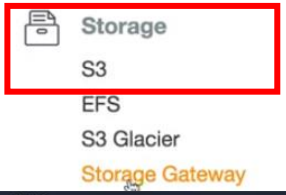
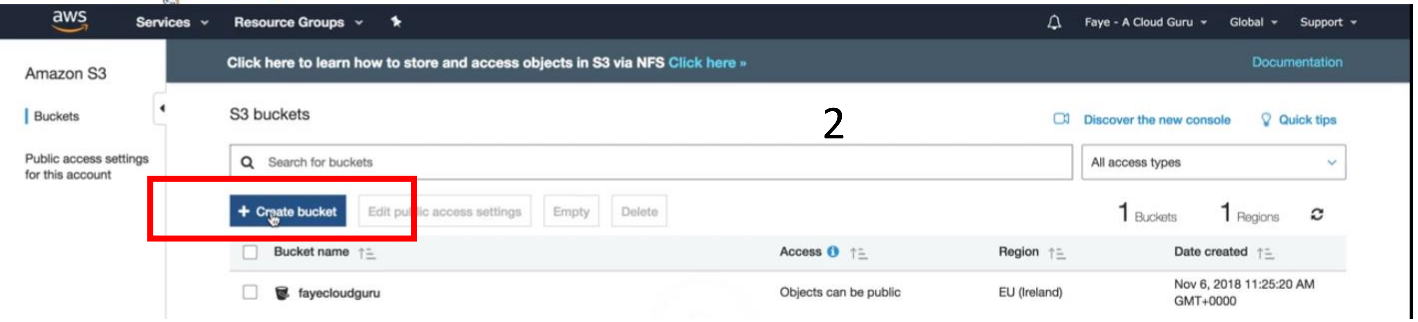
Create bucket

services



1



Click here to learn how to store and access objects in S3 via NFS Click here »

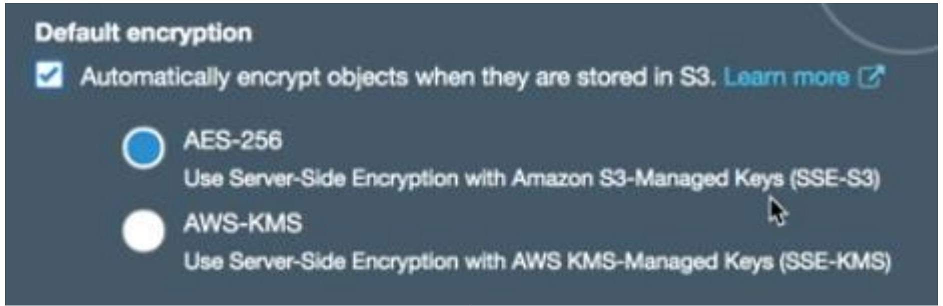
S3 buckets

Search for buckets

1 Buckets 1 Regions

Bucket name	Access	Region	Date created
fayecloudguru	Objects can be public	EU (Ireland)	Nov 6, 2018 11:25:20 AM GMT+0000

