AWS re:Start

LAB

Working with Amazon S3

WEEK 10

aws re/start

Overview

Working with Amazon S3 involves using the AWS CLI's s3api and s3 commands to create and configure S3 buckets. The s3api commands provide granular control over S3 resources, allowing you to create buckets, set policies, and manage bucket configurations. On the other hand, s3 commands offer higher-level operations for common tasks such as uploading, downloading, and syncing files. By combining these commands, users can efficiently manage their S3 storage, automate tasks, and ensure proper configuration and access controls.

Another critical aspect of working with Amazon S3 is verifying write permissions to a user on an S3 bucket. This involves ensuring that users have the necessary permissions to upload and modify objects within the bucket. Additionally, configuring event notifications on an S3 bucket is crucial for automating workflows and integrating with other AWS services. Event notifications can trigger actions such as Lambda functions, SNS topics, or SQS queues in response to specific events like object creation or deletion. This capability enhances the functionality and responsiveness of your S3-based applications.

Topics covered

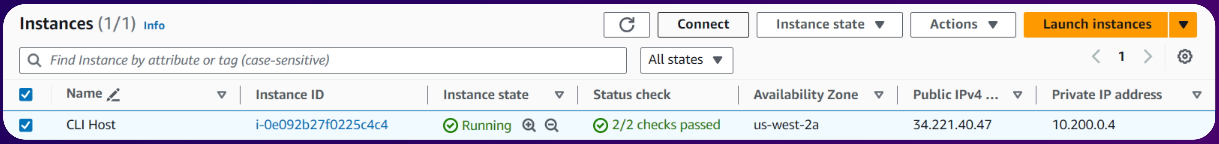
- Use the s3api and s3 AWS CLI commands to create and configure an S3 bucket.
- Verify write permissions to a user on an S3 bucket.
- Configure event notification on an S3 bucket.

Task 1

Connecting to the CLI Host EC2 instance

Step 1: Connect to the CLI Host

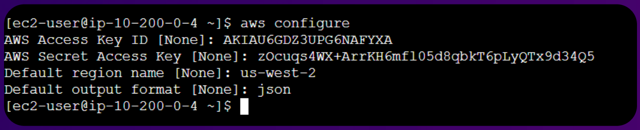
In the EC2 Management Console, navigate to the **Instances** section, select the **CLI Host**, and connect to the instance using EC2 Instance Connect.



☑	Name	Instance ID	Instance state	Status check	Availability Zone	Public IPv4 ...	Private IP address
☑	CLI Host	i-0e092b27f0225c4c4	✓ Running	✓ 2/2 checks passed	us-west-2a	34.221.40.47	10.200.0.4

Step 2: Configure the AWS CLI

To set up the AWS CLI profile with credentials, run the aws configure command in the EC2 Instance Connect terminal. At the prompts, enter the following information.



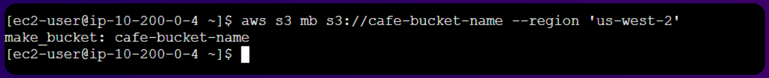
```
[ec2-user@ip-10-200-0-4 ~]$ aws configure
AWS Access Key ID [None]: AKIAU6GDZ3UPG6NAFYXA
AWS Secret Access Key [None]: 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
Default region name [None]: us-west-2
Default output format [None]: json
[ec2-user@ip-10-200-0-4 ~]$ 
```

Task 2

Creating and initializing the S3 share bucket

Step 1: Create an S3 bucket

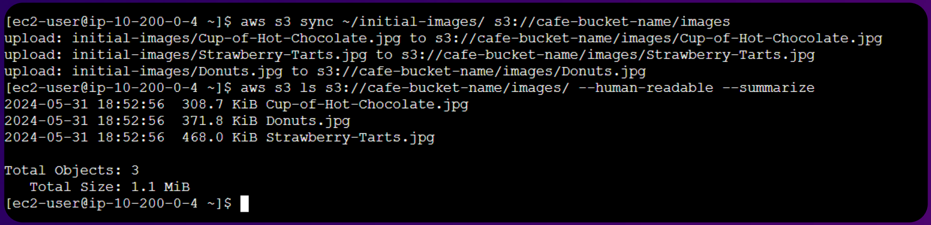
To create an S3 bucket, run the following aws s3 mb command.



```
[ec2-user@ip-10-200-0-4 ~]$ aws s3 mb s3://cafe-bucket-name --region 'us-west-2'
make_bucket: cafe-bucket-name
[ec2-user@ip-10-200-0-4 ~]$ █
```

Step 2: Sync files

To load images into the bucket, run the following aws s3 sync command. The command output lists the image files that are being uploaded. To verify that the files were synced to the S3 bucket, run the following aws s3 ls command. You see the details of the image files that were uploaded, including the number of files uploaded and the total size of the files.



