



# 56°

**Lab - AWS re/Start**

**Actividad: Trabajo con  
Amazon S3**



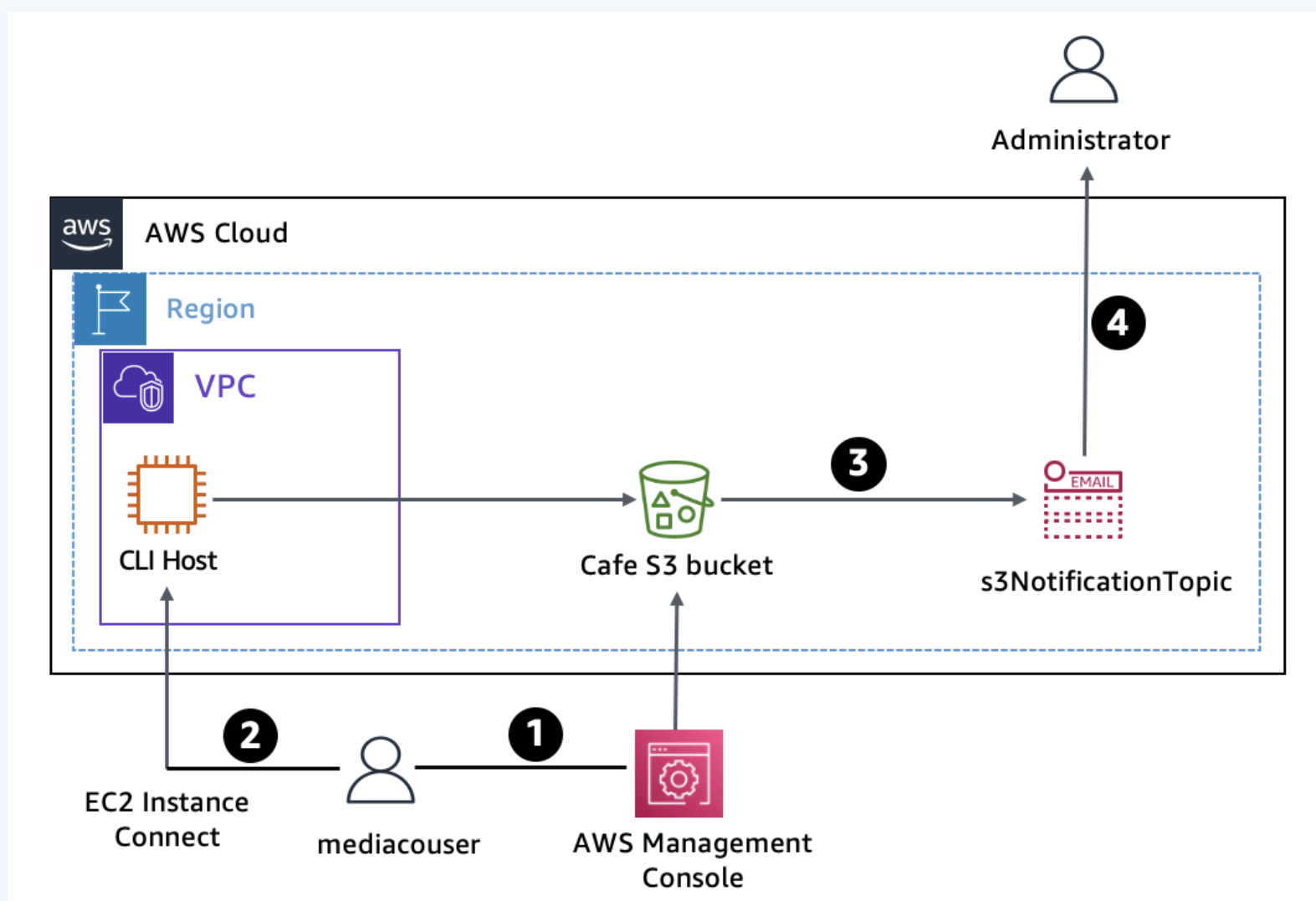
## Tarea 01



# Interactuando con Amazon S3

Los objetivos son:

- Utilice los comandos de la CLI de AWS s3api y s3 para crear y configurar un bucket de S3.
- Verificar los permisos de escritura de un usuario en un bucket de S3.
- Configurar la notificación de eventos en un bucket de S3.