2

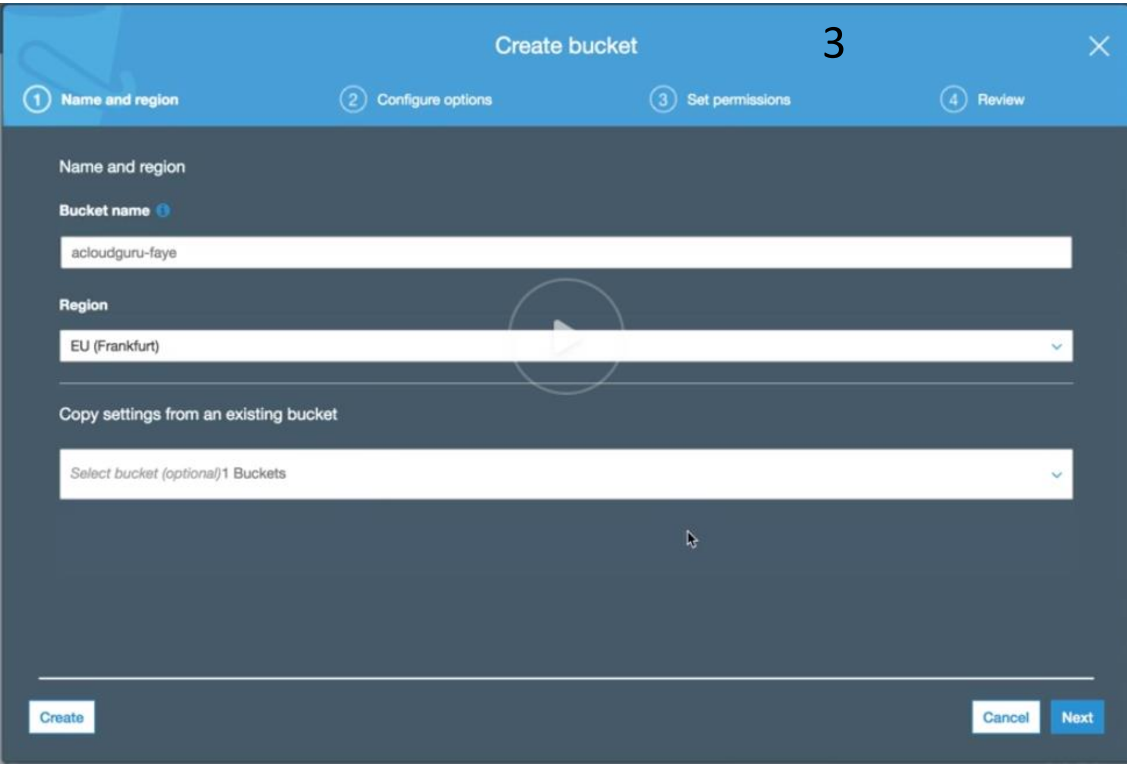


Default encryption

☑ Automatically encrypt objects when they are stored in S3. Learn more

● AES-256
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

○ AWS-KMS
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)



3

Name and region

Bucket name

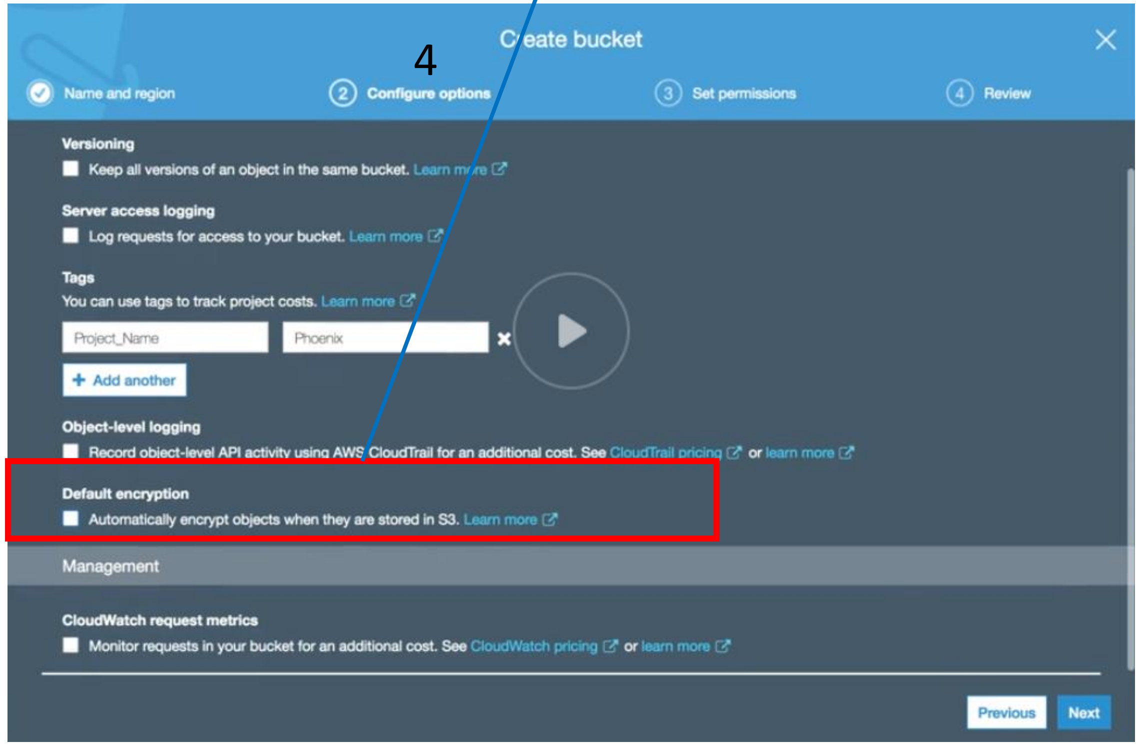
acloudguru-faye

Region

EU (Frankfurt)

Copy settings from an existing bucket

Select bucket (optional)1 Buckets



4

Versioning

□ Keep all versions of an object in the same bucket. Learn more

Server access logging

□ Log requests for access to your bucket. Learn more

Tags

You can use tags to track project costs. Learn more

Project_Name	Phoenix

Object-level logging

□ Record object-level API activity using AWS CloudTrail for an additional cost. See CloudTrail pricing or learn more