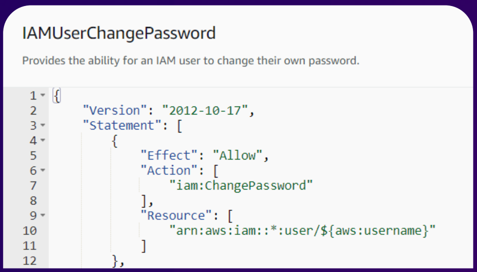
```
[ec2-user@ip-10-200-0-4 ~]$ aws s3 sync ~/initial-images/ s3://cafe-bucket-name/images
upload: initial-images/Cup-of-Hot-Chocolate.jpg to s3://cafe-bucket-name/images/Cup-of-Hot-Chocolate.jpg
upload: initial-images/Strawberry-Tarts.jpg to s3://cafe-bucket-name/images/Strawberry-Tarts.jpg
upload: initial-images/Donuts.jpg to s3://cafe-bucket-name/images/Donuts.jpg
[ec2-user@ip-10-200-0-4 ~]$ aws s3 ls s3://cafe-bucket-name/images/ --human-readable --summarize
2024-05-31 18:52:56  308.7 KiB Cup-of-Hot-Chocolate.jpg
2024-05-31 18:52:56  371.8 KiB Donuts.jpg
2024-05-31 18:52:56  468.0 KiB Strawberry-Tarts.jpg

Total Objects: 3
   Total Size: 1.1 MiB
[ec2-user@ip-10-200-0-4 ~]$ █
```

Task 3

Reviewing the IAM group and user permissions

Step 1: Review the mediaco IAM group

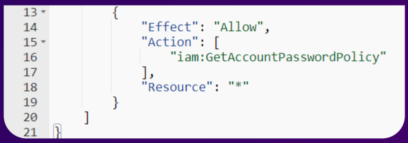
In the IAM Management Console, navigate to the **User groups** section, and select the **mediaco** group. In the **Permissions** tab, review the **IAMUserChangePassword** permissions policy.



IAMUserChangePassword

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

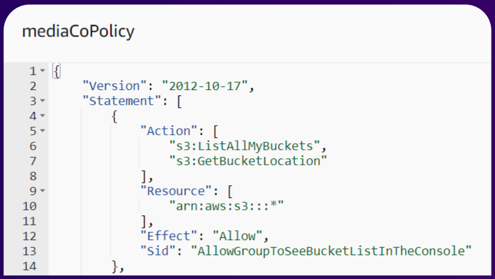
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ChangePassword"
            ],
            "Resource": [
                "arn:aws:iam::*:user/${aws:username}"
            ]
        },
```



```
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetAccountPasswordPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

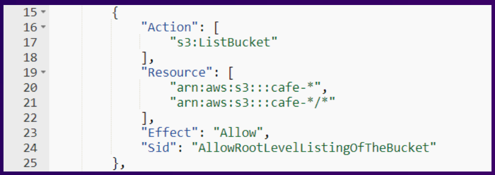
Step 2: Review the mediaCoPolicy

Review the **mediaCoPolicy** permissions policy.

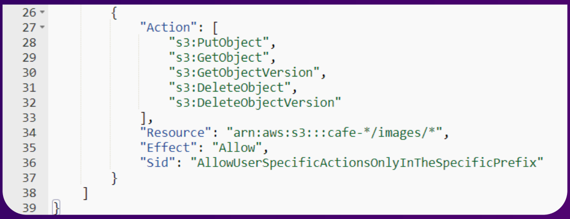


mediaCoPolicy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ],
            "Effect": "Allow",
            "Sid": "AllowGroupToSeeBucketListInTheConsole"
        },
```



