

Lab 185

Sony Etcheverne , Fidel Fernandez ,
Batten Velaíquez , Agustín Esteche

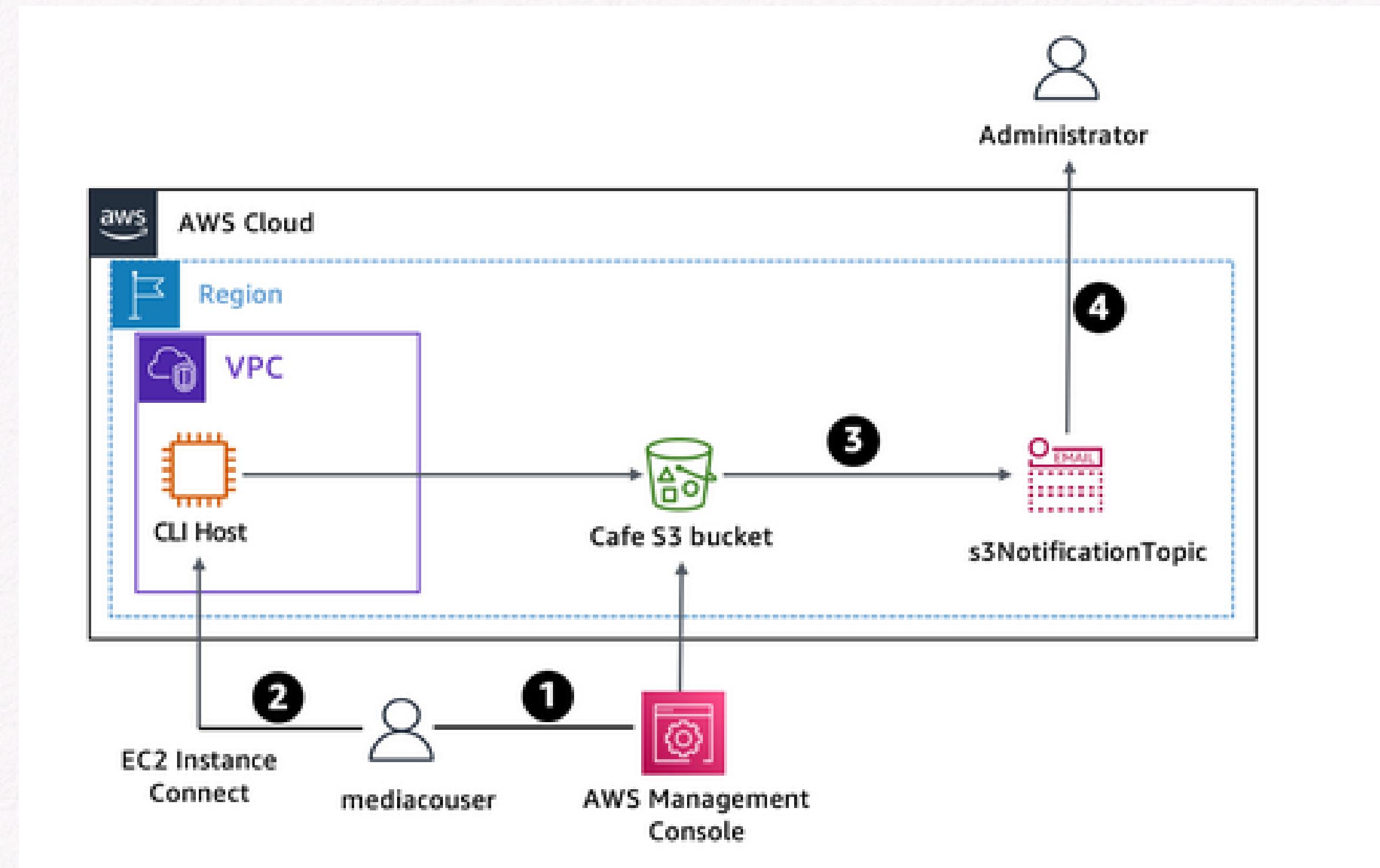




Objetivos

- Utilizar los comandos s3api y s3 de AWS CLI para crear y configurar un depósito S3.
- Verifique los permisos de escritura para un usuario en un depósito de S3.
- Configure la notificación de eventos en un depósito de S3.