Default encryption

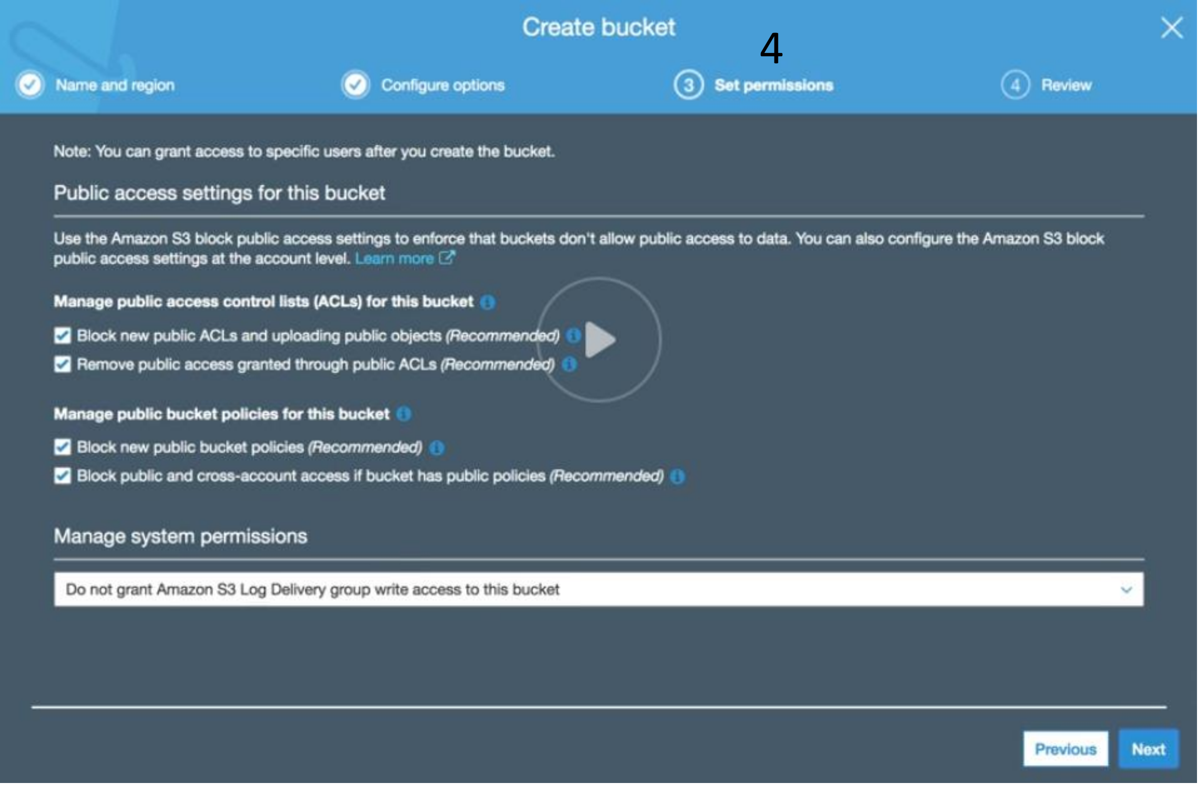
□ Automatically encrypt objects when they are stored in S3. Learn more

Management

CloudWatch request metrics

□ Monitor requests in your bucket for an additional cost. See CloudWatch pricing or learn more

4



Note: You can grant access to specific users after you create the bucket.

Public access settings for this bucket

Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. Learn more

Manage public access control lists (ACLs) for this bucket

☑ Block new public ACLs and uploading public objects *(Recommended)*

☑ Remove public access granted through public ACLs *(Recommended)*

Manage public bucket policies for this bucket

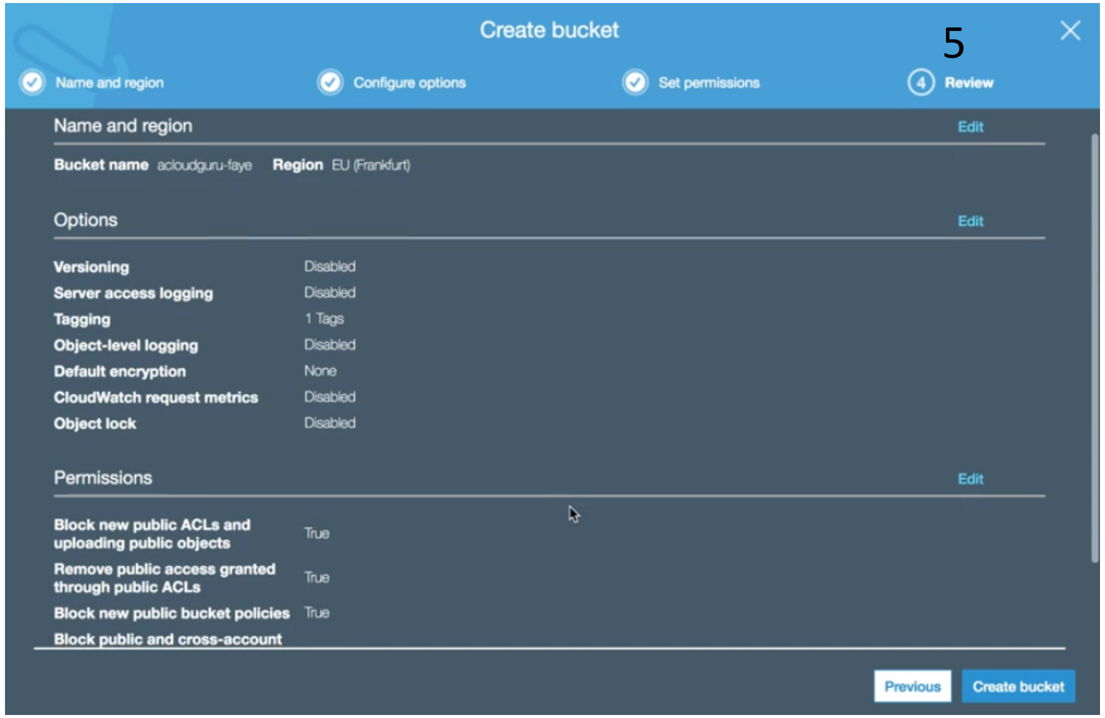
☑ Block new public bucket policies *(Recommended)*

