

Datos Generales:

Nombre: Tomás Alfredo Villaseca Constantinescu

País: Chile

Fecha: 06/11/2023

Contacto: tomas.villaseca.c@gmail.com

Al final de este laboratorio, usted podrá hacer lo siguiente:

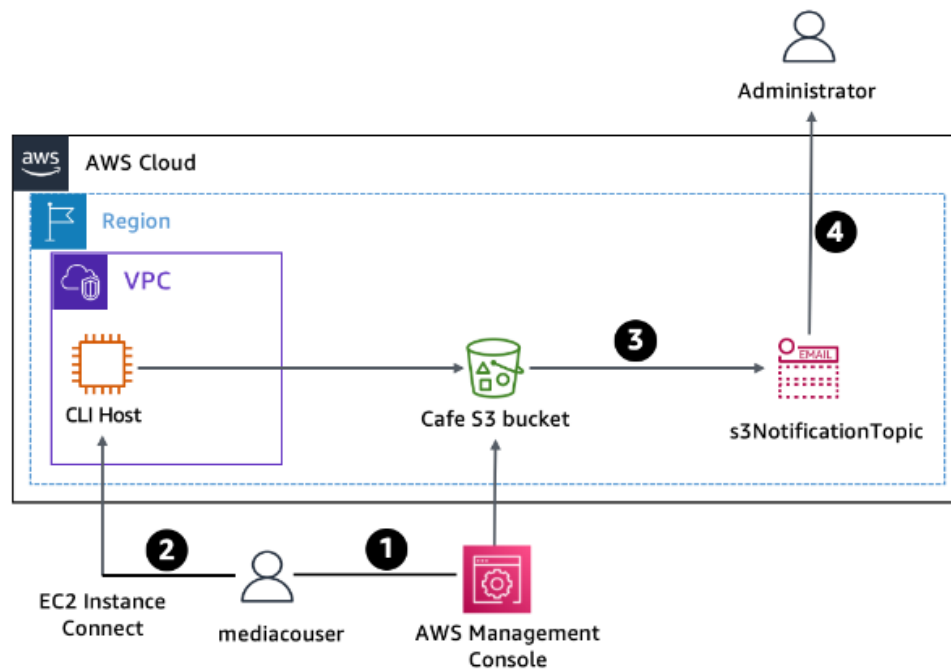
- Utilizar los comandos de la CLI de AWS s3api y s3 para crear y configurar un bucket de S3.
- Verificar los permisos de escritura de un usuario en un bucket de S3.
- Configurar la notificación de eventos en un bucket de S3.

Resumen Laboratorio:

En este laboratorio, creará y configurará un bucket de Amazon Amazon S3 para compartir imágenes con un usuario externo de una empresa de medios de comunicación (mediacouser) que ha sido contratado para proporcionar imágenes de los productos que vende la cafetería.

También se configurará el bucket S3 para que envíe automáticamente una notificación por correo electrónico al administrador cuando se modifique el contenido del bucket.

El siguiente diagrama muestra la arquitectura de componentes de la solución de compartición de archivos de Amazon S3 e ilustra su flujo de uso:



Se ha creado previamente un usuario de IAM llamado **mediacouser**, que representa a un usuario externo en una compañía de medios de comunicación, con los permisos de Amazon S3 adecuados para permitir al usuario añadir, cambiar o eliminar imágenes del bucket.

1. Cuando hay nuevas imágenes de productos disponibles o cuando deben actualizarse las existentes, un representante de la compañía de medios inicia sesión en la consola de administración de AWS como **mediacouser** para cargar, cambiar o eliminar el contenido del bucket.
2. Como alternativa, el mediador puede utilizar la interfaz de línea de comandos de AWS (CLI de AWS) para cambiar el contenido del bucket de S3.
3. Cuando Amazon S3 detecta un cambio en el contenido del bucket, publica una notificación por correo electrónico en el tema **s3NotificationTopic** de Amazon Simple Notification Service (Amazon SNS).
4. El administrador suscrito al tema SNS **s3NotificationTopic** recibe un mensaje de correo electrónico con los detalles de los cambios en el contenido del bucket.

