

## Desafío # 4

**Realizado por: Joselin Teixeira**

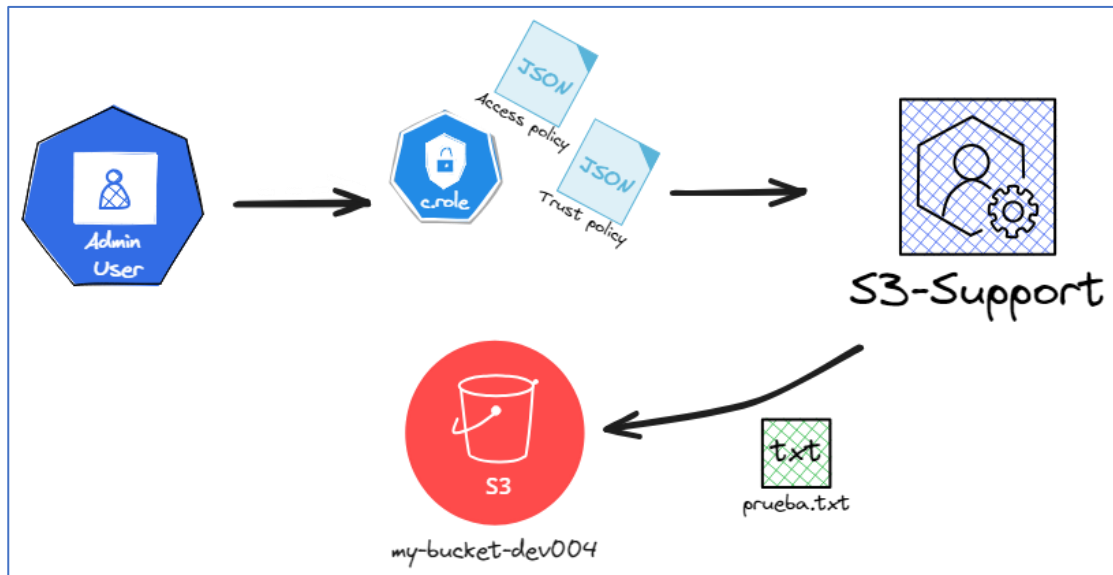
*Fecha de entrega: 28/05/2024*

### Escenario:

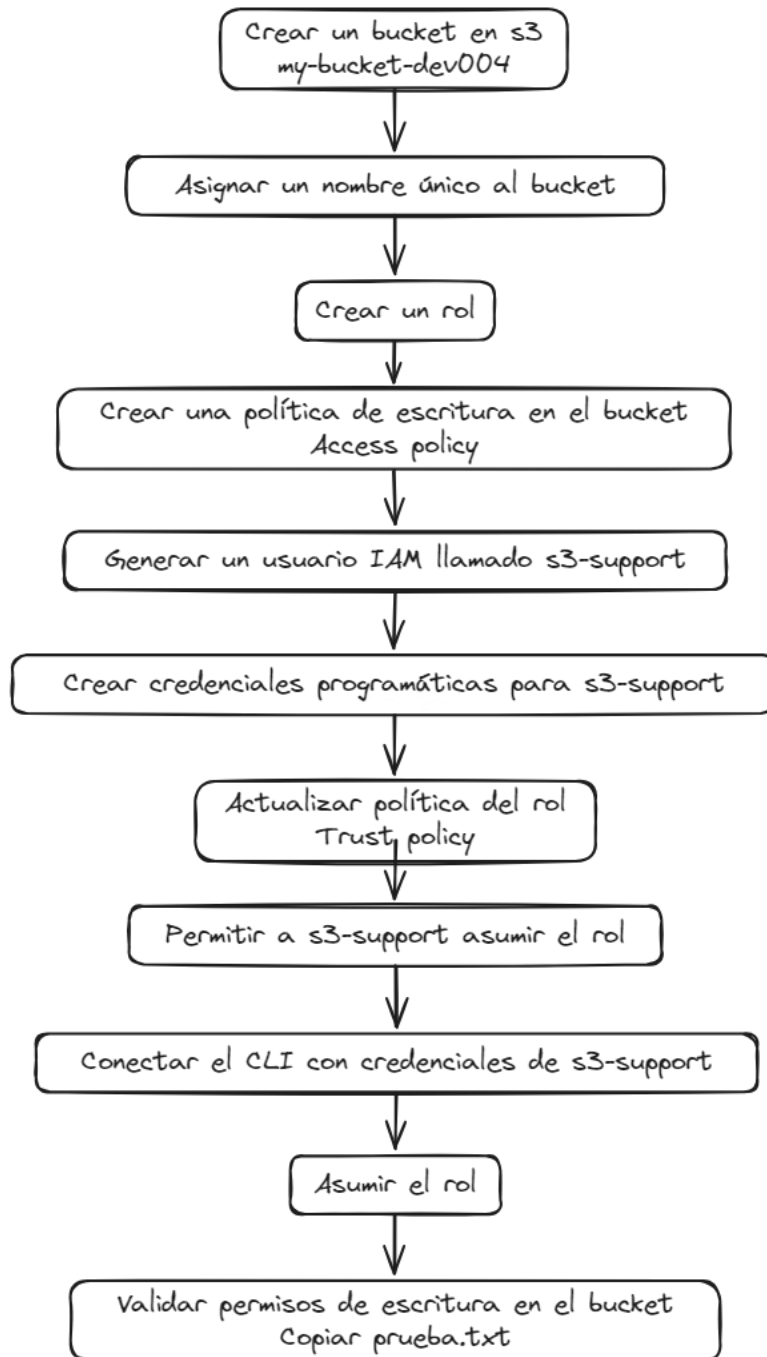
Eres un administrador de sistemas en una empresa que utiliza AWS para sus servicios en la nube. Te han asignado la tarea de configurar un rol de IAM que permita a los usuarios asumirlo desde la CLI para escribir archivos en un bucket de S3 específico.