☑ Block public and cross-account access if bucket has public policies *(Recommended)*

Manage system permissions

Do not grant Amazon S3 Log Delivery group write access to this bucket

5



Name and region — Edit

Bucket name acloudguru-faye **Region** EU (Frankfurt)

Options — Edit

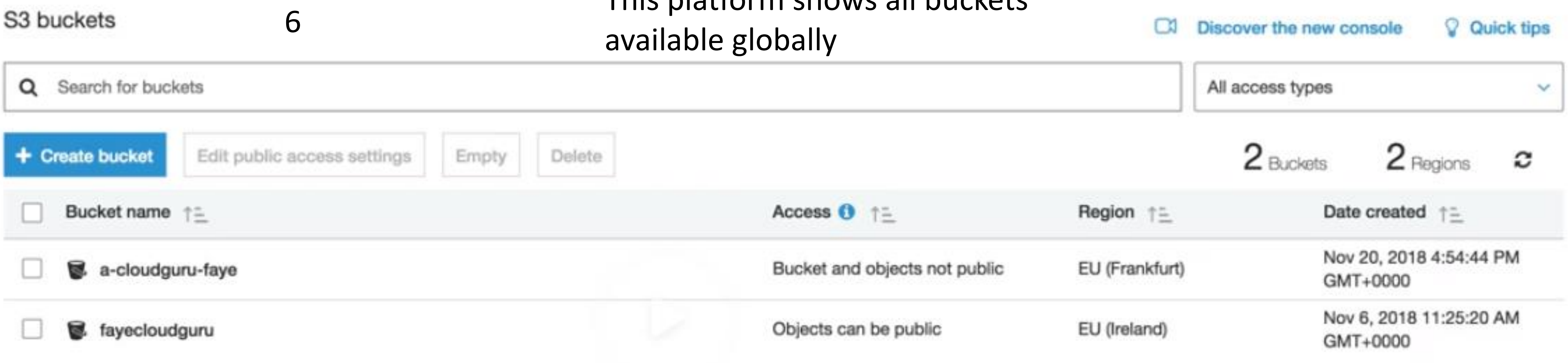
Versioning	Disabled
Server access logging	Disabled
Tagging	1 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled
Object lock	Disabled

Permissions — Edit

Block new public ACLs and uploading public objects	True
Remove public access granted through public ACLs	True
Block new public bucket policies	True
Block public and cross-account	

6

This platform shows all buckets available globally

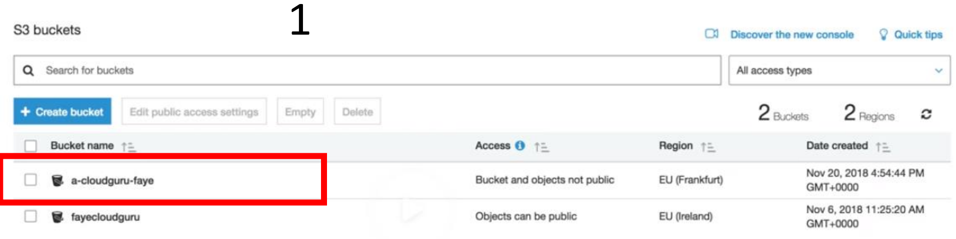


S3 buckets

2 Buckets 2 Regions

	Bucket name	Access	Region	Date created
□	a-cloudguru-faye	Bucket and objects not public	EU (Frankfurt)	Nov 20, 2018 4:54:44 PM GMT+0000
□	fayecloudguru	Objects can be public	EU (Ireland)	Nov 6, 2018 11:25:20 AM GMT+0000