Tarea 1: Conectarse a la instancia CLI Host

Tarea 1.1 – Conectarse a la instancia CLI Host

Paso 1: EC2 → Instances → CLI Host → Connect → EC2 Instance Connect

✓	Name ✎	Instance ID	Instance state
✓	CLI Host	i-0392d5afbb3e3fetc	Running

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID
i-0392d5afbb3e3fetc (CLI Host)

Connection Type

☒ Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

☐ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address
35.84.212.23

User name
Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.

Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel

Connect

```
#_
~\-  ####
~~\-  #####\
~~\  ####|
~~\  \#/
~~\  V~' '->
~~~
~~~.
~~/_/ '->
  /m/'

Amazon Linux 2
AL2 End of Life is 2025-06-30.

A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-200-0-231 ~]$
```

Tarea 1.2 – Configurar la CLI de AWS

Paso 1: Configurar la CLI de AWS usando el comando **aws configure**:

- Puede encontrar las credenciales en Details del laboratorio.

```
[ec2-user@ip-10-200-0-231 ~]$ aws configure
AWS Access Key ID [None]: AKIAYHRP5PP3D6VSBDAQ
AWS Secret Access Key [None]: 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
Default region name [None]: us-west-2
Default output format [None]: json
[ec2-user@ip-10-200-0-231 ~]$
```

Tarea 2: Crear e Iniciar el S3 Share Bucket

En esta tarea, se utilizará la CLI de AWS para crear el S3 Share Bucket y cargar algunas imágenes.

Paso 1: Para crear un Bucket S3, ejecutar el siguiente comando:

- Reemplazar <café-xxxxnn> por Bucket Name.

```
aws s3 mb s3://<cafe-xxxxnn> --region 'us-west-2'
```

```
[ec2-user@ip-10-200-0-231 ~]$ aws s3 mb s3://labbucket222444 --region 'us-west-2'
make_bucket: labbucket222444
[ec2-user@ip-10-200-0-231 ~]$
```

- BucketName → labbucket222444

Paso 2: Para cargar imágenes en el bucket S3, ejecutar el siguiente comando:

- Reemplazar <café-xxxxnn> por BucketName

```
aws s3 sync ~/initial-images/ s3://<cafe-xxxxnn>/images
```

```
[ec2-user@ip-10-200-0-231 ~]$ aws s3 sync ~/initial-images/ s3://labbucket222444/images
upload: initial-images/Cup-of-Hot-Chocolate.jpg to s3://labbucket222444/images/Cup-of-Hot-Chocolate.jpg
upload: initial-images/Strawberry-Tarts.jpg to s3://labbucket222444/images/Strawberry-Tarts.jpg
upload: initial-images/Donuts.jpg to s3://labbucket222444/images/Donuts.jpg
[ec2-user@ip-10-200-0-231 ~]$
```

Paso 3: Para verificar que los archivos están sincronizados al Bucket S3, ejecutar el siguiente comando:

- Reemplazar <café-xxxxnn> por BucketName

```
aws s3 ls s3://<café-xxxxnn>/images/ --human-readable --summarize
```

```
[ec2-user@ip-10-200-0-231 ~]$ aws s3 ls s3://labbucket222444/images/ --human-readable --summarize
2023-11-06 22:57:21 308.7 KiB Cup-of-Hot-Chocolate.jpg
2023-11-06 22:57:21 371.8 KiB Donuts.jpg
2023-11-06 22:57:21 468.0 KiB Strawberry-Tarts.jpg

Total Objects: 3
Total Size: 1.1 MiB
[ec2-user@ip-10-200-0-231 ~]$
```

Tarea 3: Revisar el IAM Group y permisos de usuario

En esta tarea, revisará los permisos asignados al grupo de usuarios IAM de mediaco.

Este grupo fue creado para proporcionar una manera para que los usuarios de la empresa de medios de comunicación utilicen la consola de administración de AWS o la CLI de AWS para cargar y modificar imágenes en el cubo compartido de S3. La creación del grupo facilita la gestión de los permisos individuales de los usuarios.





También revisará los permisos heredados por el usuario mediacouser que forma parte del grupo.