Arquitectura final:





Tarea 1: Conectarse a la instancia CLI Host EC2 y configuración de AWS CLI.

Tarea 1.1: Conexión a la instancia CLI Host EC2 y configuración de AWS CLI.

En la Consola de administración de AWS, en la barra de búsqueda, ingresamos y elegimos EC2 para abrir la Consola de administración de EC2.

Tarea 1.2: Configuración de AWS CLI en la instancia del host CLI.

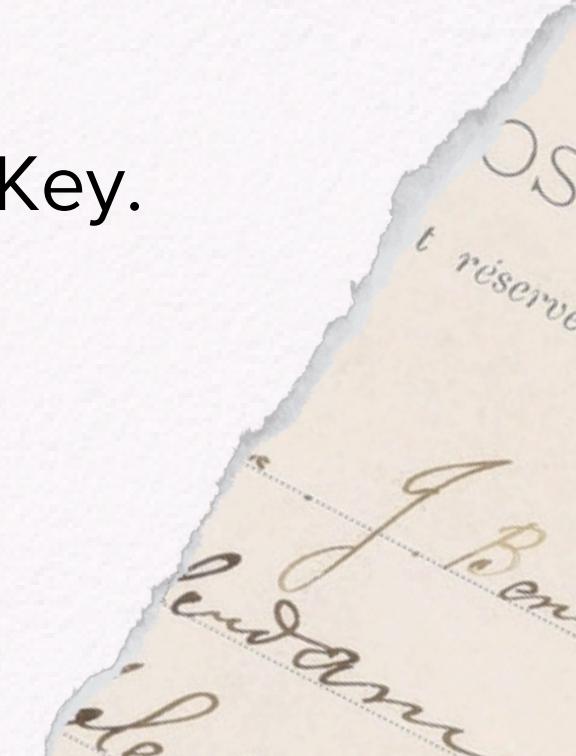
- Ingresamos aws configure en la consola y completamos la información correspondiente como se muestra a continuación:

AWS Access Key ID (ID de clave de acceso de AWS): ingrese el valor de AccessKey.

AWS Secret Access Key (Clave de acceso secreta de AWS): ingrese el valor de SecretKey.

Default region name (Nombre predeterminado de la región): ingrese us-west-2.

Default output format (Formato de resultado predeterminado): ingrese json.





Tarea 2: Creación e inicialización del bucket compartido de S3.