1



S3 buckets

Discover the new console | Quick tips

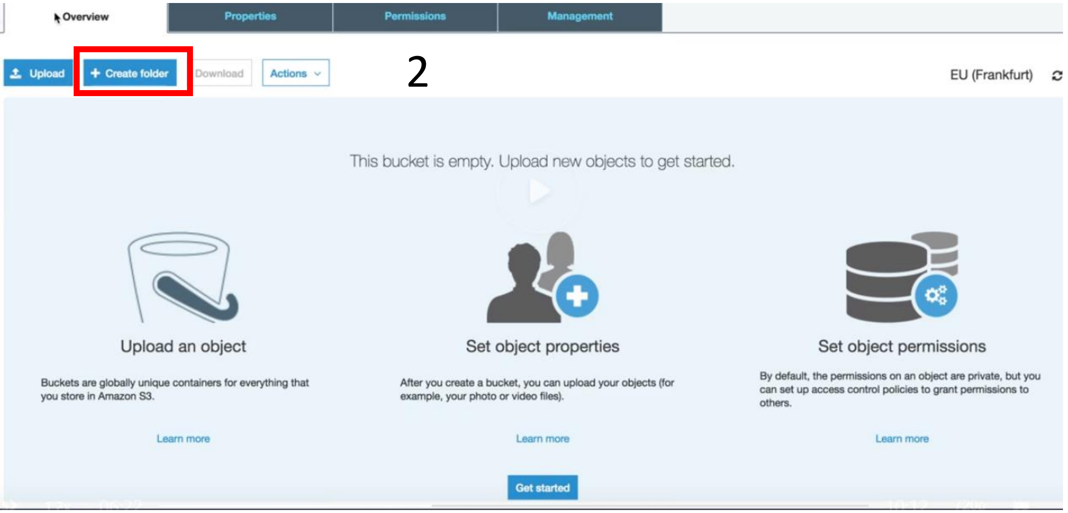
Search for buckets | All access types

+ Create bucket | Edit public access settings | Empty | Delete

2 Buckets 2 Regions

Bucket name	Access	Region	Date created
a-cloudguru-faye	Bucket and objects not public	EU (Frankfurt)	Nov 20, 2018 4:54:44 PM GMT+0000
fayecloudguru	Objects can be public	EU (Ireland)	Nov 6, 2018 11:25:20 AM GMT+0000

2



Overview | Properties | Permissions | Management

Upload | + Create folder | Download | Actions

EU (Frankfurt)

This bucket is empty. Upload new objects to get started.

Upload an object

Buckets are globally unique containers for everything that you store in Amazon S3.

Learn more

Set object properties

After you create a bucket, you can upload your objects (for example, your photo or video files).

Learn more

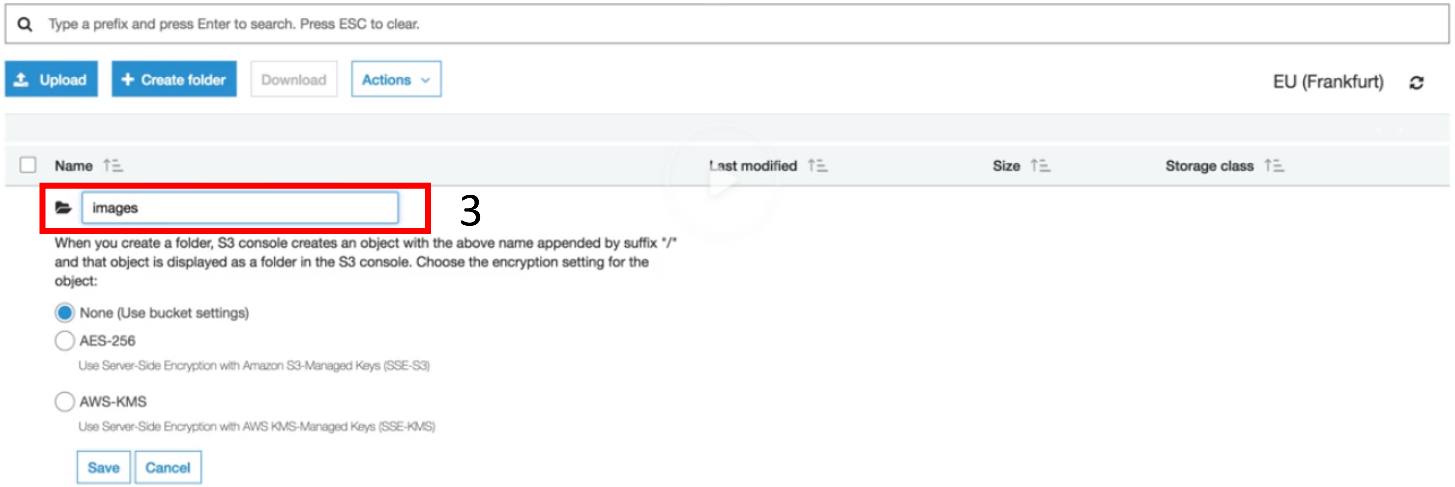
Set object permissions

By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.