Tarea 3.1 – Revisar el IAM Group mediaco

Paso 1: IAM → User Groups → mediaco

<input type="checkbox"/>	Group name
<input checked="" type="checkbox"/>	mediaco

Paso 2: IAM → User Groups → mediaco → permissions

<input type="checkbox"/>	Policy name 	Type
<input type="checkbox"/>	  IAMUserChangePassword	AWS managed
<input type="checkbox"/>	 mediaCoPolicy	Customer inline

- IAMUserChangePassword → Expandir

```

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 ]

```

- MediaCoPolicy → Expandir

AllowGroupToSeeBucketListInTheConsole → Define permisos que permiten a los usuarios utilizar la consola de S3 para ver la lista de Buckets S3 en la cuenta.

AllowRootLevelListingOfTheBucket → Define permisos que permiten a los usuarios utilizar la consola de S3 para ver la lista de objetos en los Buckets S3.

AllowUserSpecificActionsOnlyInTheSpecificPrefix → Define permisos que especifican las acciones que un usuario puede realizar en los objetos en la carpeta /café-**images/*. (Las acciones principales son GetObject, PutObject, y DeleteObject).

```

"Action": [
  "s3:ListAllMyBuckets",
  "s3:GetBucketLocation"
],
"Resource": [
  "arn:aws:s3:::*"
],
"Effect": "Allow",
"Sid": "AllowGroupToSeeBucketListInTheConsole"

```

```

"Action": [
  "s3:PutObject",
  "s3:GetObject",
  "s3:GetObjectVersion",
  "s3:DeleteObject",
  "s3:DeleteObjectVersion"
],
"Resource": "arn:aws:s3:::café-*/images/*",
"Effect": "Allow",
"Sid": "AllowUserSpecificActionsOnlyInTheSpecificPrefix"

```


```

"Action": [
  "s3:ListBucket"
],
"Resource": [
  "arn:aws:s3:::café-*",
  "arn:aws:s3:::café-*/*"
],
"Effect": "Allow",
"Sid": "AllowRootLevelListingOfTheBucket"

```


Tarea 3.2 – Revisar el IAM User mediacouser

Paso 1: IAM → Users →mediacouser → Permissions

<input type="checkbox"/> User name	<input checked="" type="checkbox"/> Policy name ↗
<input checked="" type="checkbox"/> mediacouser	<input checked="" type="checkbox"/> <input type="checkbox"/>  IAMUserChangePassword
<ul style="list-style-type: none">• IAMUserChangePassword• mediaCoPolicy	<input checked="" type="checkbox"/> <input type="checkbox"/> mediaCoPolicy

Estas políticas se asignan al IAM Group mediaco revisado en la tarea anterior.

Paso 2: IAM → Users →mediacouser → Groups

- mediacouser es miembro de IAM Group mediaco

User groups membership (1/1) <small>A user group is a collection of IAM users. Use groups to</small>	
<input checked="" type="checkbox"/> Group name ↗	
<input checked="" type="checkbox"/> mediaco	

Paso 3: IAM → Users →mediacouser → Security credentials

- Access key → Create access key

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#) [↗](#)

Create access key

- Command Line Interface (CLI)

Use case


- ☒ **Command Line Interface (CLI)**
You plan to use this access key to enable the AWS CLI to access your AWS account.

- Seleccionar casilla: “I understand the above recommendation and want to proceed to create an access key”

☒ I understand the above recommendation and want to proceed to create an access key.

- Download .csv file


Download .csv file

 mediacouser_accessKeys

Paso 4: IAM → Users → mediacouser → Security credentials

- Console sign-in link → <https://565962439670.signin.aws.amazon.com/console>

Console sign-in link

 <https://565962439670.signin.aws.amazon.com/console>

Tarea 3.3 – Probar los permisos de mediacouser

En esta tarea, se probarán los permisos revisados anteriormente realizando las operaciones de visualización, carga y eliminación en el contenido de la carpeta de imágenes del S3 Share Bucket.

Estas acciones son los casos de uso que se espera que el usuario externo de la compañía de medios realice en el bucket. Además, se probará el caso de uso no autorizado, en el que el usuario externo intenta cambiar los permisos del bucket.

Paso 1: Abrir una pestaña incognito en el navegador.