### 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 unas 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.



## Diagrama General - Desafio 4



## 1. Crear un bucket en s3.

Para crear un bucket en S3 desde la AWS CLI, utilizaremos el siguiente comando:

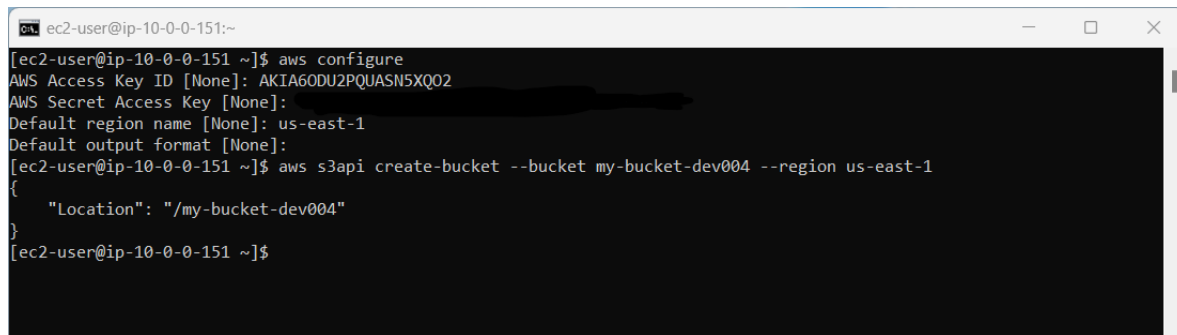
Referencias:

- [https://docs.aws.amazon.com/es\\_es/AmazonS3/latest/userguide/create-bucket-overview.html](https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/create-bucket-overview.html)

```
aws s3api create-bucket \
  --bucket my-bucket- \
  --region us-east-1
```

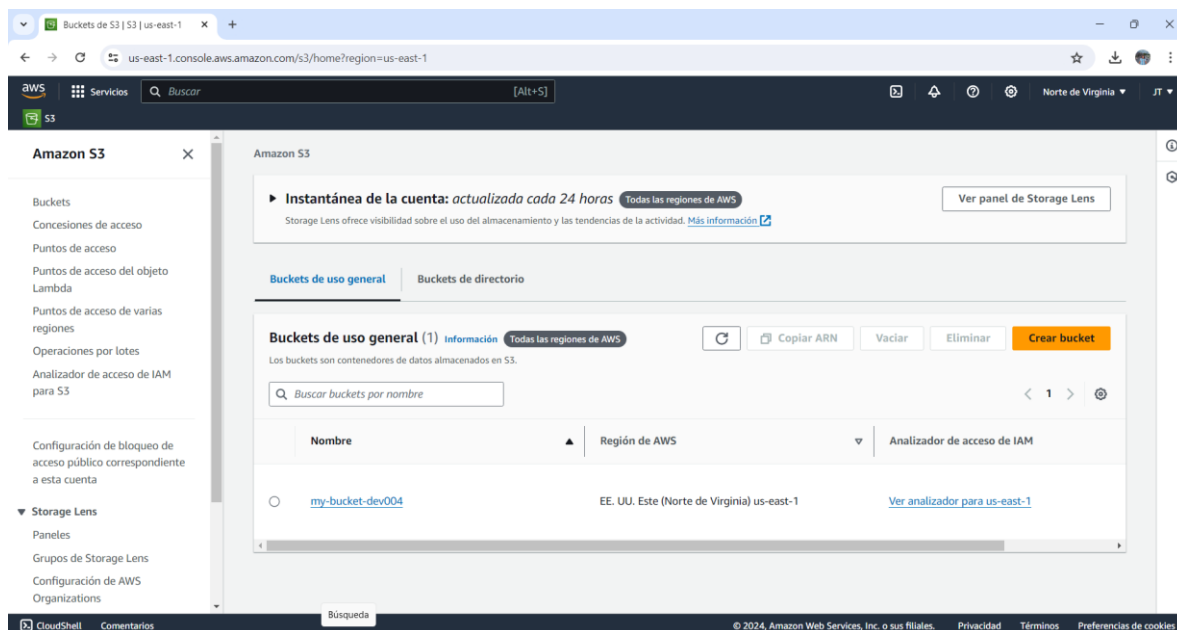
Output:

```
{
  "Location": "/my-bucket"
}
```



```
ec2-user@ip-10-0-0-151:~
[ec2-user@ip-10-0-0-151 ~]$ aws configure
AWS Access Key ID [None]: AKIA60DU2PQUASN5XQ02
AWS Secret Access Key [None]:
Default region name [None]: us-east-1
Default output format [None]:
[ec2-user@ip-10-0-0-151 ~]$ aws s3api create-bucket --bucket my-bucket-dev004 --region us-east-1
{
  "Location": "/my-bucket-dev004"
}
[ec2-user@ip-10-0-0-151 ~]$
```

Verificamos desde la consola AWS que efectivamente se generó el Bucket



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

Referencias:

- [https://docs.aws.amazon.com/es\\_es/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example4.html](https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example4.html)
- [https://docs.aws.amazon.com/es\\_es/AmazonS3/latest/userguide/example-bucket-policies.html?icmpid=docs\\_amazons3\\_console#example-bucket-policies-public-access](https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/example-bucket-policies.html?icmpid=docs_amazons3_console#example-bucket-policies-public-access)

Se utiliza `cat << EOF >` `policy.json` para crear el archivo `policy.json` con la política JSON especificada. Luego se ejecuta el comando `ls` para validar que fue creado el archivo.

```
ec2-user@ip-10-0-0-151:~  
[ec2-user@ip-10-0-0-151 ~]$ aws configure  
AWS Access Key ID [None]: AKIA60DU2PQUASN5XQ02  
AWS Secret Access Key [None]: +3gXookwbuDHw6qMZ0hQmWxoQ4iysGe6+B9uAJAI  
Default region name [None]: us-east-1  
Default output format [None]:  
[ec2-user@ip-10-0-0-151 ~]$ aws s3api create-bucket --bucket my-bucket-dev004 --region us-east-1  
{  
  "Location": "/my-bucket-dev004"  
}  
[ec2-user@ip-10-0-0-151 ~]$ cat << EOF > policy.json  
> {  
>   "Version": "2012-10-17",  
>   "Statement": [  
>     {  
>       "Effect": "Allow",  
>       "Action": [  
>         "s3:ListBucket*",  
>         "s3:PutBucket*",  
>         "s3:GetBucket*"  
>       ],  
>       "Resource": [  
>         "arn:aws:s3:::my-bucket"  
>       ]  
>     }  
>   ]  
> }  
> EOF  
[ec2-user@ip-10-0-0-151 ~]$ ls  
policy.json  
[ec2-user@ip-10-0-0-151 ~]$
```