Learn more

Get started

3



Type a prefix and press Enter to search. Press ESC to clear.

Upload | + Create folder | Download | Actions

EU (Frankfurt)

Name | Last modified | Size | Storage class

images

When you create a folder, S3 console creates an object with the above name appended by suffix "/" and that object is displayed as a folder in the S3 console. Choose the encryption setting for the object:

● None (Use bucket settings)

○ AES-256

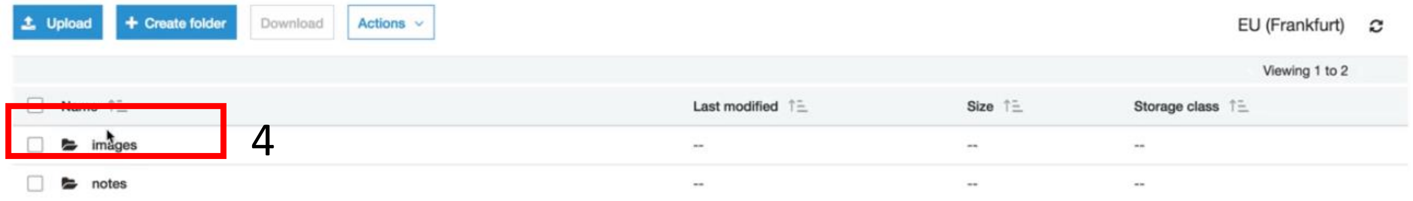
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

○ AWS-KMS

Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Save | Cancel

4



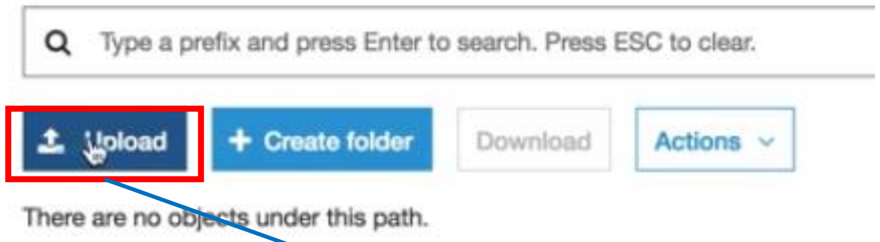
Upload | + Create folder | Download | Actions

EU (Frankfurt)

Viewing 1 to 2

Name	Last modified	Size	Storage class
images	--	--	--
notes	--	--	--

5



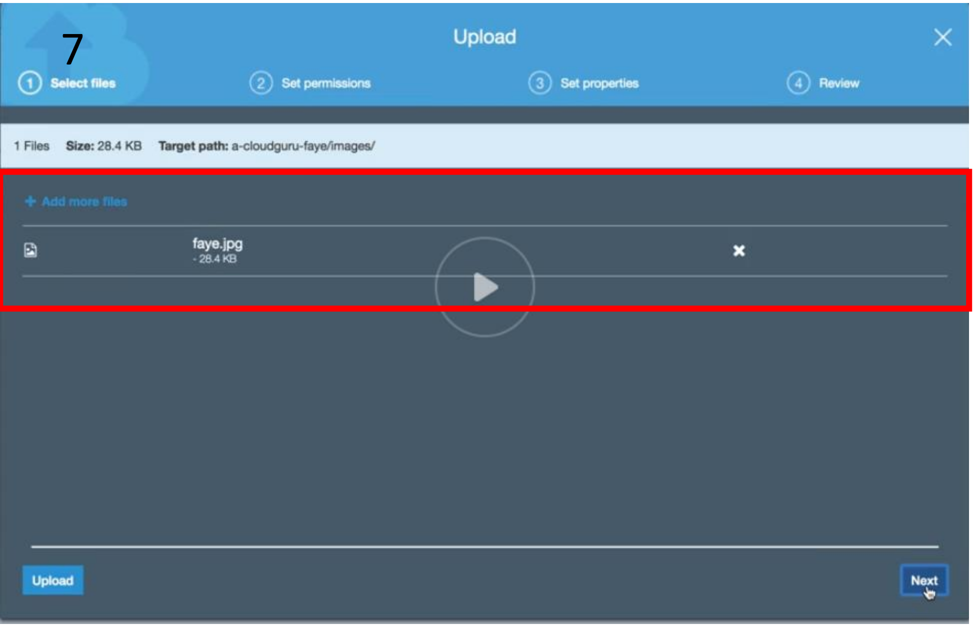
Type a prefix and press Enter to search. Press ESC to clear.

Upload | + Create folder | Download | Actions

There are no objects under this path.