```
        {
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::cafe-*",
                "arn:aws:s3:::cafe-*/*"
            ],
            "Effect": "Allow",
            "Sid": "AllowRootLevelListingOfTheBucket"
        },
```



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

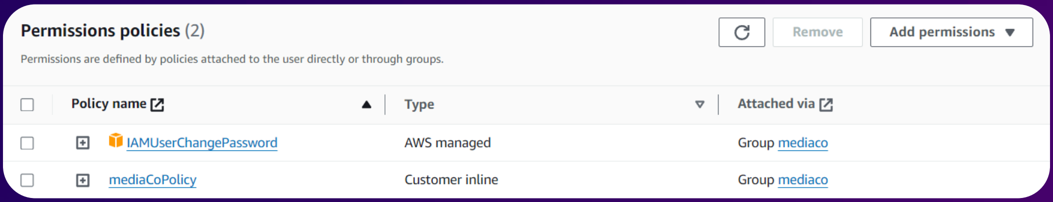
aws re/start

Task 3

Reviewing the IAM group and user permissions

Step 3: Review the mediacouser IAM user

Navigate to the **Users** section, and select the **mediacouser**. In the **Permissions** tab, you should see two permissions policies. These policies are assigned to the **mediaco** IAM group.



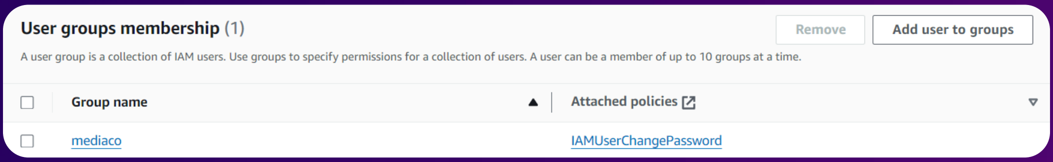
Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

□	Policy name ▲	Type	Attached via
□	⊞ IAMUserChangePassword	AWS managed	Group mediaco
□	⊞ mediaCoPolicy	Customer inline	Group mediaco

Step 4: Review group membership

In the **Groups** tab, you should see that the **mediacouser** user is a member of the **mediaco** IAM group and therefore inherits the permissions assigned to the **mediaco** group.



User groups membership (1)

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.

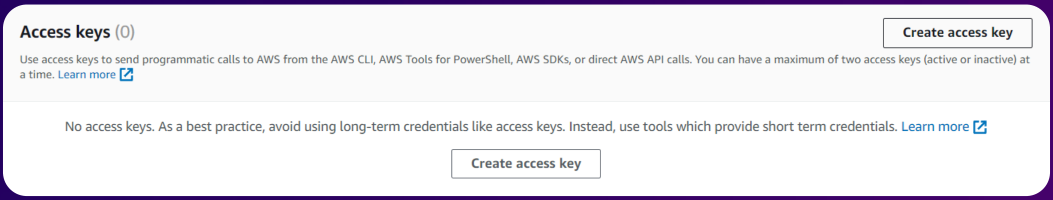
□	Group name ▲	Attached policies
□	mediaco	IAMUserChangePassword

Task 3

Reviewing the IAM group and user permissions

Step 5: Create access key

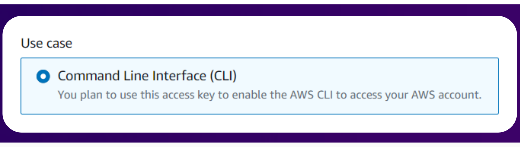
Choose the **Security credentials** tab. In the **Access keys** section, choose Create access key, and choose the following options. Choose Download .csv file.



Access keys (0)

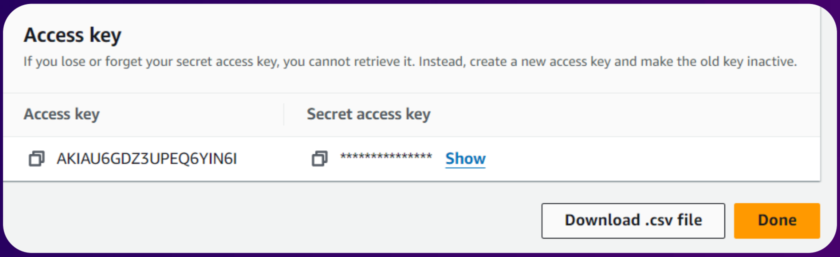
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

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



Use case

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



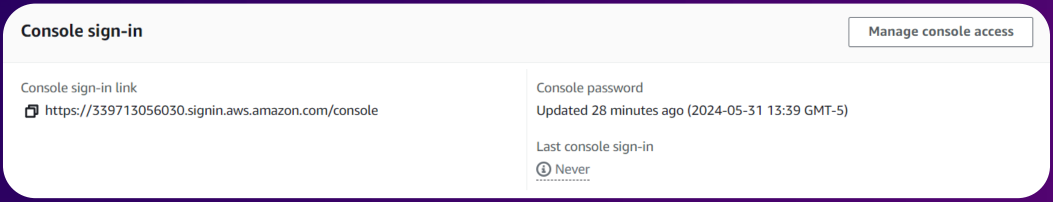
Access key

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	Secret access key
AKIAU6GDZ3UPEQ6YIN6I	*************** Show

Step 6: Review Console sign-in

In the **Console sign-in** section, copy the Console sign-in link.



Console sign-in

Console sign-in link
https://339713056030.signin.aws.amazon.com/console

Console password
Updated 28 minutes ago (2024-05-31 13:39 GMT-5)

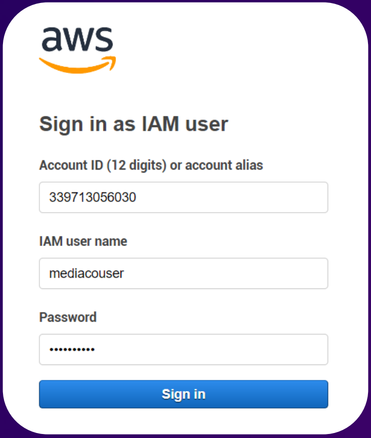
Last console sign-in
Never

Task 3

Reviewing the IAM group and user permissions

Step 7: Sign in as mediacouser

Access the Console sign-in link, and sign in as the IAM user **mediacouser**.



Sign in as IAM user

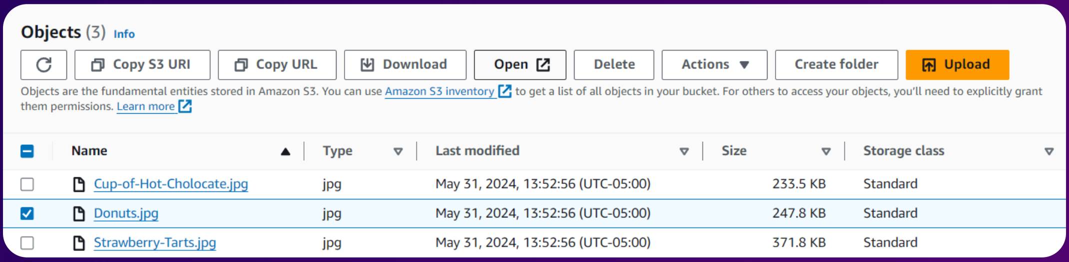
Account ID (12 digits) or account alias: 339713056030

IAM user name: mediacouser

Password: ••••••••••

Step 8: Review bucket objects

In S3 Management Console, select your bucket, select the **images/** folder, and review the objects list. To test the view operation, select an object, and choose Open.



Objects (3) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

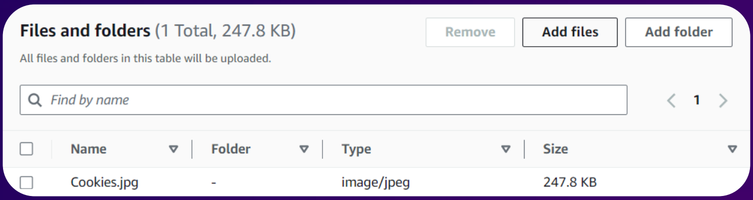
	Name	Type	Last modified	Size	Storage class
□	Cup-of-Hot-Cholocate.jpg	jpg	May 31, 2024, 13:52:56 (UTC-05:00)	233.5 KB	Standard
☑	Donuts.jpg	jpg	May 31, 2024, 13:52:56 (UTC-05:00)	247.8 KB	Standard
□	Strawberry-Tarts.jpg	jpg	May 31, 2024, 13:52:56 (UTC-05:00)	371.8 KB	Standard

Task 3

Reviewing the IAM group and user permissions

Step 9: Upload bucket files

To test the upload operation, choose Upload. Choose Add files, and choose any image or picture from your local computer.



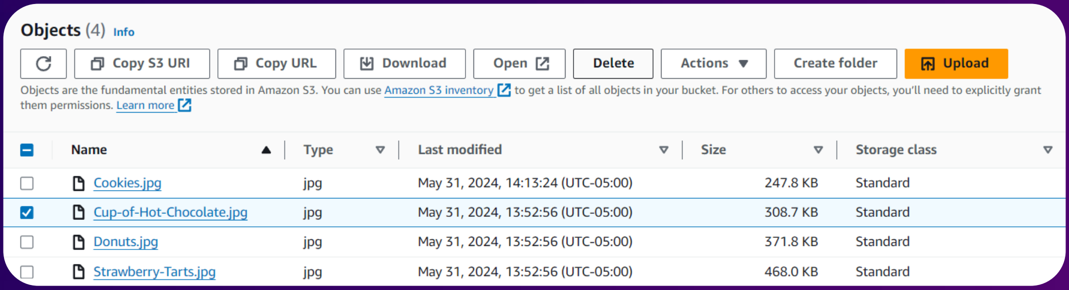
Files and folders (1 Total, 247.8 KB)

All files and folders in this table will be uploaded.

☐	Name	Folder	Type	Size
☐	Cookies.jpg	-	image/jpeg	247.8 KB

Step 10: Delete bucket objects

To test the delete operation, select an object, and choose Delete.



Objects (4)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

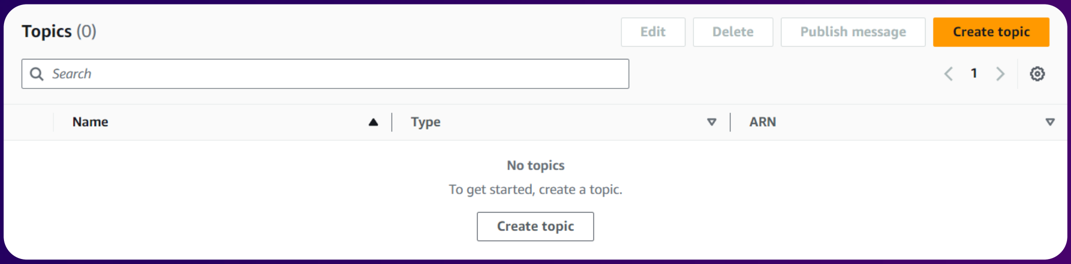
☐	Name	Type	Last modified	Size	Storage class
☐	Cookies.jpg	jpg	May 31, 2024, 14:13:24 (UTC-05:00)	247.8 KB	Standard
☑	Cup-of-Hot-Chocolate.jpg	jpg	May 31, 2024, 13:52:56 (UTC-05:00)	308.7 KB	Standard
☐	Donuts.jpg	jpg	May 31, 2024, 13:52:56 (UTC-05:00)	371.8 KB	Standard
☐	Strawberry-Tarts.jpg	jpg	May 31, 2024, 13:52:56 (UTC-05:00)	468.0 KB	Standard

Task 4

Configuring event notifications on the S3 share bucket

Step 1: Create topic

In the Simple Notification Service Console, navigate to the **Topics** section, and select Create topic.

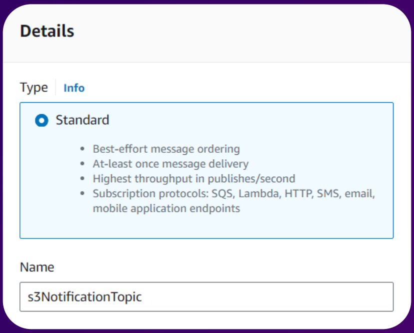


No topics

To get started, create a topic.

Step 2: Topic details

In the **Details** section, configure the following settings.



Type

● 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

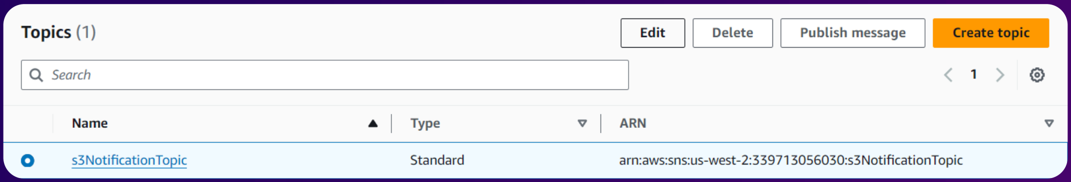
s3NotificationTopic

Task 4

Configuring event notifications on the S3 share bucket

Step 3: Edit Topic

Select the newly created **s3NotificationTopic**, copy the ARN value, and select Edit.



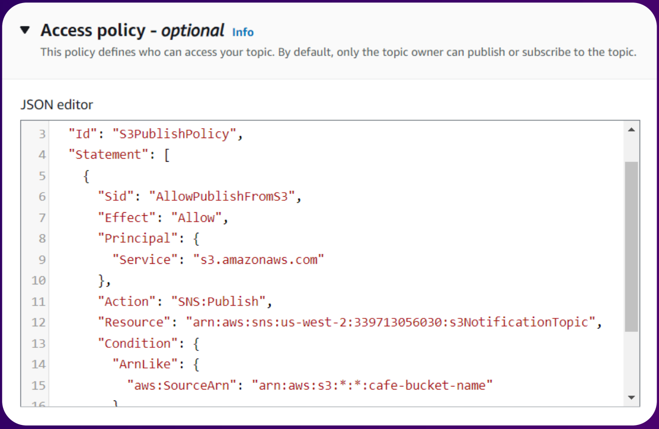
Topics (1)

Edit | Delete | Publish message | Create topic

	Name	Type	ARN
●	s3NotificationTopic	Standard	arn:aws:sns:us-west-2:339713056030:s3NotificationTopic

Step 4: Edit Access policy

In the **Access policy** section, configure the topic's access policy. This policy grants the cafe S3 share bucket permission to publish messages to the **s3NotificationTopic** SNS topic.



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