- Pegar Console sign-in link.
- IAM User Name = mediacouser
- Password = Training!

Sign in as IAM user

Account ID (12 digits) or account alias

565962439670

IAM user name

mediacouser

Password

.....

Paso 2: S3 → labbucket222444

	Nombre	Región de AWS
	labbucket222444	EE. UU. Oeste (Oregón) us-west-2

<input checked="" type="checkbox"/>	Name	Type
<input checked="" type="checkbox"/>	images/	Folder

- Images → Donuts.jpg → Open

<input checked="" type="checkbox"/>	Donuts.jpg	jpg
-------------------------------------	------------	-----

- Images → Upload → Add files

Upload

Add files



<input checked="" type="checkbox"/>	pngwing.com.png	png
-------------------------------------	-----------------	-----

- Images → Cup-of-Hot-Chocolate.jpg → Delete

<input checked="" type="checkbox"/>	Cup-of-Hot-Chocolate.jpg	jpg
-------------------------------------	--------------------------	-----

To confirm deletion, type *permanently delete* in the text input field.

permanently delete

✔ Successfully deleted objects

View details below.

Paso 3: S3 → BucketName → Permissions

- Insufficient permissions

labbucket222444 [Información](#)

Objetos | Propiedades | **Permisos** | Métricas | Administración | Puntos de acceso

Información general sobre los permisos

Acceso

✖ Permisos insuficientes

Tarea 4: Configuración de notificaciones de eventos en el S3 Share Bucket

En esta tarea, se configurará el S3 Share Bucket para generar una notificación de evento a un SNS topic siempre que cambie el contenido del bucket.

Tarea 4.1 – Crear y configurar el SNS Topic S3NotificationTopic

Paso 1: SNS → Topics → Create Topic

- Standard

- **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

Name

S3NotificationTopic

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

Paso 2: SNS → Topics → S3NotificationTopic

- Topic ARN → arn:aws:sns:us-west-2:565962439670:S3NotificationTopic
- Access Policy → Edit → Expandir → Reemplazar contenido del editor JSON por la política entregada por el laboratorio.

```
1 {
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-2:565962439670:S3NotificationTopic",
13      "Condition": {
14        "ArnLike": {
15          "aws:SourceArn": "arn:aws:s3:*:*:labbucket222444"
```

Paso 3: SNS → Topics → S3NotificationTopic → Subscriptions

- Create subscription

No subscriptions found

Create subscription

- Topic ARN → S3NotificationTopic
- Protocol → Email
- Endpoint = tomas.villaseca.c@gmail.com

Topic ARN

arn:aws:sns:us-west-2:565962439670:S3NotificationTopic

Protocol

The type of endpoint to subscribe

Email

Endpoint

An email address that can receive notifications from Amazon SNS.

tomas.villaseca.c@gmail.com

Paso 4: Revisar correo electrónico → Confirmar subscripción

AWS Notifications

para mí ▼

You have chosen to subscribe to the topic:

arn:aws:sns:us-west-2:565962439670:S3NotificationTopic

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):

[Confirm subscription](#)



Simple Notification Service

Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:

arn:aws:sns:us-west-2:565962439670:S3NotificationTopic:db190b2f-1b59-4db6-a994-42577ed688b6

If it was not your intention to subscribe, [click here to unsubscribe](#).

Tarea 4.2 – Añadir una configuración de notificación de eventos al S3 Bucket

En esta tarea, se creará un archivo de configuración de notificaciones de eventos que identifica los eventos que publicará Amazon S3 y el destino de Topics al que Amazon S3 enviará las notificaciones de eventos.

Paso 1: En el terminal de CLI Host, utilice nano para editar el archivo “S3EventNotification.json”.