## 3. Crear Usuario

# Comando `aws iam create-user`

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

```
ec2-user@ip-10-0-0-151:~  
[ec2-user@ip-10-0-0-151 ~]$ aws iam create-user --user-name s3-support  
{  
  "User": {  
    "Path": "/",  
    "UserName": "s3-support",  
    "UserId": "AIDA60DU2PQUWL5MD3V",  
    "Arn": "arn:aws:iam::992382450728:user/s3-support",  
    "CreateDate": "2024-05-26T01:49:50+00:00"  
  }  
}  
[ec2-user@ip-10-0-0-151 ~]$
```

Creamos credenciales de acceso para el usuario:

```
ec2-user@ip-10-0-0-151:~$ aws iam create-user --user-name s3-support
{
  "User": {
    "Path": "/",
    "UserName": "s3-support",
    "UserId": "AIDA6ODU2PQUDWLA5MD3V",
    "Arn": "arn:aws:iam:992382450728:user/s3-support",
    "CreateDate": "2024-05-26T01:49:50+00:00"
  }
}
[ec2-user@ip-10-0-0-151 ~]$ ls
policy.json  trust-policy.json
[ec2-user@ip-10-0-0-151 ~]$ aws iam create-access-key --user-name s3-support
{
  "AccessKey": {
    "UserName": "s3-support",
    "AccessKeyId": "AKIA6ODU2PQUKUQOM7SH",
    "Status": "Active",
    "SecretAccessKey": "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",
    "CreateDate": "2024-05-26T01:54:15+00:00"
  }
}
[ec2-user@ip-10-0-0-151 ~]$
```

4. Ahora, se crea el rol de IAM utilizando la política de confianza:

Inicialmente tenemos un archivo JSON para la política de confianza del rol llamado trust-policy.json:

```
ec2-user@ip-10-0-0-151:~$ cat trust-policy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam:992382450728:user/s3-support"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

# Comando `aws iam create-role`

# Este comando crea un nuevo rol en IAM con el nombre especificado y define el documento de política de confianza que establece quién puede asumir el rol.

```
aws iam create-role --role-name s3-write-role --assume-role-policy-document file://trust-policy.json
```

```
ec2-user@ip-10-0-0-151:~$ aws iam create-role --role-name s3-write-role --assume-role-policy-document file://trust-policy.json
{
  "Role": {
    "Path": "/",
    "RoleName": "s3-write-role",
    "RoleId": "AROAG6ODU2PQUPUHNHSHBU",
    "Arn": "arn:aws:iam:992382450728:role/s3-write-role",
    "CreateDate": "2024-05-26T03:15:32+00:00",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam:992382450728:user/s3-support"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  }
}
[ec2-user@ip-10-0-0-151 ~]$
```

Aplicar política de permiso a rol

# Comando aws iam put-role-policy

# Este comando adjunta una política al rol recién creado para definir los permisos que tiene el rol.

```
aws iam put-role-policy --role-name s3-write-role --policy-name s3-write-policy --policy-document file://policy.json
```

```
ec2-user@ip-10-0-0-151:~$ aws iam put-role-policy --role-name s3-write-role --policy-name s3-write-policy --policy-document file://policy.json
```

Estos comandos en conjunto permiten crear un nuevo rol en IAM llamado "s3-write-role" con una política de confianza definida en trust-policy.json y luego adjuntar una política de permisos especificada en policy.json a ese rol para definir los permisos que tendrá el rol en AWS.

# Configuramos las credenciales de AWS CLI para el usuario s3-support

Aws configure

# Para asumir el rol, primero se obtiene las credenciales temporales utilizando sts:assume-role:

```
aws sts assume-role --role-arn arn:aws:iam::992382450728:role/S3WriteRole --role-session-name S3WriteSession
```

```
ec2-user@ip-10-0-0-151:~$ aws configure
Last login: Sun May 26 02:21:14 2024 from 45.77.162.236
[ec2-user@ip-10-0-0-151 ~]$ aws configure
AWS Access Key ID [*****]: AKIA60DU2PQUKUQOM7SH
AWS Secret Access Key [*****]: D/LaFwSjUYZn/deU//uEd8KMnuAzlexoNJ/CN8A4
Default region name [us-east-1]:
Default output format [None]:
[ec2-user@ip-10-0-0-151 ~]$ ls
policy.json  trust-policy.json
[ec2-user@ip-10-0-0-151 ~]$ aws configure --profile s3-support
AWS Access Key ID [None]: AKIA60DU2PQUKUQOM7SH
AWS Secret Access Key [None]: D/LaFwSjUYZn/deU//uEd8KMnuAzlexoNJ/CN8A4
[ec2-user@ip-10-0-0-151 ~]$ aws sts assume-role --role-arn arn:aws:iam::992382450728:role/S3WriteRole --role-session-name S3WriteSession
{
  "Credentials": {
    "AccessKeyId": "ASTIA60DU2PQUFU3Q22EM",
    "SecretAccessKey": "b5KyLkcpbysV+e3LvE2eyC5ARLYSDNzBfpU9zTPq",
    "SessionToken": "IQoJb3JpZ2luX2VjEDsaCXVzLWVhc3QtMSJGMEQCFyCXwVUgYma3FJfEL7iCLHwL+ftBaE5FSqt3zde6obUAi8TmywY09aAjkktreSohaJ3KY8tLjivq7cm6feYrFR6SqAgio//////////8BEAAaDDk5MjM4MjQ1MDcyOCIMScPdkwS7km5csBxKvgBKKXmxipTTGMwovwaplyGMj2j1VYDLfsXBRsKmqZQNZANP05wzKxbpf3t3sHMFOMdEHGViagV04LM8dnYxrk/d5b+4BWZLjsUm0iB0YYzs5XF8svmYJK14E7qXYiHvy2q3RqKFSgPwDHyQwE7GrFNmr6sU29Bq7iwdM0MLzPXSMMjdz924r8H+79u8WqiSKTK8T2BiJFfeXgmFT9zyvp/ZcIM6ZWky6GKq3rMwU1NshHLZi+4HGg6YGhJhwi9Kht4yalaKoU37g4ISHiX3sEHxzfaGLp1pp8mQ0L/E57NP3LHW057v9ZrHWQaBpuamSQ2Lx1xdvQ9wgwosHKsgY6ngEicUT0XVWNG/UWz48ltpHenjeozEwMDUwYDoK+yR14zIKQShNGZMTem98BNqblJ2H9mwGnJ1EXDBNDCLfbWbHoEWKE3xjeuVqzfx3skgMVv5piFTMGwVM00z6kZTpM2k6q8SeeQ7SzoYQceat/bOb1Q2L28q9B+Kz6s+6N7w+SVJodiH9YC9Yu/gA14N1u21wyHxm3zm4rfXN/YEd+w==",
    "Expiration": "2024-05-26T03:38:26+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROA60DU2PQUCLQFYVAQD:S3WriteSession",
    "Arn": "arn:aws:sts::992382450728:assumed-role/S3WriteRole/S3WriteSession"
  }
}
```

Ahora actualizamos la política de confianza del rol s3-write-role para permitir que el usuario s3-support pueda asumir el rol:

```
ec2-user@ip-10-0-0-151:~$ aws iam update-assume-role-policy --role-name s3-write-role --policy-document file://trust-policy.json
[ec2-user@ip-10-0-0-151 ~]$
```

## 6. Asumiendo el rol

```
ec2-user@ip-10-0-0-151:~$ aws iam update-assume-role-policy --role-name s3-write-role --policy-document file:///trust-policy.json
[ec2-user@ip-10-0-0-151 ~]$ aws configure --profile s3-support
AWS Access Key ID [*****]: AKIA60DU2PQUKUQW7SH
AWS Secret Access Key [*****]: D/LaFwsjUYZn/deU//uEd8KMMuAzlexoNJ/CN8A4
Default region name [us-east-1]:
Default output format [None]:
[ec2-user@ip-10-0-0-151 ~]$ aws sts assume-role --role-arn arn:aws:iam::992382450728:role/s3-write-role --role-session-name s3-write-session --profile s3-support
{
  "Credentials": {
    "AccessKeyId": "ASIA60DU2PQUCXRB8U05",
    "SecretAccessKey": "m4T0AbXan0N5t20fP0wrt13upgN7LaZ03wv/Yfr4",
    "SessionToken": "IQoJb3JpZ2luX2VjEDwaCXVzLWVhc3QtMSJGMEQICIM/Fj67IzZfuurvo/IsWdncG8xGMI5QRTT+wjGSPbObAIA87LatDubGzSMnaDS1iWIp8cNk/OQ61qzEE17466YBrSqmAgi1/////////8BEAAADdk5MjM4MjQ1MDcyOCIMia6gOGaPrcutGTR2Kvob1dkmZvohGLSgYsQ0q+7o9y3l2WYkk0whkhJZ3b6fJon4pNy063SWEwEK36BuiLMQK14uuWUY3FPKQ83UblJBugytwvraQ5QJiDkcyLwVT6DZe3qa+nR1cLOKHXqCAXp9gRw6h1cZb0+lcda/noxhY9XPCIMi5BtNfvM7SzL/whhyk55yyH+3TXnX1iXlKLwCAg+cs3EnCeykevZHG4SuZsTgpoICtzbP6Lwr7Y/ewbKONZc66iM2Ib2TveeJFnT4UXnB/qdPncQl0LHF/CONJiz1As0boK/oKuEsUId8EAdeCk7kyVDkh87u8R3TIGz/yRuQ3HxMG5KTCV18qyBjqeAbcKZTHhkpZCcFKIIwRSu02NiUpXJ8hIFYyQ0g2vuHbnL7ZIC2iW/5f08c/9quKRsDPU3MlJ1ZIm27wDpDGJusqUy5FCv1hDUazYzvZalBYXht2e9PU1aQWBC/coZrbbUoU3e65/uykrIMIG2WfrzYx4lGIWe8D0wuaV6VawQg1BmXQMj2aoMlMGfPxVl1UyoRX16XSUiNmzv03kRz",
    "Expiration": "2024-05-26T04:25:09+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROA60DU2PQUPUHNSKBU:s3-write-session",
    "Arn": "arn:aws:sts::992382450728:assumed-role/s3-write-role/s3-write-session"
  }
}
```

Mediante el siguiente comando podemos verificar el contenido del bucket:

# Verificar el contenido del bucket

aws s3 ls s3://my-bucket-dev004