```
  "Id": "S3PublishPolicy",
  "Statement": [
    {
      "Sid": "AllowPublishFromS3",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:339713056030:s3NotificationTopic",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:*:*:cafe-bucket-name"
        }
```

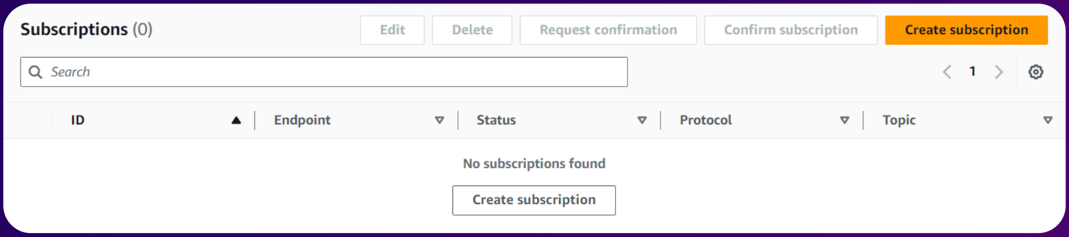
aws re/start

Task 4

Configuring event notifications on the S3 share bucket

Step 5: Create subscription

Navigate to the **Subscriptions** section, and select Create subscription.



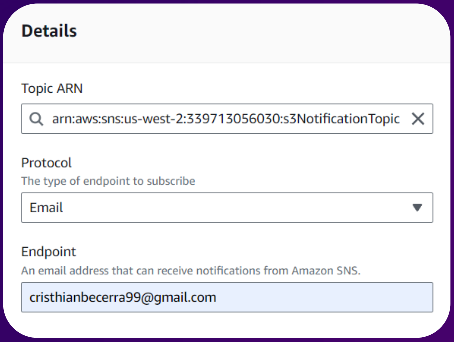
Subscriptions (0)

ID	Endpoint	Status	Protocol	Topic

No subscriptions found

Step 6: Subscription details

In the **Details** section, configure the following settings.



Details

Topic ARN: arn:aws:sns:us-west-2:339713056030:s3NotificationTopic

Protocol
The type of endpoint to subscribe
Email

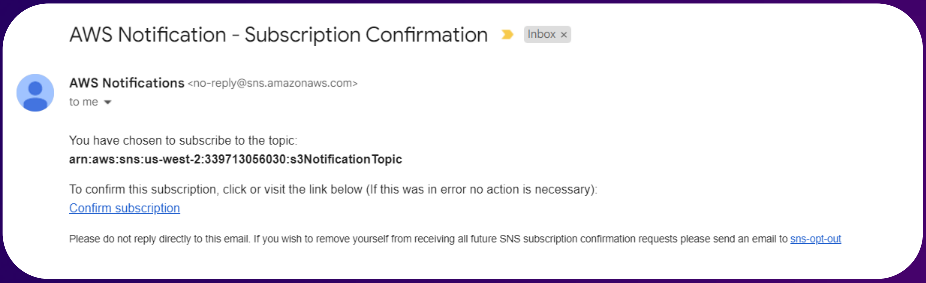
Endpoint
An email address that can receive notifications from Amazon SNS.
cristhianbecerra99@gmail.com

Task 4

Configuring event notifications on the S3 share bucket

Step 7: Check email inbox

Check the inbox for the email address that you provided. You should see an email message with the subject AWS Notification - Subscription Confirmation.



AWS Notification - Subscription Confirmation

AWS Notifications <no-reply@sns.amazonaws.com>

to me

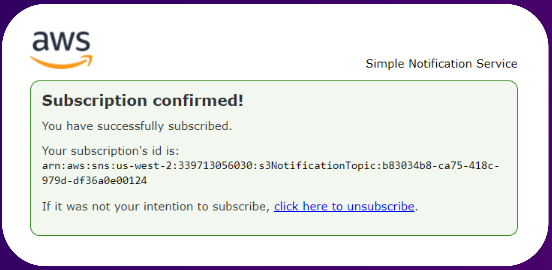
You have chosen to subscribe to the topic:
arn:aws:sns:us-west-2:339713056030:s3NotificationTopic

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

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out

Step 8: Confirm subscription

Choose Confirm subscription. A new browser tab opens and displays a page with the message Subscription confirmed!.



Simple Notification Service

Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:
arn:aws:sns:us-west-2:339713056030:s3NotificationTopic:b83034b8-ca75-418c-979d-df36a0e00124

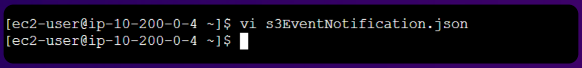
If it was not your intention to subscribe, click here to unsubscribe.

Task 4

Configuring event notifications on the S3 share bucket

Step 9: Create a configuration file

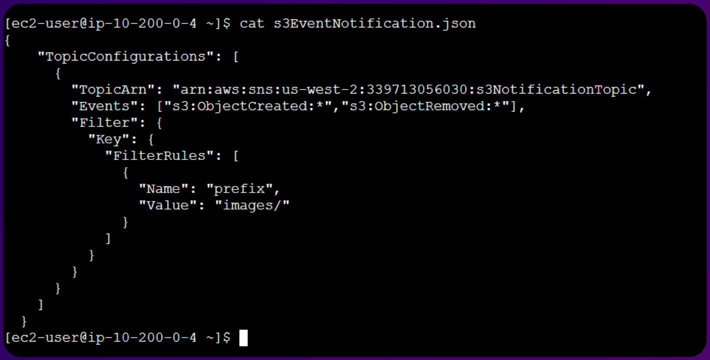
Create an event notification configuration file that identifies the events that Amazon S3 will publish and the topic destination where Amazon S3 will send the event notifications. Enter the following command to edit a new file named **s3EventNotification.json**.