# Tarea 01



Empezamos creando el bucket en AWS CLI:

```
[ec2-user@ip-10-200-0-171 ~]$ aws configure
AWS Access Key ID [*****Czy0]: AKIA6ODU5F3TU4UOMI5H
AWS Secret Access Key [*****MI5H]: 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
Default region name [us-west-2]: us-west-2
Default output format [json]: json
[ec2-user@ip-10-200-0-171 ~]$ aws s3 mb s3://cafe-mrvlab2303 --region 'us-west-2'
make_bucket: cafe-mrvlab2303
[ec2-user@ip-10-200-0-171 ~]$
```

Y cargamos las imágenes en este:

```
[ec2-user@ip-10-200-0-171 ~]$ aws s3 sync ~/initial-images/ s3://cafe-mrvlab2303/images
upload: initial-images/Donuts.jpg to s3://cafe-mrvlab2303/images/Donuts.jpg
upload: initial-images/Cup-of-Hot-Chocolate.jpg to s3://cafe-mrvlab2303/images/Cup-of-Hot-Chocolate.jpg
upload: initial-images/Strawberry-Tarts.jpg to s3://cafe-mrvlab2303/images/Strawberry-Tarts.jpg
[ec2-user@ip-10-200-0-171 ~]$ aws s3 ls s3://cafe-mrvlab2303/images/ --human-readable --summarize
2024-03-07 00:09:31    308.7 KiB Cup-of-Hot-Chocolate.jpg
2024-03-07 00:09:31    371.8 KiB Donuts.jpg
2024-03-07 00:09:31    468.0 KiB Strawberry-Tarts.jpg

Total Objects: 3
    Total Size: 1.1 MiB
[ec2-user@ip-10-200-0-171 ~]$
```

Haciendo una revisión de las políticas asignadas al usuario *mediacouser* en AWS IAM:

The screenshot displays two AWS IAM policies in the console. The top policy is 'IAMUserChangePassword', which is AWS managed and belongs to the 'mediaco' group. It provides the ability for an IAM user to change their own password. The bottom policy is 'mediaCoPolicy', which is a customer inline policy also belonging to the 'mediaco' group. It grants permissions for listing buckets and getting bucket locations in S3, as well as getting the account password policy.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:ChangePassword"
8       ],
9       "Resource": [
10        "arn:aws:iam::*:user/${aws:username}"
11      ]
12    },
13    {
14      "Effect": "Allow",
15      "Action": [
16        "iam:GetAccountPasswordPolicy"
17      ],
18      "Resource": "*"
19    }
20  ]
}
```

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "s3:ListAllMyBuckets",
7         "s3:GetBucketLocation"
8       ],
9       "Resource": [
10        "arn:aws:s3::*"
11      ],
12      "Effect": "Allow",
13      "Sid": "AllowGroupToSeeBucketListInTheConsole"
14    },
15    {
16      "Action": [
17        "s3:ListBucket"
18      ],
19      "Resource": [
20        "arn:aws:s3:::cafe-*",

```

# Tarea 01



También, creamos un access/secret key a este usuario:

Retrieve access keys Info

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key

AKIA6ODU5F3T26KX7AZX

Secret access key

NnRjIO9Iuycv+vv66eGLyWwDQAIrVzNK4y3xnI [Hide](#)

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Download .csv file

Done

Nos logeamos como dicho usuario, para probar los permisos

## Sign in as IAM user

Account ID (12 digits) or account alias

992382627559

IAM user name

mediacouser

Password

.....

☐ Remember this account

Sign in

Podemos cargar y eliminar objetos, pero no alterar los permisos del bucket

Amazon S3 > Buckets > [cafe-mrvlab2303](#) > images/

images/

Copy S3 URI

Objects

Properties

Objects (3) Info

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Show versions

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	Donuts.jpg	jpg	March 6, 2024, 19:09:31 (UTC-05:00)	371.8 KB	Standard
<input type="checkbox"/>	github.png	png	March 6, 2024, 19:17:50 (UTC-05:00)	16.5 KB	Standard
<input type="checkbox"/>	Strawberry-Tarts.jpg	jpg	March 6, 2024, 19:09:31 (UTC-05:00)	468.0 KB	Standard

Amazon S3 > Buckets > [cafe-mrvlab2303](#)

cafe-mrvlab2303 Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

Insufficient permissions

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

You don't have permission to view the Block public access (bucket settings) configuration

You need s3:GetAccountPublicAccessBlock to view the Block public access (bucket settings) configuration. [Learn more about Identity and access management in Amazon S3](#)

► API response

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

You don't have permission to get bucket policy

You or your AWS administrator must update your IAM permissions to allow s3:GetBucketPolicy. After you obtain the necessary permission, refresh the page. [Learn more about Identity and access management in Amazon S3](#)

# Tarea 01



Ahora, vamos a configurar la notificación según algún evento en el bucket de S3

Amazon SNS > Topics > Create topic

Create topic

Details

Type [Info](#)

Topic type cannot be modified after topic is created

☐ FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS

☒ Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Name

s3NotificationTopic

Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (\_).