```
ec2-user@ip-10-0-0-151:~$ aws iam update-assume-role-policy --role-name s3-write-role --policy-document file:///trust-policy.json
[ec2-user@ip-10-0-0-151 ~]$ aws configure --profile s3-support
AWS Access Key ID [*****]: AKIA60DU2PQUKUQW7SH
AWS Secret Access Key [*****]: D/LaFwsjUYZn/deU//uEd8KMMuAzlexoNJ/CN8A4
Default region name [us-east-1]:
Default output format [None]:
[ec2-user@ip-10-0-0-151 ~]$ aws sts assume-role --role-arn arn:aws:iam::992382450728:role/s3-write-role --role-session-name s3-write-session --profile s3-support
{
  "Credentials": {
    "AccessKeyId": "ASIA60DU2PQUCXRB8U05",
    "SecretAccessKey": "m4T0AbXan0N5t20fP0wrt13upgN7LaZ03wv/Yfr4",
    "SessionToken": "IQoJb3JpZ2luX2VjEDwaCXVzLWVhc3QtMSJGMEQICIM/Fj67IzZfuurvo/IsWdncG8xGMI5QRTT+wjGSPbObAIA87LatDubGzSMnaDS1iWIp8cNk/OQ61qzEE17466YBrSqmAgi1/////////8BEAAADdk5MjM4MjQ1MDcyOCIMia6gOGaPrcutGTR2Kvob1dkmZvohGLSgYsQ0q+7o9y3l2WYkk0whkhJZ3b6fJon4pNy063SWEwEK36BuiLMQK14uuWUY3FPKQ83UblJBugytwvraQ5QJiDkcyLwVT6DZe3qa+nR1cLOKHXqCAXp9gRw6h1cZb0+lcda/noxhY9XPCIMi5BtNfvM7SzL/whhyk55yyH+3TXnX1iXlKLwCAg+cs3EnCeykevZHG4SuZsTgpoICtzbP6Lwr7Y/ewbKONZc66iM2Ib2TveeJFnT4UXnB/qdPncQl0LHF/CONJiz1As0boK/oKuEsUId8EAdeCk7kyVDkh87u8R3TIGz/yRuQ3HxMG5KTCV18qyBjqeAbcKZTHhkpZCcFKIIwRSu02NiUpXJ8hIFYyQ0g2vuHbnL7ZIC2iW/5f08c/9quKRsDPU3MlJ1ZIm27wDpDGJusqUy5FCv1hDUazYzvZalBYXht2e9PU1aQWBC/coZrbbUoU3e65/uykrIMIG2WfrzYx4lGIWe8D0wuaV6VawQg1BmXQMj2aoMlMGfPxVl1UyoRX16XSUiNmzv03kRz",
    "Expiration": "2024-05-26T04:25:09+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROA60DU2PQUPUHNSKBU:s3-write-session",
    "Arn": "arn:aws:sts::992382450728:assumed-role/s3-write-role/s3-write-session"
  }
}
[ec2-user@ip-10-0-0-151 ~]$ aws s3 ls s3://my-bucket-dev004
2024-05-26 03:27:56      44511 4 - AWS Uso de roles.pdf
[ec2-user@ip-10-0-0-151 ~]$
```

# Creamos un archivo vacío llamado prueba.txt

Touch prueba.txt

```
ec2-user@ip-10-0-0-151:~$ aws iam update-assume-role-policy --role-name s3-write-role --policy-document file:///trust-policy.json
[ec2-user@ip-10-0-0-151 ~]$ aws configure --profile s3-support
AWS Access Key ID [*****]: AKIA60DU2PQUKUQW7SH
AWS Secret Access Key [*****]: D/LaFwsjUYZn/deU//uEd8KMMuAzlexoNJ/CN8A4
Default region name [us-east-1]:
Default output format [None]:
[ec2-user@ip-10-0-0-151 ~]$ aws sts assume-role --role-arn arn:aws:iam::992382450728:role/s3-write-role --role-session-name s3-write-session --profile s3-support
{
  "Credentials": {
    "AccessKeyId": "ASIA60DU2PQUCXRB8U05",
    "SecretAccessKey": "m4T0AbXan0N5t20fP0wrt13upgN7LaZ03wv/Yfr4",
    "SessionToken": "IQoJb3JpZ2luX2VjEDwaCXVzLWVhc3QtMSJGMEQICIM/Fj67IzZfuurvo/IsWdncG8xGMI5QRTT+wjGSPbObAIA87LatDubGzSMnaDS1iWIp8cNk/OQ61qzEE17466YBrSqmAgi1/////////8BEAAADdk5MjM4MjQ1MDcyOCIMia6gOGaPrcutGTR2Kvob1dkmZvohGLSgYsQ0q+7o9y3l2WYkk0whkhJZ3b6fJon4pNy063SWEwEK36BuiLMQK14uuWUY3FPKQ83UblJBugytwvraQ5QJiDkcyLwVT6DZe3qa+nR1cLOKHXqCAXp9gRw6h1cZb0+lcda/noxhY9XPCIMi5BtNfvM7SzL/whhyk55yyH+3TXnX1iXlKLwCAg+cs3EnCeykevZHG4SuZsTgpoICtzbP6Lwr7Y/ewbKONZc66iM2Ib2TveeJFnT4UXnB/qdPncQl0LHF/CONJiz1As0boK/oKuEsUId8EAdeCk7kyVDkh87u8R3TIGz/yRuQ3HxMG5KTCV18qyBjqeAbcKZTHhkpZCcFKIIwRSu02NiUpXJ8hIFYyQ0g2vuHbnL7ZIC2iW/5f08c/9quKRsDPU3MlJ1ZIm27wDpDGJusqUy5FCv1hDUazYzvZalBYXht2e9PU1aQWBC/coZrbbUoU3e65/uykrIMIG2WfrzYx4lGIWe8D0wuaV6VawQg1BmXQMj2aoMlMGfPxVl1UyoRX16XSUiNmzv03kRz",
    "Expiration": "2024-05-26T04:25:09+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROA60DU2PQUPUHNSKBU:s3-write-session",
    "Arn": "arn:aws:sts::992382450728:assumed-role/s3-write-role/s3-write-session"
  }
}
[ec2-user@ip-10-0-0-151 ~]$ aws s3 ls s3://my-bucket-dev004
2024-05-26 03:27:56      44511 4 - AWS Uso de roles.pdf
[ec2-user@ip-10-0-0-151 ~]$ touch prueba.txt
[ec2-user@ip-10-0-0-151 ~]$ aws s3 cp prueba.txt s3://my-bucket-dev004
upload: ./prueba.txt to s3://my-bucket-dev004/prueba.txt
[ec2-user@ip-10-0-0-151 ~]$
```

Finalmente validamos que el usuario asumió el rol y verificamos la escritura en el bucket

# Verificar la escritura en el bucket