```
[ec2-user@ip-10-200-0-4 ~]$ vi s3EventNotification.json
[ec2-user@ip-10-200-0-4 ~]$ 
```

Step 10: Review the configuration file

Review the intent of this configuration. It requests that Amazon S3 publish an event notification to the **s3NotificationTopic** SNS topic whenever an ObjectCreated or ObjectRemoved event is performed on objects inside an Amazon S3 resource with a prefix of **images/**.



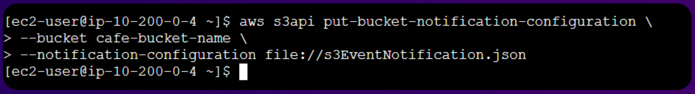
```
[ec2-user@ip-10-200-0-4 ~]$ cat s3EventNotification.json
{
    "TopicConfigurations": [
      {
        "TopicArn": "arn:aws:sns:us-west-2:339713056030:s3NotificationTopic",
        "Events": ["s3:ObjectCreated:*","s3:ObjectRemoved:*"],
        "Filter": {
          "Key": {
            "FilterRules": [
              {
                "Name": "prefix",
                "Value": "images/"
              }
            ]
          }
        }
      }
    ]
  }
[ec2-user@ip-10-200-0-4 ~]$ 
```

Task 4

Configuring event notifications on the S3 share bucket

Step 11: Associate the configuration file

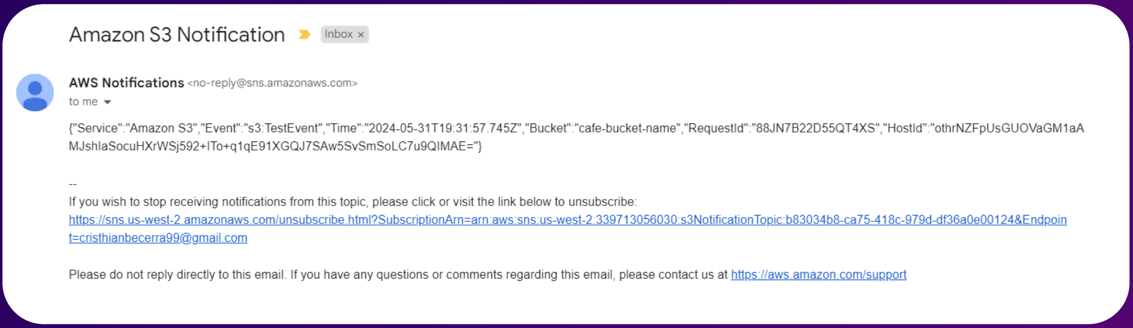
To associate the event notification configuration file with the S3 share bucket, run the following aws s3api put-bucket-notification-configuration command.