- Reemplazar el contenido por el JSON entregado por el laboratorio.
- <ARN of S3NotificationTopic> por Topic ARN copiado anteriormente.

```
{
  "TopicConfigurations": [
    {
      "TopicArn": "arn:aws:sns:us-west-2:565962439670:S3NotificationTopic",
      "Events": [
        "s3:ObjectCreated:*",
        "s3:ObjectRemoved:*"
      ],
      "Filter": {
        "Key": {
          "FilterRules": [
            {
              "Name": "prefix",
              "Value": "images/"
            }
          ]
        }
      }
    }
  ]
}
```

Paso 2: Para asociar el archivo de configuración de eventos con el S3 Share Bucket, ejecutar el siguiente comando:

- Reemplazar <café-xxxnnn> por Bucket Name.

```
aws s3api put-bucket-notification-configuration --bucket <cafe-xxxxxx> --notification-configuration
file://s3EventNotification.json
```

```
ec2-user@ip-10-200-0-231 ~]$ aws s3api put-bucket-notification-configuration --bucket labbucket222444 --notification-configuration file:///s3EventNotification.json
ec2-user@ip-10-200-0-231 ~|$
```

Paso 3: Revisar correo electrónico → Notificación SNS

```
{ "Service": "Amazon S3", "Event": "s3:TestEvent", "Time": "2023-11-06T23:51:31.053Z", "Bucket": "labbucket222444", "RequestId":
```

Tarea 5: Probar las notificaciones de eventos de S3 Share Bucket

En esta tarea, se probará la configuración de la notificación de eventos del S3 Share Bucket realizando los casos de uso que mediacouser espera realizar en el bucket.

Estas acciones incluyen la introducción y eliminación de objetos del bucket, que envían notificaciones por correo electrónico.

También se probará una operación no autorizada para verificar que se rechaza.

Paso 1: Configurar la CLI de AWS con las credenciales de mediacouser.

- Access Key ID → Valor de Access Key ID de mediacouser_accessKeys.csv
- Secret Access Key → Valor de Secret Access Key de mediacouser_accessKeys.csv
- Default region name → us-west-2
- Default output format → json

```
[ec2-user@ip-10-200-0-231 ~]$ aws configure
AWS Access Key ID [*****AJHB]: AKIAYHRP5PP3CNTRKAJHB
AWS Secret Access Key [*****Evxm]: TCy2Ftes+gfPhOIvw/6blzKPl9Jft1PBx/HvEvxm
Default region name [us-west-2]: us-west-2
Default output format [json]: json
[ec2-user@ip-10-200-0-231 ~]$
```

Paso 2: Testear la acción **PUT** cargando el archivo Caramel-Delight.jpg desde la carpeta new-images en el CLI Host, ejecutar el siguiente comando:

- Reemplazar <café-xxxxnn> por Bucket Name.

```
aws s3api put-object --bucket <cafe-xxxxnn> --key images/Caramel-Delight.jpg --body ~/new-images/Caramel-Delight.jpg
```

```
[ec2-user@ip-10-200-0-231 ~]$ aws s3api put-object --bucket labbucket222444
{
  "ETag": "\"31ac30da619244b0ce786f106e4f3df7\"",
  "ServerSideEncryption": "AES256"
}
[ec2-user@ip-10-200-0-231 ~]$
```

- ETag → "\"31ac30da619244b0ce786f106e4f3df7\""

Paso 3: Revisar correo electrónico → Notificación SNS

```
{
  "Records": [
    {
      "eventVersion": "2.1",
      "eventSource": "aws:s3",
      "awsRegion": "us-west-2",
      "eventTime": "2023-11-06T23:55:53.457Z",
      "eventName": "ObjectCreated:Put",
      "sourceIPAddress": "35.84.212.23",
      "responseElements": {
        "x-amz-request-id": "PC55F1T9AB8N6F93",
        "x-amz-id-2": "NrstzREHwoq7nRVvZ3eZbt8l/wj6fKlkoy1ICs"
      },
      "s3SchemaVersion": "1.0",
      "configurationId": "OGY4N2MwOGEtMDM1Zi00OTljLWJhOGMtNDhYjdiMj1",
      "bucket": {
        "name": "labbucket222444",
        "ownerIdentity": {
          "key": "images/Caramel-Delight.jpg",
          "size": 239148,
          "eTag": "\"31ac30da619244b0ce786f106e4f3df7\"",
          "sequencer": "0065497D0968C67931"
        }
      }
    }
  ]
}
```

Paso 4: Testear la acción **GET** obteniendo el objeto images/Donut.jpg desde el Bucket S3, ejecutar el comando:

- Reemplazar <café-xxxxnnn> por Bucket Name.

```
aws s3api get-object --bucket <cafe-xxxxnnn> --key images/Donuts.jpg Donuts.jpg
```

```
[ec2-user@ip-10-200-0-231 ~]$ aws s3api get-object --bucket labbucket222444 --key images/Donuts.jpg Donuts.jpg
{
  "AcceptRanges": "bytes",
  "ContentType": "image/jpeg",
  "LastModified": "Mon, 06 Nov 2023 22:57:21 GMT",
  "ContentLength": 380753,
  "ETag": "\"405b0bcc53cb5ab713c967dc1422b4f4\"",
  "ServerSideEncryption": "AES256",
  "Metadata": {}
}
[ec2-user@ip-10-200-0-231 ~]$
```

Paso 5: Revisar correo electrónico → Notificación SNS

```
{
  "Records": [
    {
      "eventVersion": "2.1",
      "eventSource": "aws:s3",
      "awsRegion": "us-west-2",
      "eventTime": "2023-11-06T23:55:53.457Z",
      "eventName": "ObjectCreated:Put",
      "sourceIPAddress": "35.84.212.23",
      "responseElements": {
        "x-amz-request-id": "PC55F1T9AB8N6F93",
        "x-amz-id-2": "NrstzREHwoq7nRVvZ3eZ"
      },
      "s3SchemaVersion": "1.0",
      "configurationId": "OGY4N2MwOGEtMDM1Zi00OTIjLWJhOGMtNDA5NDhhYjdiMjI1",
      "bucket": {
        "name": "labbucket222444",
        "ownerIdentity": {
          "principal": "arn:aws:iam::111111111111:user"
        }
      },
      "key": "images/Caramel-Delight.jpg",
      "size": 239148,
      "eTag": "31ac30da619244b0ce786f106e4f3df7",
      "sequencer": "0065497D0968C67931"
    }
  ]
}
```

Paso 6: Testear la acción **DELETE** eliminando el objeto images/Strawberry-Tarts.jpg en el Bucket S3, ejecutar el comando:

- Reemplazar <café-xxxxnnn> por Bucket Name.

```
aws s3api delete-object --bucket <cafe-xxxxnnn> --key images/Strawberry-Tarts.jpg
```

```
[ec2-user@ip-10-200-0-231 ~]$ aws s3api delete-object --bucket labbucket222444 --key images/Strawberry-Tarts.jpg
[ec2-user@ip-10-200-0-231 ~]$
```

Paso 7: Revisar correo electrónico → Notificación SNS

```
{
  "Records": [
    {
      "eventVersion": "2.1",
      "eventSource": "aws:s3",
      "awsRegion": "us-west-2",
      "eventTime": "2023-11-06T23:58:44.333Z",
      "eventName": "ObjectRemoved:Delete",
      "sourceIPAddress": "35.84.212.23",
      "responseElements": {
        "x-amz-request-id": "NH5VMZKN81C1WK8N",
        "x-amz-id-2": "MglKu48pR42xkRWOU3BVyUciVcLcBR0NZ3O+"
      },
      "s3SchemaVersion": "1.0",
      "configurationId": "OGY4N2MwOGEtMDM1Zi00OTIjLWJhOGMtNDA5NDhhYjdiMjI1",
      "bucket": {
        "name": "labbucket222444",
        "ownerIdentity": {
          "principal": "arn:aws:iam::111111111111:user"
        }
      },
      "key": "images/Strawberry-Tarts.jpg",
      "sequencer": "0065497DB450B83B49"
    }
  ]
}
```

Paso 8: Testear el cambio de permisos del objeto Donuts.jpg para que pueda ser leído públicamente, ejecutar el siguiente comando:

- Reemplazar <café-xxxxnn> por Bucket Name.

```
aws s3api put-object-acl --bucket <café-xxxxnn> --key images/Donuts.jpg --acl public-read
```

```
[ec2-user@ip-10-200-0-231 ~]$ aws s3api put-object-acl --bucket labbucket222444 --key images/Donuts.jpg --acl public-read
An error occurred (AccessDenied) when calling the PutObjectAcl operation: Access Denied
[ec2-user@ip-10-200-0-231 ~]$
```

Laboratorio Completado