6

Upload files


7

Upload

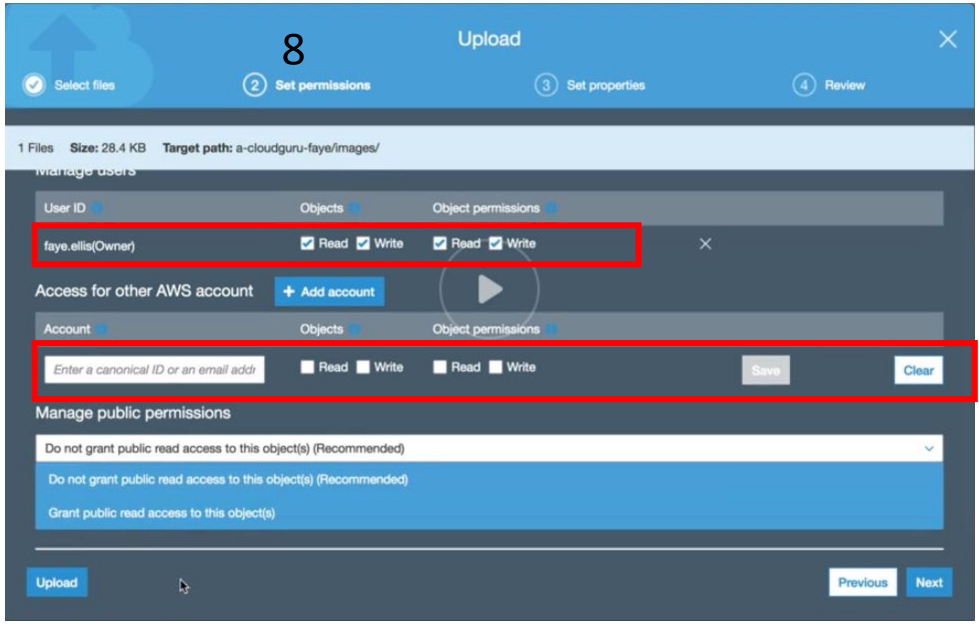
① Select files ② Set permissions ③ Set properties ④ Review

1 Files **Size:** 28.4 KB **Target path:** a-cloudguru-faye/images/

+ Add more files

faye.jpg - 28.4 KB ×

Upload Next


8

Upload

Select files ② Set permissions ③ Set properties ④ Review

1 Files **Size:** 28.4 KB **Target path:** a-cloudguru-faye/images/

Manage users

User ID	Objects	Object permissions
faye.ellis(Owner)	☑ Read ☑ Write	☑ Read ☑ Write

Access for other AWS account + Add account

Account	Objects	Object permissions
Enter a canonical ID or an email addr	□ Read □ Write	□ Read □ Write

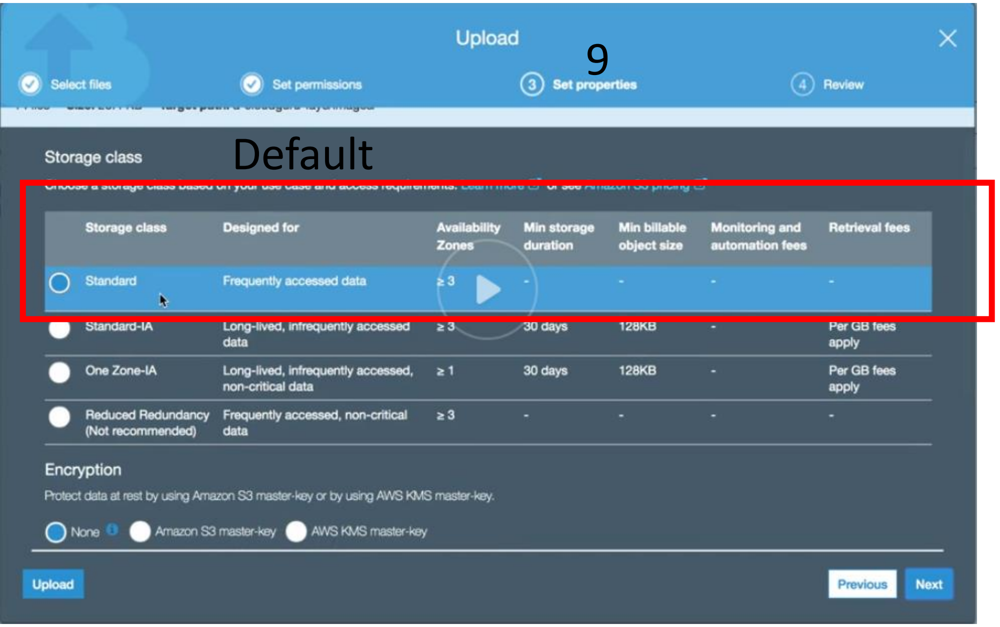
Manage public permissions

Do not grant public read access to this object(s) (Recommended)

- Do not grant public read access to this object(s) (Recommended)
- Grant public read access to this object(s)

Upload Previous Next

This is access control list and possible for – per file and per object.
By default, bucket contents are accessible by owner. We can add account and give read-write permissions to make other person accessible to the contents.