```
[ec2-user@ip-10-200-0-4 ~]$ aws s3api put-bucket-notification-configuration \
> --bucket cafe-bucket-name \
> --notification-configuration file://s3EventNotification.json
[ec2-user@ip-10-200-0-4 ~]$ █
```

Step 12: Check email inbox

Open the new email message with the subject Amazon S3 Notification. Notice that the value of the "Event" key is "s3:TestEvent". Amazon S3 sent this notification as a test of the event notifications configuration that you set up.



AWS Notifications <no-reply@sns.amazonaws.com>
to me

{"Service":"Amazon S3","Event":"s3:TestEvent","Time":"2024-05-31T19:31:57.745Z","Bucket":"cafe-bucket-name","RequestId":"88JN7B22D55QT4XS","HostId":"othrNZFpUsGUOVaGM1aAMJshlaSocuHXrWSj592+ITo+q1qE91XGQJ7SAw5SvSmSoLC7u9QIMAE="}

--
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-2:339713056030:s3NotificationTopic:b83034b8-ca75-418c-979d-df36a0e00124&Endpoint=cristhianbecerra99@gmail.com

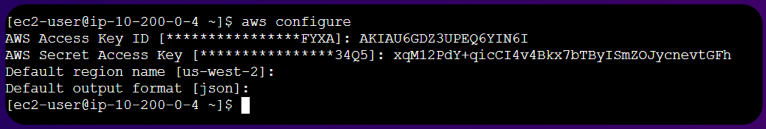
Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support

Task 5

Testing the S3 share bucket event notifications

Step 1: Configure the AWS CLI

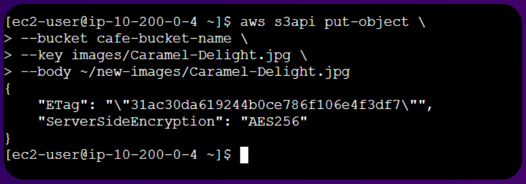
To configure the CLI Host's AWS CLI client software to use the mediacouser credentials, enter the aws configure command. At the prompts, enter the following information.