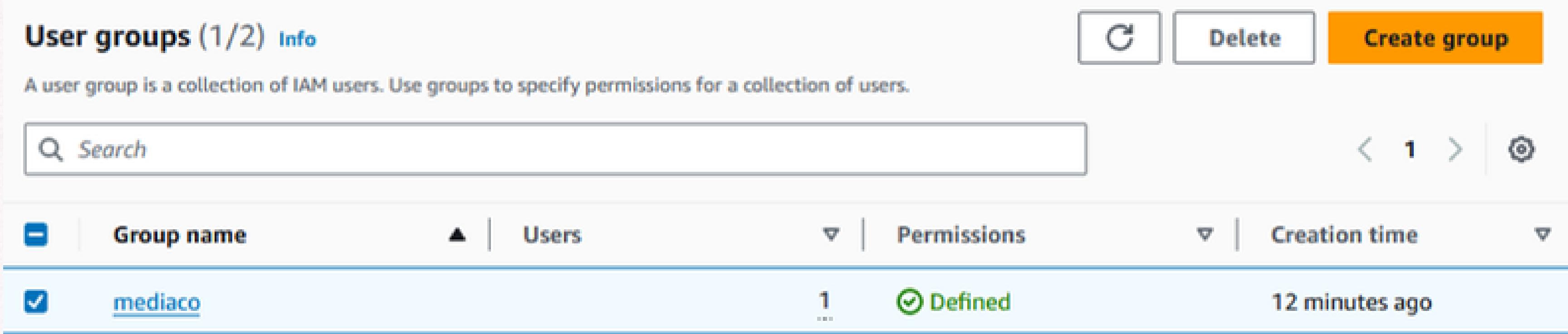
Utilizaremos la CLI de AWS para crear el bucket compartido de S3 y cargar algunas imágenes. Para hacerlo, ejecutaremos los siguientes comandos en la ventana del terminal EC2 Instance Connect.

```
[ec2-user@ip-10-200-0-232 ~]$ aws s3 mb s3://cafe-abc123 --region 'us-west-2'  
make_bucket: cafe-abc123  
[ec2-user@ip-10-200-0-232 ~]$ aws s3 sync ~/initial-images/ s3://cafe-abc123/images  
upload: initial-images/Cup-of-Hot-Chocolate.jpg to s3://cafe-abc123/images/Cup-of-Hot-Chocolate.jpg  
upload: initial-images/Strawberry-Tarts.jpg to s3://cafe-abc123/images/Strawberry-Tarts.jpg  
upload: initial-images/Donuts.jpg to s3://cafe-abc123/images/Donuts.jpg  
[ec2-user@ip-10-200-0-232 ~]$ aws s3 ls s3://cafe-abc123/images/ --human-readable --summarize  
2024-07-08 23:31:07  308.7 KiB Cup-of-Hot-Chocolate.jpg  
2024-07-08 23:31:07  371.8 KiB Donuts.jpg  
2024-07-08 23:31:07  468.0 KiB Strawberry-Tarts.jpg  
  
Total Objects: 3  
  Total Size: 1.1 MiB  
[ec2-user@ip-10-200-0-232 ~]$ █
```



Tarea 3: Revisión del grupo IAM y los permisos de usuario.

Tarea 3.1: En el panel de navegación de la izquierda, elegimos Grupos de usuarios y seleccionamos **mediaco**.



The screenshot shows the AWS IAM User Groups page. At the top, there is a header with "User groups (1/2)" and "Info" buttons, and a "Create group" button. Below the header, a search bar and navigation controls (back, forward, first, last) are present. The main table has columns: Group name, Users, Permissions, and Creation time. The "mediaco" group is listed, showing 1 user, defined permissions, and a creation time of 12 minutes ago. A blue border highlights the mediaco row.

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input checked="" type="checkbox"/>	mediaco	1 ...	Defined	12 minutes ago

Presionaremos la pestaña de Permisos y expandiremos las políticas para revisarlas.

Policy name	Type	Attached entities
IAMUserChangePassword	AWS managed	1

IAMUserChangePassword

Provides the ability for an IAM user to change their own password.

```
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.    ]  
}
```

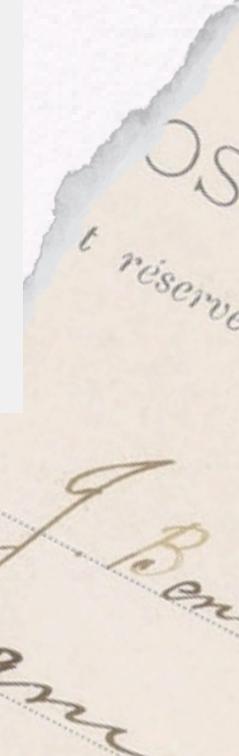
Policy name	Type	Attached entities
IAMUserChangePassword	AWS managed	1
mediaCoPolicy	Customer inline	0

mediaCoPolicy

```
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-*",  
21.             ]  
22.         }  
23.     ]  
}
```