```
aws s3 cp prueba.txt s3://my-bucket-dev004
```

```
ec2-user@ip-10-0-0-151 ~$ aws iam update-assume-role-policy --role-name s3-write-role --policy-document file:///trust-policy.json
[ec2-user@ip-10-0-0-151 ~]$ aws configure --profile s3-support
AWS Access Key ID [*****M75H]: AKIA60DU2PQUKUQOM75H
AWS Secret Access Key [*****N8A4]: D/LaFwsjUYZn/deU//uEd8KMMuAzlexoNJ/CN8A4
Default region name [us-east-1]:
Default output format [None]:
[ec2-user@ip-10-0-0-151 ~]$ aws sts assume-role --role-arn arn:aws:iam::992382450728:role/s3-write-role --role-session-name s3-write-session --profile s3-support
{
  "Credentials": {
    "AccessKeyId": "ASIA60DU2PQUCRBBU05",
    "SecretAccessKey": "m4T0AbXan0N5t20fP0wrt13upgN7LaZ03mv/Yfr4",
    "SessionToken": "IQoJb3JpZ2luX2VjEDwaCXVzLVVhc3Q0tMSjGMEQICM/Fj67IzZfuurvo/IsWdncG0xGWI5QRTT+wjGSPbObAIA87LatDubGzSMnaDS1iWIp8cNk/OQ61qzEE17i66YBrSqmAgi1/////////8BEAAADdk5MjM4MjQ1MDcyOClMa6gOGaPrcutGTR2KvoBldkmZvohGLSgYsQ0q+7o9y3l2Wykk0whkhZ3b6fJon4pNy063SWEwEK368uILMQK14uuWUY3FPKQ83UblJ8ugytwvraQ5QJlDkcyLwVT6DZe3qa+R1cLOKHXqcaXp9gRwsh1cZb0+LcdA/noxHY9XPcIMiSBtNfvM7S2L/wHhyk55yyH+3TXnX1iXlKwCAg+cs3EnCeykevZHG4SuZsTppoICtzbP6Lwr7Y/ewbKONZc66iM2Iib2TveeJFnT4UXNb/qdPncQLOLHF/CONJiz1AcoBok/oMuEsUId8EAdecLk7kyVDkh87u8R3TIgz/yRuQ3HxMG5KTCV18qyBjqeAbckZTHhkpZCcFKIIwrsUo2NiUpXJ8hIFVYQ0g2vuHbnL7ZIC2iW/5f08c/9quKRsdPU3MLJ1ZIm27mDpDGJUsqUy5FCv1hDUazYzzvZalBYXht2e9PU1AqWBC/coZrbBUoU3e65/uykrIM1G2WfrZyX4lGIWe8D0uuaV6VaWgg1BmXQMj2aoMlMGfPxvL1UyoRX16XSUiNmVz03kRz",
    "Expiration": "2024-05-26T04:25:09+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROA60DU2PQUPUHNH8KBU:s3-write-session",
    "Arn": "arn:aws:sts::992382450728:assumed-role/s3-write-role/s3-write-session"
  }
}
[ec2-user@ip-10-0-0-151 ~]$ aws s3 ls s3://my-bucket-dev004
2024-05-26 03:27:56      44511 4 - AWS Uso de roles.pdf
[ec2-user@ip-10-0-0-151 ~]$ touch prueba.txt
[ec2-user@ip-10-0-0-151 ~]$ aws s3 cp prueba.txt s3://my-bucket-dev004
upload: ./prueba.txt to s3://my-bucket-dev004/prueba.txt
[ec2-user@ip-10-0-0-151 ~]$ aws s3 ls s3://my-bucket-dev004
2024-05-26 03:27:56      44511 4 - AWS Uso de roles.pdf
2024-05-26 03:31:04           0 prueba.txt
[ec2-user@ip-10-0-0-151 ~]$ |
```

# Listamos los archivos de nuestro bucket

```
aws s3 ls s3://my-bucket-dev004
```

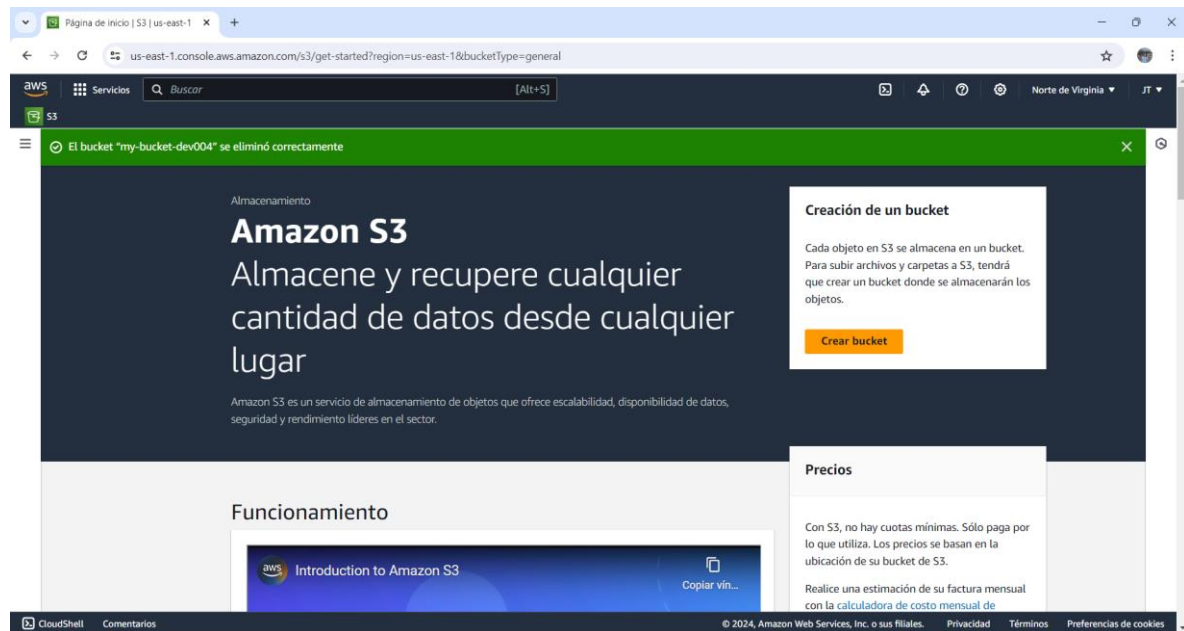
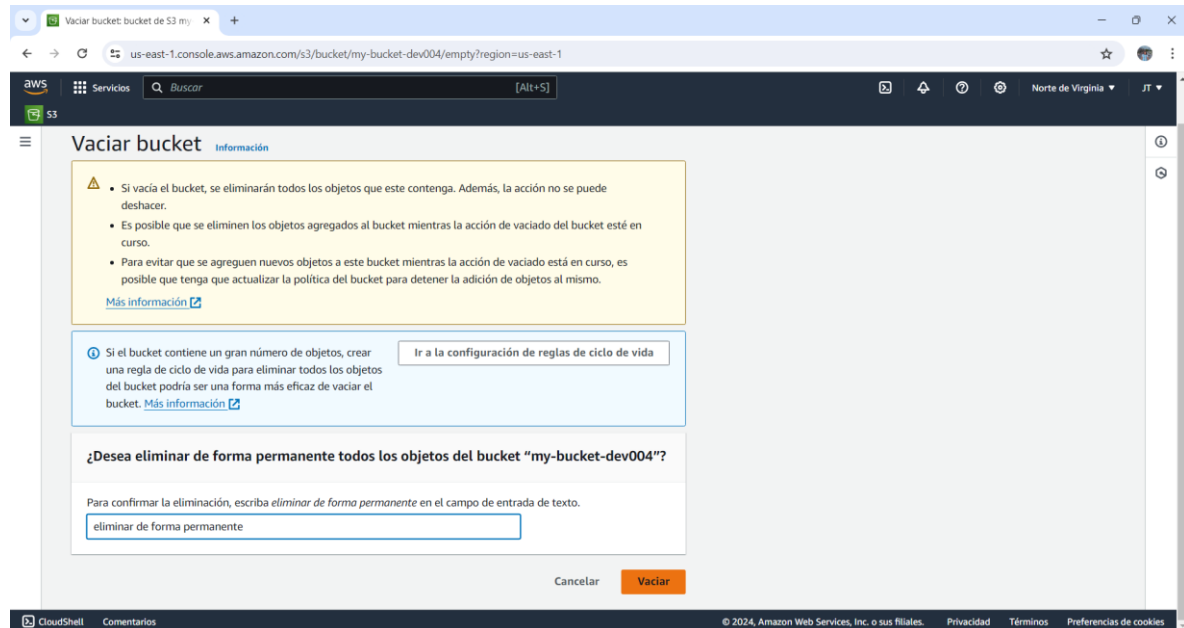
El archivo se copia correctamente, significa que la configuración del rol de IAM y los permisos de escritura en el bucket de S3 han sido establecidos correctamente.

