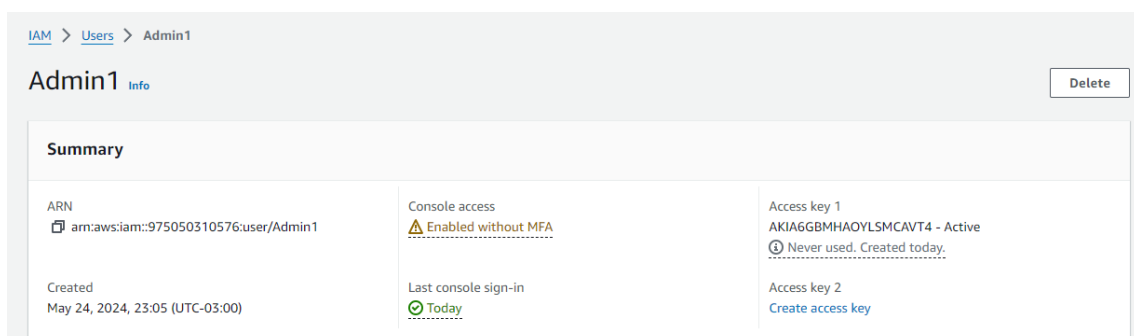
```
C:\Users\Jo>aws configure --profile Admin1
AWS Access Key ID [None]: AKIA6GBMHAOYLSCAVT4
AWS Secret Access Key [None]: /D6CHD1qNfrmQj8owq4YLNwig1iEtt7hmVded3qP
Default region name [None]: us-east-1
Default output format [None]:

C:\Users\Jo>whoami
desktop-ci90tq7\jo
```

```
C:\Users\Jo>aws configure list
      Name                               Value                               Type    Location
      ----                               -
profile                                <not set>                          None     None
access_key                            *****AVT4                        shared-credentials-file
secret_key                             *****d3qP                        shared-credentials-file
region                                 us-east-1                          config-file  ~/.aws/config

C:\Users\Jo>aws sts get-caller-identity
{
  "UserId": "AIDA6GBMHAOYNBXUX2N3F",
  "Account": "975050310576",
  "Arn": "arn:aws:iam::975050310576:user/Admin1"
}

C:\Users\Jo>
```



The screenshot shows the AWS IAM console page for the user 'Admin1'. The page includes a 'Summary' section with the following details:


Summary		
ARN arn:aws:iam::975050310576:user/Admin1	Console access Enabled without MFA	Access key 1 AKIA6GBMHAOYLSCAVT4 - Active Never used. Created today.
Created May 24, 2024, 23:05 (UTC-03:00)	Last console sign-in Today	Access key 2 Create access key

Procedemos a crear el bucket:

```
C:\Users\Jo>aws s3 mb s3://bucket-cli-1 --region us-east-1
make_bucket: bucket-cli-1
```

bucket-cli-1 [Info](#)

Objects **Properties** Permissions Metrics Management Access Points

Bucket overview		
AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN)  arn:aws:s3:::bucket-cli-1	Creation date May 26, 2024, 15:58:32 (UTC-03:00)

2. Creación de rol

Para crear el rol, utilizamos la consola para crear primero el JSON con la “trust policy” y pegarlo en nuestro pc local para que, al momento de crear el rol desde el cli, mediante un argumento específico, podamos cargarle ese archivo “json.json” con la descripción de nuestro rol para que sea asumido. En este caso, como aún no tenemos nuestro usuario “s3-support” creado, le cargamos la ARN del “Admin1”:

```
{ } json.json X
C: > Users > Jo > { } json.json > ...
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Principal": {
7                  "AWS": "arn:aws:iam::975050310576:user/Admin1"
8              },
9              "Action": "sts:AssumeRole"
10         }
11     ]
12 }
```

```
C:\Users\Jo>aws iam create-role --role-name rol-s3 --assume-role-policy-document file://json.json
{
  "Role": {
    "Path": "/",
    "RoleName": "rol-s3",
    "RoleId": "AROA6GBMHAOYBXRVEKOT",
    "Arn": "arn:aws:iam::975050310576:role/rol-s3",
    "CreateDate": "2024-05-29T23:15:29+00:00",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::975050310576:user/Admin1"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  }
}
```

Tal como vemos en este output, el rol fue creado y en su “Trust policy” tenemos cargada la del usuario “Admin1”, por lo que, de momento, el único capaz de asumir este rol sería el Admin1.