Tarea 3.2: Revisar el usuario de IAM mediacouser

En esta sección, revisaremos las propiedades del usuario mediacouser



mediacouser Info Delete

Summary		
ARN arn:aws:lambda:449824372389:user/mediacouser	Console access Enabled without MFA	Access key 1 Create access key
Created July 08, 2024, 20:21 (UTC-03:00)	Last console sign-in Never	

Permissions Groups (1) Tags (1) Security credentials Access Advisor

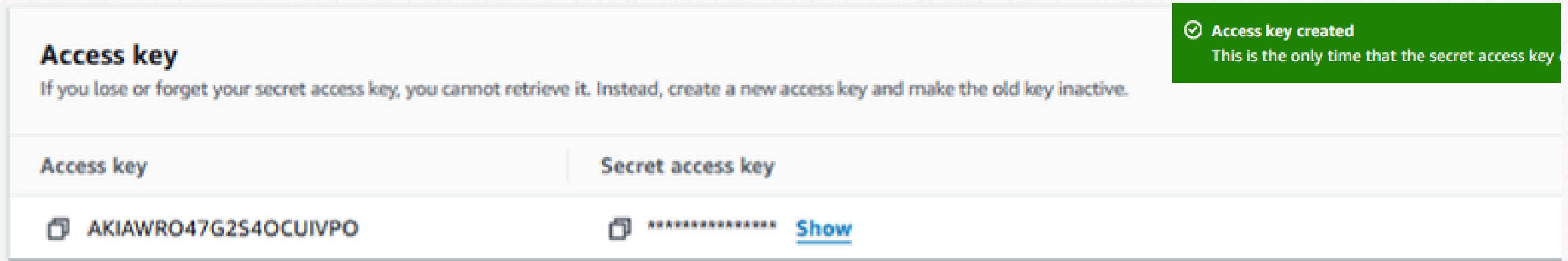
User groups membership (1)		Remove	Add user to groups
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.			
<input type="checkbox"/>	Group name	Attached policies	
<input type="checkbox"/>	mediaco	IAMUserChangePassword	



Tarea 3.2: revisar el usuario de IAM mediacouser

- Y crearemos una clave de acceso

Groups > Security Credentials > Access Key > Create Access Key.



The screenshot shows the AWS IAM Access Key creation interface. At the top right, a green success message box displays: "Access key created" with a checkmark icon and the note "This is the only time that the secret access key will be displayed. Store it securely." Below this, there are two sections: "Access key" and "Secret access key". The "Access key" section contains a copy icon and the value "AKIAWRO47G2S4OCUIVPO". The "Secret access key" section contains a copy icon, a redacted secret key value, and a "Show" link. A small note below the "Secret access key" section states: "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."



Tarea 3.3: Probar los permisos de mediacouser.

Iniciaremos sesión en la Consola de administración de AWS como mediacouser y realizaremos operaciones de visualización, carga y eliminación del contenido de la carpeta de imágenes en el bucket de recursos compartidos de S3, las credenciales de acceso serán diferentes a su cuenta principal.

- Credenciales de inicio de sesión:

Nombre de usuario de IAM: mediacouser

Contraseña: Training1!

Tarea 3.3: Probar los permisos de mediacouser.

- Prueba de visualización:

Donuts.jpg

Información

Copiar URI de S3

Descargar

Abrir





Tarea 3.3: Probar los permisos de mediacouser.

- Prueba de carga y eliminación:
- En la página Cargar, seleccione Agregar archivos y seleccione cualquier imagen o foto de su equipo local, en este caso “peru.png”.

Archivos y carpetas (1 Total, 249.0 B)

 Buscar por nombre						
Nombre	Carpeta	Tipo	Tamaño	Estado	Error	
peru.png 	-	image/png	249.0 B	 Realizado correctamente	-	

- En la página Eliminar objetos, en el cuadro ¿Eliminar objetos?, ingrese delete

Eliminado correctamente
 **1 objeto, 308.7 KB**



Tarea 4: Configuración de notificaciones de eventos en el bucket compartido de S3.

Configuraremos el bucket compartido de S3 para generar una notificación de evento a un tema de SNS cada vez que cambia el contenido del depósito.