Display name - optional [Info](#)

To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.

My Topic

Maximum 100 characters.

▼ Access policy - optional [Info](#)

This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

JSON editor

```
2  "Version": "2008-10-17",
3  "Id": "S3PublishPolicy",
4  "Statement": [
5    {
6      "Sid": "AllowPublishFromS3",
7      "Effect": "Allow",
8      "Principal": {
9        "Service": "s3.amazonaws.com"
10     },
11     "Action": "SNS:Publish",
12     "Resource": "arn:aws:sns:us-west-2:992382627559:s3NotificationTopic",
13     "Condition": {
14       "ArnLike": {
15         "aws:SourceArn": "arn:aws:s3:*:*:cafe-mrvlab2303"
```

Amazon SNS > Subscriptions > Create subscription

Create subscription

Details

Topic ARN

arn:aws:sns:us-west-2:992382627559:s3NotificationTopic

Protocol

The type of endpoint to subscribe

Email

Endpoint

An email address that can receive notifications from Amazon SNS.

millonesmam@gmail.com

After your subscription is created, you must confirm it. [Info](#)

Cada que se cree o elimine un objeto -> evento

```
aws
Services
Search [Alt+S]

{
  "TopicConfigurations": [
    {
      "TopicArn": "arn:aws:sns:us-west-2:992382627559:s3NotificationTopic",
      "Events": ["s3:ObjectCreated:*","s3:ObjectRemoved:*"],
      "Filter": {
        "Key": {
          "FilterRules": [
            {
              "Name": "prefix",
              "Value": "images/"
            }
          ]
        }
      }
    }
  ]
}
```

```
[ec2-user@ip-10-200-0-171 ~]$ aws s3api put-bucket-notification-configuration --bucket cafe-mrvlab2303 --notification-configuration file:///s3EventNotification.json
[ec2-user@ip-10-200-0-171 ~]$
```

```
aws Services Search [Alt+S]
[ec2-user@ip-10-200-0-171 ~]$ aws s3api put-object --bucket cafe-mrvlab2303 --key images/Caramel-Delight.jpg --body ~/new-images/Caramel-Delight.jpg
{
  "ETag": "\"31ac30da619244b0ce786f106e4f3df7\"",
  "ServerSideEncryption": "AES256"
}

[ec2-user@ip-10-200-0-171 ~]$
[ec2-user@ip-10-200-0-171 ~]$ aws s3api put-object --bucket cafe-mrvlab2303 --key images/Caramel-Delight.jpg --body ~/new-images/Caramel-Delight.jpg
{
  "ETag": "\"31ac30da619244b0ce786f106e4f3df7\"",
  "ServerSideEncryption": "AES256"
}

[ec2-user@ip-10-200-0-171 ~]$ aws s3api get-object --bucket cafe-mrvlab2303 --key images/Donuts.jpg Donuts.jpg
{
  "AcceptRanges": "bytes",
  "ContentType": "image/jpeg",
  "LastModified": "Thu, 07 Mar 2024 00:09:31 GMT",
  "ContentLength": 380753,
  "ETag": "\"405b0bcc53cb5ab713c967dc1422b4f4\"",
  "ServerSideEncryption": "AES256",
  "Metadata": {}
}

[ec2-user@ip-10-200-0-171 ~]$ aws s3api delete-object --bucket cafe-mrvlab2303 --key images/Strawberry-Tarts.jpg
[ec2-user@ip-10-200-0-171 ~]$
```

cuando se crea un objeto

The image is a screenshot of an email notification from AWS. At the top, the email is titled 'Amazon S3 Notification' with a status 'Recibidos'. The main heading of the email is 'cuando se eliminó'. Below this, the sender is identified as 'AWS Notifications' from 'sns.amazonaws.com', with a timestamp of '19:39 (hace 0 minutos)'. The email is addressed 'para mí'. The body of the email contains a JSON record of an S3 event. The event is 'ObjectRemoved: Delete' for the file 'images/Strawberry-Tarts.jpg' in the bucket 'cafe-mrvlab2303'. The record includes details like 'eventVersion', 'eventSource', 'awsRegion', 'eventTime', 'eventName', 'userIdentity', 'principalId', 'requestParameters', 'sourceIPAddress', 'responseElements', 's3', 's3SchemaVersion', 'configurationId', and 'key'.

```
[ec2-user@ip-10-200-0-171 ~]$ aws s3api put-object-acl --bucket cafe-mrvlab2303 --key images/Donuts.jpg --acl public-read
```

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

```
[ec2-user@ip-10-200-0-171 ~]$
```