```
ec2-user@ip-10-0-0-151 ~$ aws iam update-assume-role-policy --role-name s3-write-role --policy-document file:///trust-policy.json
[ec2-user@ip-10-0-0-151 ~]$ aws configure --profile s3-support
AWS Access Key ID [*****M75H]: AKIA60DU2PQUKUQOM75H
AWS Secret Access Key [*****N8A4]: D/LaFwsjUYZn/deU//uEd8KMMuAzlexoNJ/CN8A4
Default region name [us-east-1]:
Default output format [None]:
[ec2-user@ip-10-0-0-151 ~]$ aws sts assume-role --role-arn arn:aws:iam::992382450728:role/s3-write-role --role-session-name s3-write-session --profile s3-support
{
  "Credentials": {
    "AccessKeyId": "ASIA60DU2PQUCRBBU05",
    "SecretAccessKey": "m4T0AbXan0N5t20fP0wrt13upgN7LaZ03mv/Yfr4",
    "SessionToken": "IQoJb3JpZ2luX2VjEDwaCXVzLVVhc3Q0tMSjGMEQICM/Fj67IzZfuurvo/IsWdncG0xGWI5QRTT+wjGSPbObAIA87LatDubGzSMnaDS1iWIp8cNk/OQ61qzEE17i66YBrSqmAgi1/////////8BEAAADdk5MjM4MjQ1MDcyOClMa6gOGaPrcutGTR2KvoBldkmZvohGLSgYsQ0q+7o9y3l2Wykk0whkhZ3b6fJon4pNy063SWEwEK368uILMQK14uuWUY3FPKQ83UblJ8ugytwvraQ5QJlDkcyLwVT6DZe3qa+R1cLOKHXqcaXp9gRwsh1cZb0+LcdA/noxHY9XPcIMiSBtNfvM7S2L/wHhyk55yyH+3TXnX1iXlKwCAg+cs3EnCeykevZHG4SuZsTppoICtzbP6Lwr7Y/ewbKONZc66iM2Iib2TveeJFnT4UXNb/qdPncQLOLHF/CONJiz1AcoBok/oMuEsUId8EAdecLk7kyVDkh87u8R3TIgz/yRuQ3HxMG5KTCV18qyBjqeAbckZTHhkpZCcFKIIwrsUo2NiUpXJ8hIFVYQ0g2vuHbnL7ZIC2iW/5f08c/9quKRsdPU3MLJ1ZIm27mDpDGJUsqUy5FCv1hDUazYzzvZalBYXht2e9PU1AqWBC/coZrbBUoU3e65/uykrIM1G2WfrZyX4lGIWe8D0uuaV6VaWgg1BmXQMj2aoMlMGfPxvL1UyoRX16XSUiNmVz03kRz",
    "Expiration": "2024-05-26T04:25:09+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROA60DU2PQUPUHNH8KBU:s3-write-session",
    "Arn": "arn:aws:sts::992382450728:assumed-role/s3-write-role/s3-write-session"
  }
}
[ec2-user@ip-10-0-0-151 ~]$ aws s3 ls s3://my-bucket-dev004
2024-05-26 03:27:56      44511 4 - AWS Uso de roles.pdf
[ec2-user@ip-10-0-0-151 ~]$ touch prueba.txt
[ec2-user@ip-10-0-0-151 ~]$ aws s3 cp prueba.txt s3://my-bucket-dev004
upload: ./prueba.txt to s3://my-bucket-dev004/prueba.txt
[ec2-user@ip-10-0-0-151 ~]$ aws s3 ls s3://my-bucket-dev004
2024-05-26 03:27:56      44511 4 - AWS Uso de roles.pdf
2024-05-26 03:31:04           0 prueba.txt
[ec2-user@ip-10-0-0-151 ~]$ touch prueba2.txt
[ec2-user@ip-10-0-0-151 ~]$ aws s3 cp prueba2.txt s3://my-bucket-dev004
upload: ./prueba2.txt to s3://my-bucket-dev004/prueba2.txt
[ec2-user@ip-10-0-0-151 ~]$ aws s3 ls s3://my-bucket-dev004
2024-05-26 03:27:56      44511 4 - AWS Uso de roles.pdf
2024-05-26 03:31:04           0 prueba.txt
2024-05-26 03:46:39           0 prueba2.txt
[ec2-user@ip-10-0-0-151 ~]$ |
```



## Eliminación de los servicios

### Eliminar el Bucket



Terminar EC2

Panel de EC2

Vista global de EC2

Eventos

Console-to-Code

Vista previa

Instancias

Instancias

Tipos de instancia

Plantillas de lanzamiento

Solicitudes de spot

Savings Plans

Instancias reservadas

Alojamientos dedicados

Reservas de capacidad

Novedad

Imágenes

AMI

Catálogo de AMI

Elastic Block Store

Instancias (1/1)

Información

Conectar

Estado de la instancia

Acciones

Lanzar instancias

Buscar instancia por atributo o etiqueta (case-sensitive)

Estado de la instancia

Quitar los filtros

Detener instancia

Iniciar instancia

Reiniciar instancia

Hibernar instancia

Terminar instancia

Ver alarmas

us-east-1a

ec2-50

i-Od2ea734c274d2c3a (Server004)

Detalles

Estado y alarmas

Monitoreo

Seguridad

Redes

Almacenamiento

Etiquetas

Resumen de instancia

Información

ID de la instancia

i-Od2ea734c274d2c3a (Server004)

Dirección IPv4 pública

50.16.180.234 | dirección abierta

Direcciones IPv4 privadas

10.0.0.151

DNS de IPv4 pública

ec2-50-16-180-234.compute-1.amazonaws.com | dirección abierta

Direcciones IP elásticas

Estado de la instancia

En ejecución

Nombre DNS de IP privada (solo IPv4)

ip-10-0-0-151.ec2.internal

Nombre de IP: ip-10-0-0-151.ec2.internal

Responder al nombre DNS de recurso privado

Nombre de instancia

Tipo de instancia

CloudShell

Comentarios