Luego, el tema de SNS envía un mensaje de correo electrónico a sus usuarios suscritos con el mensaje de notificación.

Realizaremos los siguientes pasos:

- Crearemos el tema SNS s3NotificationTopic.
 - Concederemos permiso a Amazon S3 para publicar en el tema.
 - Nos suscribiremos al tema.
 - Agregaremos una configuración de notificación de eventos al bucket de S3.
- 

Tarea 4.1: Creación y configuración del tema SNS s3NotificationTopic.

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 (_).

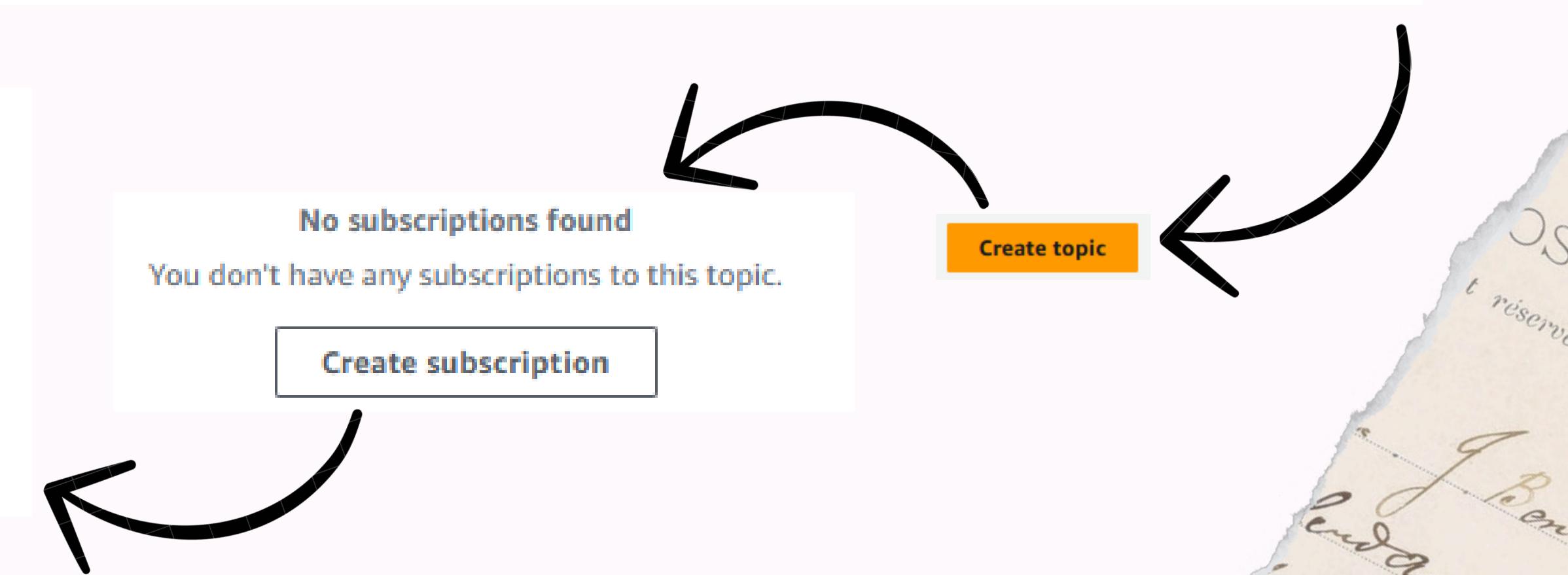
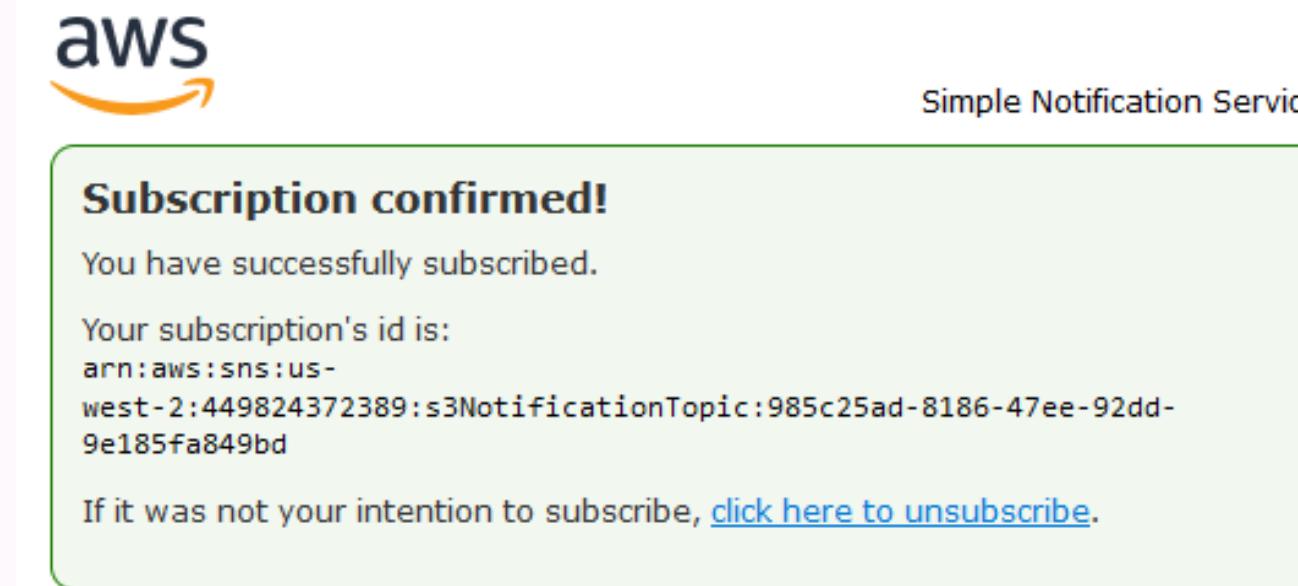
[Create topic](#)