Podemos ver en la consola como segunda evidencia que el “rol-s3” fue creado exitosamente:

IAM > Roles > rol-s3

rol-s3 Info

Summary

Creation date	ARN
May 29, 2024, 20:15 (UTC-03:00)	arn:aws:iam::975050310576:role/rol-s3
Last activity	Maximum session duration
-	1 hour

[Permissions](#) | [Trust relationships](#) | [Tags](#) | [Access Advisor](#) | [Revoke sessions](#)

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::975050310576:user/Admin1"
8       },
9       "Action": "sts:AssumeRole"
10    }
11  ]
12 }
```

Le otorgamos al rol la policy para poder listar, subir y descargar archivos de los bucket de s3:

```
C:\Users\Jo>aws iam put-role-policy --role-name rol-s3 --policy-name s3 --policy-document file://s3.json
```

```
{ s3.json x
C: > Users > Jo > {} s3.json > ...
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "s3:PutObject",
9         "s3:GetObject",
10        "s3:ListAllMyBuckets",
11        "s3:ListBucket"
12      ],
13       "Resource": "*"
14     }
15   ]
16 }
```

3. Creación de usuario IAM

Primero creamos un grupo para los usuarios soporte que asumirán los roles correspondientes:

```
C:\Users\Jo>aws iam create-group --group-name grupo-de-soporte
{
  "Group": {
    "Path": "/",
    "GroupName": "grupo-de-soporte",
    "GroupId": "AGPA6GBMHAOYFFDEOZNQY",
    "Arn": "arn:aws:iam::975050310576:group/grupo-de-soporte",
    "CreateDate": "2024-05-27T00:20:15+00:00"
  }
}
```

[IAM](#) > [User groups](#) > grupo-de-soporte

grupo-de-soporte [Info](#) [Delete](#)

Summary [Edit](#)

User group name	Creation time	ARN
grupo-de-soporte	May 26, 2024, 21:20 (UTC-03:00)	arn:aws:iam::975050310576:group/grupo-de-soporte

Creamos usuario y lo asignamos al “grupo-de-soporte”:

```
C:\Users\Jo>aws iam create-user --user-name s3-support
{
  "User": {
    "Path": "/",
    "UserName": "s3-support",
    "UserId": "AIDA6GBMHAOYA0BTJFSSL",
    "Arn": "arn:aws:iam::975050310576:user/s3-support",
    "CreateDate": "2024-05-27T00:27:09+00:00"
  }
}

C:\Users\Jo>aws iam add-user-to-group --group-name grupo-de-soporte --user-name s3-support
C:\Users\Jo>
```

[IAM](#) > [User groups](#) > grupo-de-soporte

grupo-de-soporte [Info](#)

Summary

User group name
grupo-de-soporte

Creation time
May 26, 2024, 21:20 (UTC-03:00)

Users (1)

Permissions

Access Advisor

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Q Search

☐

User name [🔗](#)

▲ | Gr

☐

[s3-support](#)

1

De esta manera concluimos el paso 3, crear el usuario con el nombre que fue solicitado en el enunciado, a saber, “s3-support”.


4. Actualización de política de IAM

Para actualizar la política del rol necesitamos el ARN de nuestro usuario “s3-support”, una vez lo obtenemos, lo reemplazamos por el que tiene cargada el rol-s3, que es la del usuario “Admin1”:

```
C:\Users\Jo>aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "Admin1",
      "UserId": "AIDA6GBMHAOYNBXUX2N3F",
      "Arn": "arn:aws:iam::975050310576:user/Admin1",
      "CreateDate": "2024-05-25T02:05:29+00:00",
      "PasswordLastUsed": "2024-05-29T22:07:31+00:00"
    },
    {
      "Path": "/",
      "UserName": "s3-support",
      "UserId": "AIDA6GBMHAOYA0BTJFSSL",
      "Arn": "arn:aws:iam::975050310576:user/s3-support",
      "CreateDate": "2024-05-27T00:27:09+00:00"
    },
    {
      "Path": "/",
      "UserName": "support-prueba",
      "UserId": "AIDA6GBMHAOYISYILWZLM",
      "Arn": "arn:aws:iam::975050310576:user/support-prueba",
      "CreateDate": "2024-05-25T02:45:32+00:00",
      "PasswordLastUsed": "2024-05-26T19:41:54+00:00"
    }
  ]
}
```

Tomamos el ARN que necesitamos: "arn:aws:iam::975050310576:user/s3-support" y lo pegamos cambiando en nuestro archivo json:

```
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More

{} json.json x
C: > Users > Jo > {} json.json > [ ] Statement > {} 0 > {} Principal >  AWS
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Principal": {
7                  "AWS": "arn:aws:iam::975050310576:user/s3-support"
8              },
9              "Action": "sts:AssumeRole"
10         }
11     ]
12 }
```

Modificamos nuestro rol:

```
C:\Users\Jo>aws iam update-assume-role-policy --role-name rol-s3 --policy-document file://json.json
```

Verificamos:

```
C:\Users\Jo>aws iam get-role --role-name rol-s3
{
  "Role": {
    "Path": "/",
    "RoleName": "rol-s3",
    "RoleId": "AROA6GBMHAOYBXRVEKOT",
    "Arn": "arn:aws:iam::975050310576:role/rol-s3",
    "CreateDate": "2024-05-29T23:15:29+00:00",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::975050310576:user/s3-support"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    },
    "MaxSessionDuration": 3600,
    "RoleLastUsed": {}
  }
}
```

Actualizando el ARN con el correspondiente comando, ya se encuentra actualizado y como dice la documentación, el comando update no tiene output:

```
C:\Users\Jo>aws iam update-role --role-name rol-s3
C:\Users\Jo>aws iam get-role --role-name rol-s3
{
  "Role": {
    "Path": "/",
    "RoleName": "rol-s3",
    "RoleId": "ARO0A6GBMHA0YBXRVEKOT",
    "Arn": "arn:aws:iam::975050310576:role/rol-s3",
    "CreateDate": "2024-05-29T23:15:29+00:00",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::975050310576:user/s3-support"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    },
    "MaxSessionDuration": 3600,
    "RoleLastUsed": {}
  }
}

C:\Users\Jo>
```

5. Conexión mediante cli del usuario

Conectamos por primera vez nuestro usuario “s3-support” con nuestro cli local, para eso debemos crear unas Access key para este usuario:

```
C:\Users\Jo>aws iam create-access-key --user-name s3-support
{
  "AccessKey": {
    "UserName": "s3-support",
    "AccessKeyId": "AKIA6GBMHAOYMB6WJVG5",
    "Status": "Active",
    "SecretAccessKey": "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",
    "CreateDate": "2024-05-30T00:27:26+00:00"
  }
}
```

Los dos datos que precisamos guardar son "AccessKey":
"AKIA6GBMHAOYMB6WJVG5" y "SecretAccessKey":
"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".

Cargamos nuestras credenciales:

```
C:\Users\Jo>aws configure --profile s3-support
AWS Access Key ID [None]: AKIA6GBMHAOYMB6WJVG5
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]:

C:\Users\Jo>aws sts get-caller-identity
{
  "UserId": "AIDA6GBMHAOYNBXUX2N3F",
  "Account": "975050310576",
  "Arn": "arn:aws:iam::975050310576:user/Admin1"
}

C:\Users\Jo>_
```

Si vemos en la imagen, las key del usuario s3-support fueron correctamente cargadas, al consultar por el usuario logeado, nos arroja la información del usuario “Admin1”, esto se debe a que en el archivo credentials, donde se encuentran alojada toda la información de los usuarios, los datos del Admin1 están como default:

```
> Usuarios > Jo > .aws

credentials: Bloc de notas

Archivo Edición Formato Ver Ayuda

[default]
aws_access_key_id = AKIA6GBMHAOYLSMCAVT4
aws_secret_access_key = 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
[Admin1]
aws_access_key_id = AKIA6GBMHAOYLSMCAVT4
aws_secret_access_key = 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
[s3-support]
aws_access_key_id = AKIA6GBMHAOYMB6WJVGS
aws_secret_access_key = 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
```

Modificamos el archivo eliminando el default, de otra manera siempre nos conectará como Admin1:

```
> Usuarios > Jo > .aws

credentials: Bloc de notas

Archivo Edición Formato Ver Ayuda

[Admin1]
aws_access_key_id = AKIA6GBMHAOYLSMCAVT4
aws_secret_access_key = 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
[s3-support]
aws_access_key_id = AKIA6GBMHAOYMB6WJVGS
aws_secret_access_key = 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
```

```
C:\Users\Jo>aws sts get-caller-identity

Unable to locate credentials. You can configure credentials by running "aws configure".

C:\Users\Jo>aws configure
AWS Access Key ID [None]: AKIA6GBMHAOYMB6WJVGS
AWS Secret Access Key [None]: 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
Default region name [us-east-1]:
Default output format [None]:

C:\Users\Jo>aws sts get-caller-identity
{
  "UserId": "AIDA6GBMHAOYA0BTJFSSL",
  "Account": "975050310576",
  "Arn": "arn:aws:iam::975050310576:user/s3-support"
}
```

6. Asunción de rol específico y pruebas

Asumimos el rol “rol-s3”

```
C:\Users\Jo>aws sts assume-role --role-arn arn:aws:iam::975050310576:role/rol-s3 --role-session-name para-s3
{
  "Credentials": {
    "AccessKeyId": "ASIA6GBMHAOYBKXINKXM",
    "SecretAccessKey": "9T17TKqc29NG+6ULqZuc8ew70PnU5UtxxbgjrT3/",
    "SessionToken": "IQoJb3JpZ2luX2VjEFAaCXVzLWVhc3QtMSJHMEUCIDyeuynMhe0BYgnjvoJHZT4z3qWV4t5/BwCfh+nB11LHAiEAuiGb7cZyImHT
DK6QatNhyRbgQ3DIpyrXAZgwJ+FJUjBVf6WBMuFHTs1k8NMfJwP4HsaUfS0iWqeKMD8G0UhlP+X1RS1jhbKAT3XM3aMG6WtvvsGgdLfm77meessQSKdJ/t21tvgqy
5FTu3n6nH17FLfy/SWp+UWPEXHgTX9szzmnB1T/rpMBHT7Ji6k3W35JWMI/HU8GVHoZYur7ew8XWYk73GrEX4AWDxuAT4b2vh41Y+esgOz5ipCoJ05QBU6rDnUX+k
6E150Ygutk7qe6fQf7a6EVKZbvTJ1PnNqswUhaPPRS1zqv71wuejZn//eRjcGxEJB40ENbPeRbLft5+YoYSJNRa+LkKP38btom+dfWBURFs2v22CHw8QrIFwG1bma
",
    "Expiration": "2024-06-06T16:47:31+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROA6GBMHAOYBXRVUEKOT:para-s3",
    "Arn": "arn:aws:sts::975050310576:assumed-role/rol-s3/para-s3"
  }
}
```

Ahora que tenemos la “AccessKey”, “SecretAccessKey” y el “SessionToken”, modificamos nuestro archivo “credentials” para crear un usuario llamado “rol-s3-cred2” con esos datos:



```
credentials: Bloc de notas
Archivo Edición Formato Ver Ayuda
[Admin1]
aws_access_key_id = AKIA6GBMHAOYLSMCAVT4
aws_secret_access_key = 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
[s3-support]
aws_access_key_id = AKIA6GBMHAOYMB6WJVGS
aws_secret_access_key = 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
[default]
aws_access_key_id = AKIA6GBMHAOYMB6WJVGS
aws_secret_access_key = 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
[rol-s3-cred]
source_profile = rol-s3-cred2
role_arn = arn:aws:iam::975050310576:role/rol-s3
[rol-s3-cred2]
aws_access_key_id=ASIA6GBMHAOYBKXINKXM
aws_secret_access_key=9T17TKqc29NG+6ULqZuc8ew70PnU5UtxxbgjrT3/
aws_session_token=IQoJb3JpZ2luX2VjEFAaCXVzLWVhc3QtMSJHMEUCIDyeuynMhe0BYgnjvo
```

Terminado esto, vamos a tener acceso a los bucket de s3 (según lo que permita la policy del recurso) y cada comando vamos a terminarlo indicando el perfil temporal creado más arriba para que nos dé acceso al servicio de s3:

Listamos buckets:

```
C:\Users\Jo>aws s3 ls --profile rol-s3-cred2
2024-05-26 15:58:32 bucket-cli-1
2024-05-24 23:46:36 bucket-rpeuba
```

General purpose buckets

Directory buckets

General purpose buckets (2) Info

All AWS Regions

Buckets are containers for data stored in S3.

	Name	AWS Region
<input type="radio"/>	bucket-cli-1	US East (N. Virginia) us-east-1
<input type="radio"/>	bucket-rpeuba	US East (N. Virginia) us-east-1

Probamos subir un archivo desde nuestro pc local al bucket creado en este ejercicio:

```
C:\Users\Jo>aws s3 cp s3.json s3://bucket-cli-1/holamundo.txt --profile rol-s3-cred2
upload: .\s3.json to s3://bucket-cli-1/holamundo.txt

C:\Users\Jo>aws s3 ls s3://bucket-cli-1

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied

C:\Users\Jo>aws s3 ls s3://bucket-cli-1 --profile rol-s3-cred2
2024-06-06 13:40:38          361 holamundo.txt

C:\Users\Jo>
```

holamundo.txt Info

Copy S3 URI

Download

Open

Properties

Permissions

Versions

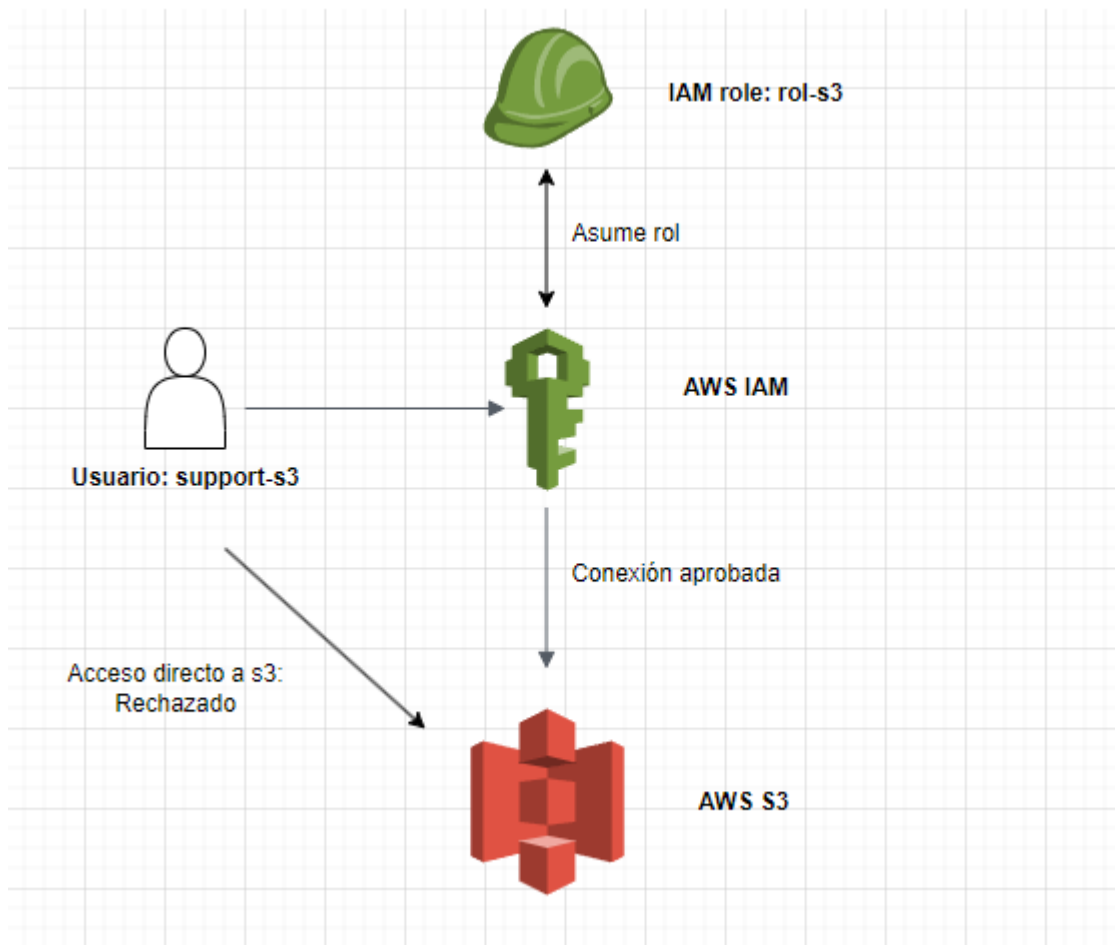
Object overview

Owner	pedro.alandia.aws1	S3 URI	s3://bucket-cli-1/holamundo.txt
AWS Region	US East (N. Virginia) us-east-1	Amazon Resource Name (ARN)	arn:aws:s3:::bucket-cli-1/holamundo.txt
Last modified	June 6, 2024, 13:40:38 (UTC-03:00)	Entity tag (Etag)	cbc0991c04ed230828cd9fb8bd739c21
Size	361.0 B	Object URL	https://bucket-cli-1.s3.amazonaws.com/holamundo.txt
Type	txt		

Lista de comandos utilizados