© 2024, Amazon Web Services, Inc. o sus filiales.

Privacidad

Términos

Preferencias de cookies

Instancias | EC2 | us-east-1

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:instanceState=running

Instancias (1/1)

Información

Conectar

Estado de la instancia

Acciones

Lanzar instancias

Buscar instancia por atributo o etiqueta (case-sensitive)

Estado de la instancia

Quitar los filtros

Detener instancia

Iniciar instancia

Reiniciar instancia

Hibernar instancia

Terminar instancia

Ver alarmas

us-east-1a

ec2-50

i-Od2ea734c274d2c3a (Server004)

Detalles

Estado y alarmas

Monitoreo

Seguridad

Redes

Almacenamiento

Etiquetas

Resumen de instancia

Información

ID de la instancia

i-Od2ea734c274d2c3a (Server004)

Dirección IPv4 pública

50.16.180.234 | dirección abierta

Direcciones IPv4 privadas

10.0.0.151

DNS de IPv4 pública

ec2-50-16-180-234.compute-1.amazonaws.com | dirección abierta

Direcciones IP elásticas

Estado de la instancia

En ejecución

Nombre DNS de IP privada (solo IPv4)

ip-10-0-0-151.ec2.internal

Nombre de IP: ip-10-0-0-151.ec2.internal

Responder al nombre DNS de recurso privado

Nombre de instancia

Tipo de instancia

¿Terminar instancia?

En una instancia respaldada por EBS, la acción predeterminada se aplica al volumen de EBS raíz que se eliminará cuando se termine la instancia. El almacenamiento en las unidades locales se perderá.

¿Está seguro de que desea terminar estas instancias?

ID de la instancia

i-Od2ea734c274d2c3a (Server004)

Protección de terminación

Disabled

Para confirmar que desea terminar las instancias, elija el botón de terminar que aparece a continuación. Las instancias que tengan la protección de terminación habilitada no se terminarán. La terminación de la instancia no se puede deshacer.

Cancelar

Terminar

Se ha terminado correctamente i-0d2ea734c274d2c3a

### Instancias

Buscar instancia por atributo o etiqueta (case-sensitive)

Estado de la instancia = running

Name	ID de la instancia	Estado de la instancia	Tipo de inst...	Comprobación de	Estado de la ali	Zona de dispon...	DNS d
No se encontraron instancias que coincidan							

#### i-0d2ea734c274d2c3a (Server004)

Detalles Estado y alarmas Novedad Monitoreo Seguridad Redes Almacenamiento Etiquetas

**Resumen de instancia**

ID de la instancia	Dirección IPv4 pública		Direcciones IPv4 privadas
i-0d2ea734c274d2c3a (Server004)	50.16.180.234   dirección abierta		10.0.0.151
Dirección IPv6	Estado de la instancia		DNS de IPv4 pública
-	Cerrándose		ec2-50-16-180-234.compute-1.amazonaws.com   dirección abierta
Tipo de nombre de anfitrión	Nombre DNS de IP privada (solo IPv4)		Direcciones IP elásticas
Nombre de IP: ip-10-0-0-151.ec2.internal	ip-10-0-0-151.ec2.internal		
Responder al nombre DNS de recurso privado	Tipo de instancia		

## Eliminar Rol

### Roles

Eliminar Crear rol

Un rol de IAM es una identidad que se puede crear y que tiene permisos específicos con credenciales que son válidas por periodos cortos. Los roles pueden ser asumidos por entidades de confianza.

Nombre del rol	Entidades de confianza	Última actividad
<input type="checkbox"/> AWSServiceRoleForSupport	Servicio de AWS: support (Rol vincu...	-
<input type="checkbox"/> AWSServiceRoleForTrustedAdvisor	Servicio de AWS: trustedadvisor (Rol...	-
<input checked="" type="checkbox"/> s3-write-role	Cuenta: 992382450728	-

#### Roles Anywhere

Administrar

Autentique las cargas de trabajo que no son de AWS y proporcione acceso seguro a los servicios de AWS.

Obtenga acceso a AWS a partir de las cargas de trabajo que no son de AWS

Opere las cargas de trabajo que no son de AWS mediante la misma estrategia de autenticación y

Estándar X.509

Utilice su propia infraestructura de PKI existente o AWS Certificate Manager Private Certificate Authority para autenticar identidades.

Credenciales temporales

Utilice las credenciales temporales fácilmente y aproveche la seguridad mejorada que proporcionan.

Eliminar usuario