```
[ec2-user@ip-10-200-0-4 ~]$ aws configure
AWS Access Key ID [****************FYXA]: AKIAU6GDZ3UPEQ6YIN6I
AWS Secret Access Key [****************34Q5]: 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
Default region name [us-west-2]:
Default output format [json]:
[ec2-user@ip-10-200-0-4 ~]$ 
```

Step 2: Upload a file

To upload a file to the S3 share bucket, run the following aws s3api put-object command.



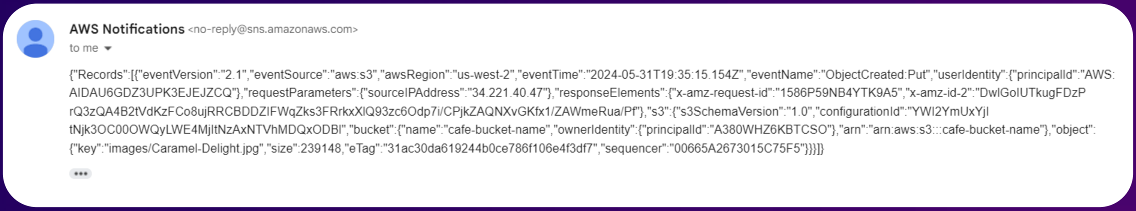
```
[ec2-user@ip-10-200-0-4 ~]$ aws s3api put-object \
> --bucket cafe-bucket-name \
> --key images/Caramel-Delight.jpg \
> --body ~/new-images/Caramel-Delight.jpg
{
    "ETag": "\"31ac30da619244b0ce786f106e4f3df7\"",
    "ServerSideEncryption": "AES256"
}
[ec2-user@ip-10-200-0-4 ~]$ 
```

Task 5

Testing the S3 share bucket event notifications

Step 3: Check email inbox

Examine the notification message. The value of the eventName key is **ObjectCreated:Put**. The value of the key object is **images/Caramel-Delight.jpg,** which is the image file key that you specified in the command. This notification indicates that a new object with a key of **images/Caramel-Delight.jpg** was added (put) into the S3 share bucket.



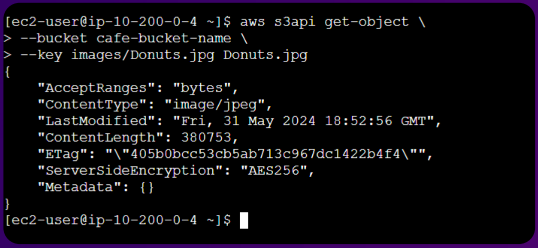
AWS Notifications <no-reply@sns.amazonaws.com>

to me

```
{"Records":[{"eventVersion":"2.1","eventSource":"aws:s3","awsRegion":"us-west-2","eventTime":"2024-05-31T19:35:15.154Z","eventName":"ObjectCreated:Put","userIdentity":{"principalId":"AWS:
AIDAU6GDZ3UPK3EJEJZCQ"},"requestParameters":{"sourceIPAddress":"34.221.40.47"},"responseElements":{"x-amz-request-id":"1586P59NB4YTK9A5","x-amz-id-2":"DwlGoIUTkugFDzP
rQ3zQA4B2tVdKzFCo8ujRRCBDDZIFWqZks3FRrkxXIQ93zc6Odp7i/CPjkZAQNXvGKfx1/ZAWmeRua/Pf"},"s3":{"s3SchemaVersion":"1.0","configurationId":"YWI2YmUxYjI
tNjk3OC00OWQyLWE4MjItNzAxNTVhMDQxODBl","bucket":{"name":"cafe-bucket-name","ownerIdentity":{"principalId":"A380WHZ6KBTCSO"},"arn":"arn:aws:s3:::cafe-bucket-name"},"object":
{"key":"images/Caramel-Delight.jpg","size":239148,"eTag":"31ac30da619244b0ce786f106e4f3df7","sequencer":"00665A2673015C75F5"}}}]}
```

Step 4: Get an object

To get an object, run the following aws s3api get-object command. Notice that an email notification was not generated for this operation. This operation does not generate an email notification because the share bucket is configured to send notifications only when objects are created or deleted.