Configuración adicional:

▼ 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.

```
23 "Resource": "arn:aws:sns:us-west-2:449824372389:s3NotificationTopic",  
24  
25 "Condition": {  
26  
27 "ArnLike": {  
28  
29 "aws:SourceArn": "arn:aws:s3::*:cafe-abc123"
```





Tarea 4.2: Agregar una configuración de notificación de eventos al bucket S3.

En la ventana de terminal para la instancia de CLI Host, ingresamos el siguiente comando para editar un nuevo archivo llamado s3EventNotification.json:

```
vi s3EventNotification.json
```



```
GNU nano 2.9.8 s3EventNotification.json

{
  "TopicConfigurations": [
    {
      "TopicArn": "arn:aws:sns:us-west-2:449824372389:s3NotificationTopic",
      "Events": ["s3:ObjectCreated:*", "s3:ObjectRemoved:*"],
      "Filter": {
        "Key": {
          "FilterRules": [
            {
              "Name": "prefix",
              "Value": "images/"
            }
          ]
        }
      }
    }
  ]
}
```

Así entraremos en el modo inserción para reemplazar el valor del ARN -->

- Para asociar el archivo de configuración de eventos con el depósito compartido de S3, ejecutamos el siguiente comando, reemplazando <cafe-xxxxxx> con el nombre de nuestro bucket S3:

```
aws s3api put-bucket-notification-configuration --bucket cafe-abc123 --notification-configuration file://s3EventNotification.json
```

- Esperamos unos momentos y revisamos nuestro e-mail con la confirmación:



Amazon S3 Notification ➤ Recibidos ✖

AWS Notifications <no-reply@sns.amazonaws.com>
para mi ▾ 21:32 (hace 0 minutos) ★ ☺ ⏴ ⏵