```
aws configure --profile Admin1
aws configure list
aws sts get-caller-identity
aws s3 mb s3://bucket-cli-1 --region us-east-1
aws iam create-role --role-name rol-s3 --assume-role-policy-document file://json.json
aws iam create-group --group-name grupo-de-soporte
aws iam create-user --user-name s3-support
aws iam add-user-to-group --group-name grupo-de-soporte --user-name s3-support
aws iam list-users
aws iam update-assume-role-policy --role-name rol-s3 --policy-document
file://json.json
aws iam get-role --role-name rol-s3
aws iam update-role --role-name rol-s3
aws iam get-role --role-name rol-s3
aws iam create-access-key --user-name s3-support
aws configure --profile s3-support
aws sts get-caller-identity
aws sts assume-role --role-arn arn:rol-s3 --role-session-name para-s3
aws s3 ls --profile rol-s3-cred2
aws s3 cp s3.json s3://bucket-cli-1/holamundo.txt --profile rol-s3-cred2
aws s3 ls s3://bucket-cli-1 --profile rol-s3-cred2
```


Diagrama servicios AWS



El usuario “support-s3” no puede realizar modificaciones en s3 ya que las políticas de su grupo de trabajo no lo permiten, ni el servicio S3 posee al usuario autorizado.

El camino feliz es solicitar mediante AWS IAM el rol que tiene cargado políticas para modificar S3. Una vez asume este rol, puede acceder a las funciones permitidas por el rol a AWS S3.

Bibliografía

<https://docs.aws.amazon.com/cli/latest/reference/iam/create-role.html>

<https://docs.aws.amazon.com/IAM/latest/UserGuide/roles-managingrole-editing-cli.html>

<https://docs.aws.amazon.com/cli/latest/reference/iam/update-role.html>

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html

<https://docs.aws.amazon.com/cli/latest/reference/iam/put-role-policy.html>

<https://www.youtube.com/watch?v=6Hwdxm3jowI>

<https://docs.aws.amazon.com/sdkref/latest/guide/feature-assume-role-credentials.html>

<https://docs.aws.amazon.com/sdkref/latest/guide/access-assume-role.html>

<https://docs.aws.amazon.com/cli/latest/userguide/cli-services-s3-commands.html>