```
[ec2-user@ip-10-200-0-4 ~]$ aws s3api get-object \
> --bucket cafe-bucket-name \
> --key images/Donuts.jpg Donuts.jpg
{
    "AcceptRanges": "bytes",
    "ContentType": "image/jpeg",
    "LastModified": "Fri, 31 May 2024 18:52:56 GMT",
    "ContentLength": 380753,
    "ETag": "\"405b0bcc53cb5ab713c967dc1422b4f4\"",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
[ec2-user@ip-10-200-0-4 ~]$
```

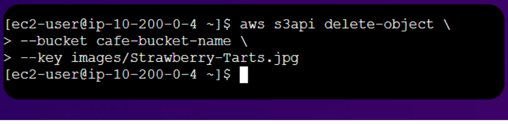
aws re/start

Task 5

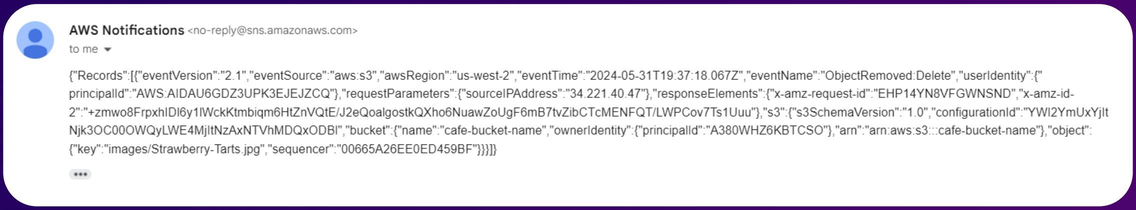
Testing the S3 share bucket event notifications

Step 5: Delete an object

To delete an object, run the following aws s3api delete-object command. Examine the notification message. The value of the eventName key is **ObjectRemoved:Delete**. The value of the object key is **images/Strawberry-Tarts.jpg**, which is the image file key that you specified in the command. This notification indicates that the object with a key of **images/Strawberry-Tarts.jpg** was deleted from the S3 share bucket.



```
[ec2-user@ip-10-200-0-4 ~]$ aws s3api delete-object \
> --bucket cafe-bucket-name \
> --key images/Strawberry-Tarts.jpg
[ec2-user@ip-10-200-0-4 ~]$ █
```

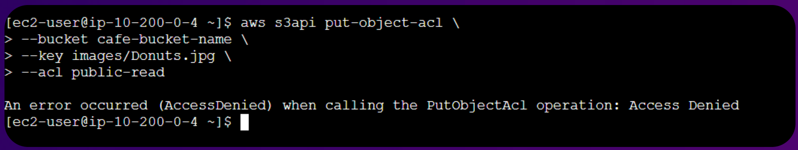


AWS Notifications <no-reply@sns.amazonaws.com>
to me

{"Records":[{"eventVersion":"2.1","eventSource":"aws:s3","awsRegion":"us-west-2","eventTime":"2024-05-31T19:37:18.067Z","eventName":"ObjectRemoved:Delete","userIdentity":{"
principalId":"AWS:AIDAU6GDZ3UPK3EJEJZCQ"},"requestParameters":{"sourceIPAddress":"34.221.40.47"},"responseElements":{"x-amz-request-id":"EHP14YN8VFGWNSND","x-amz-id-
2":"+zmwo8FrpxhIDl6y1lWckKtmbiqm6HtZnVQtE/J2eQoalgostkQXho6NuawZoUgF6mB7tvZibCTcMENFQT/LWPCov7Ts1Uuu"},"s3":{"s3SchemaVersion":"1.0","configurationId":"YWI2YmUxYjlt
Njk3OC00OWQyLWE4MjltNzAxNTVhMDQxODBl","bucket":{"name":"cafe-bucket-name","ownerIdentity":{"principalId":"A380WHZ6KBTCSO"},"arn":"arn:aws:s3:::cafe-bucket-name"},"object":
{"key":"images/Strawberry-Tarts.jpg","sequencer":"00665A26EE0ED459BF"}}}]}

Step 6: Change the permission of the object

To try to change the permission of the **Donuts.jpg** object so that it can be read publicly, run the following aws s3api put-object-acl command. The command fails as expected.



```
[ec2-user@ip-10-200-0-4 ~]$ aws s3api put-object-acl \
> --bucket cafe-bucket-name \
> --key images/Donuts.jpg \
> --acl public-read

An error occurred (AccessDenied) when calling the PutObjectAcl operation: Access Denied
[ec2-user@ip-10-200-0-4 ~]$ █
```

Conclusions

aws s3api put-bucket-notification-configuration
Use this command to set up and manage event notifications for an S3 bucket, enabling automated workflows and integrations with other AWS services.

aws s3api put-object
This command allows you to upload objects to an S3 bucket, making it essential for adding and updating files in your storage.

aws s3api get-object
Retrieve objects from an S3 bucket with this command, facilitating data access and download operations for applications and users.

aws s3api delete-object
Use this command to remove objects from an S3 bucket, helping maintain storage hygiene and manage the lifecycle of your data.

aws s3api put-object-acl
This command sets access control lists (ACLs) for objects, ensuring proper permissions and access management for your stored data.

aws re/start

Cristhian Becerra

cristhian-becerra-espinoza

+51 951 634 354

cristhianbecerra99@gmail.com

Lima, Peru

aws re/start