{"Service": "Amazon S3", "Event": "s3:TestEvent", "Time": "2024-07-09T00:32:32.128Z", "Bucket": "cafe-abc123", "RequestId": "A0ZJEC2HEY3XJ3PP", "HostId": "qsizCwWZgVdlXcqWOdxMZNVE5Wdxo8UxvAhwYCEurl8xTrfYokbM0IXyPK/mzL+/PT4zz+glsg="}

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
<https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:449824372389:s3NotificationTopic:985c25ad-8186-47ee-92dd-9e185fa849bd&Endpoint=sonyetcherry13@gmail.com>

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>



Tarea 5: Probando las notificaciones de eventos del bucket compartido de S3.

- Para configurar el software cliente AWS CLI del host CLI para utilizar las credenciales de mediacouser, en la ventana SSH de la instancia del host CLI, ingresamos el siguiente comando con las siguientes credenciales:

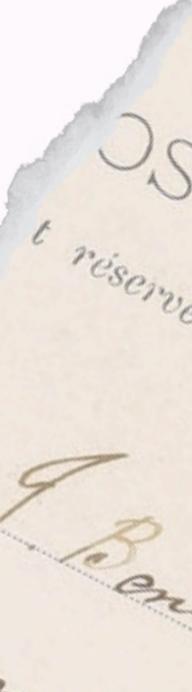
```
[ec2-user@ip-10-200-0-232 ~]$ aws configure
AWS Access Key ID [*****IVPO]:
AWS Secret Access Key [*****N1yB]:
Default region name [us-west-2]:
Default output format [json]:
[ec2-user@ip-10-200-0-232 ~]$ █
```



Tarea 5: Probando las notificaciones de eventos del bucket compartido de S3.

- A continuación, pruebaremos el uso de **put** y **get** subiendo el archivo de imagen Caramel-Delight.jpg y tomando también obteniendo Donuts.jpg desde la carpeta new-images en el CLI Host.
- Para hacerlo, utilizaremos el siguiente comando:

```
[ec2-user@ip-10-200-0-232 ~]$ aws s3api put-object --bucket cafe-abc123 --key images/Caramel-Delight.jpg -  
{  
    "ETag": "\"3iac30da619244b0ce786f106e4f3df7\"",  
    "ServerSideEncryption": "AES256"  
}  
[ec2-user@ip-10-200-0-232 ~]$ aws s3api get-object --bucket cafe-abc123 --key images/Donuts.jpg Donuts.jpg  
{  
    "AcceptRanges": "bytes",  
    "ContentType": "image/jpeg",  
    "LastModified": "Mon, 08 Jul 2024 23:31:07 GMT",  
    "ContentLength": 380753,  
    "ETag": "\"405b0bcc53cb5ab713c967dc1422b4f4\"",  
    "ServerSideEncryption": "AES256",  
    "Metadata": ()  
}
```





Tarea 5: Probando las notificaciones de eventos del bucket compartido de S3.

- Luego, verificaremos en la bandeja de entrada la dirección de correo electrónico que utilizamos para suscribirse al tema SNS s3NotificationTopic.



- Esta notificación indica que se agregó un nuevo objeto con una clave de imágenes/Caramel-Delight.jpg en el depósito compartido de S3.



Tarea 5: Probando las notificaciones de eventos del bucket compartido de S3.

- Finalmente, probaremos el comando delete eliminando el objeto con una clave de imágenes/Strawberry-Tarts.jpg del bucket.

```
[ec2-user@ip-10-200-0-232 ~]$ aws s3api delete-object --bucket cafe-abc123 --key images/Strawberry-Tarts.jpg
```

- En este comando se intenta cambiar los permisos del bucket pero no nos lo permite

```
[ec2-user@ip-10-200-0-232 ~]$ aws s3api put-object-acl --bucket cafe-abc123 --key images/Donuts.jpg --acl public-read
An error occurred (AccessDenied) when calling the PutObjectAcl operation: Access Denied
[ec2-user@ip-10-200-0-232 ~]$ █
```





Gracias