9

Upload

Select files Set permissions ③ Set properties ④ Review

Storage class

Default

Choose a storage class based on your use case and access requirements. Learn more or see Amazon S3 pricing

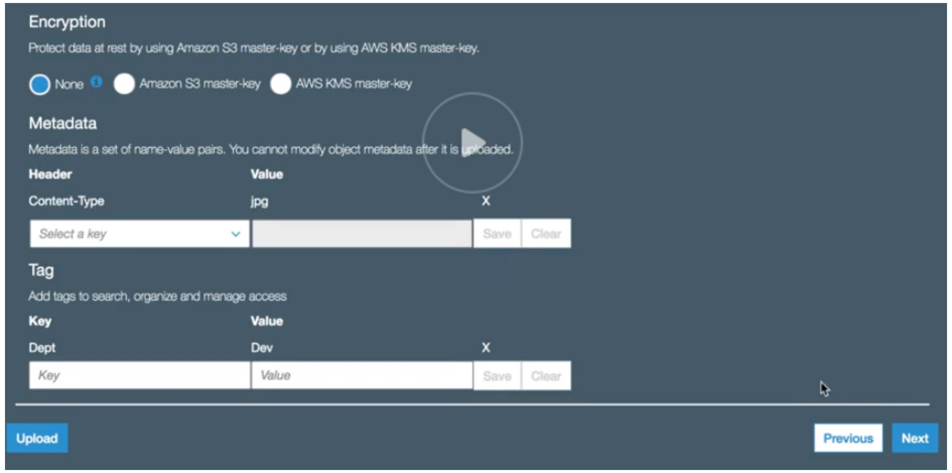
	Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
●	Standard	Frequently accessed data	≥ 3	-	-	-	-
○	Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per GB fees apply
○	One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per GB fees apply
○	Reduced Redundancy (Not recommended)	Frequently accessed, non-critical data	≥ 3	-	-	-	-

Encryption

Protect data at rest by using Amazon S3 master-key or by using AWS KMS master-key.

● None ○ Amazon S3 master-key ○ AWS KMS master-key

Upload Previous Next


Encryption

Protect data at rest by using Amazon S3 master-key or by using AWS KMS master-key.

● None ○ Amazon S3 master-key ○ AWS KMS master-key

Metadata

Metadata is a set of name-value pairs. You cannot modify object metadata after it is uploaded.

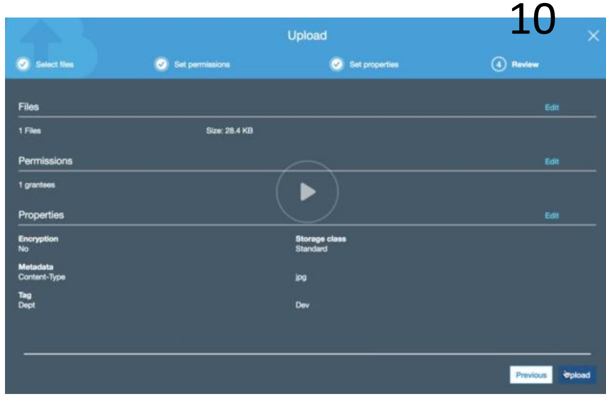
Header	Value	
Content-Type	jpg	X
Select a key		Save Clear

Tag

Add tags to search, organize and manage access

Key	Value	
Dept	Dev	X
Key	Value	Save Clear

Upload Previous Next


10

Upload

Select files Set permissions Set properties ④ Review

Files Edit

1 Files Size: 28.4 KB

Permissions Edit

1 grantees

Properties Edit

Encryption No

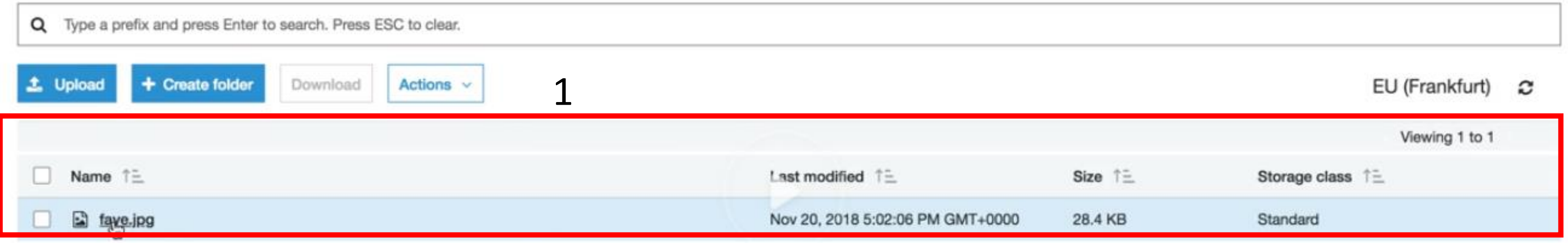
Storage class Standard

Metadata Content-Type jpg

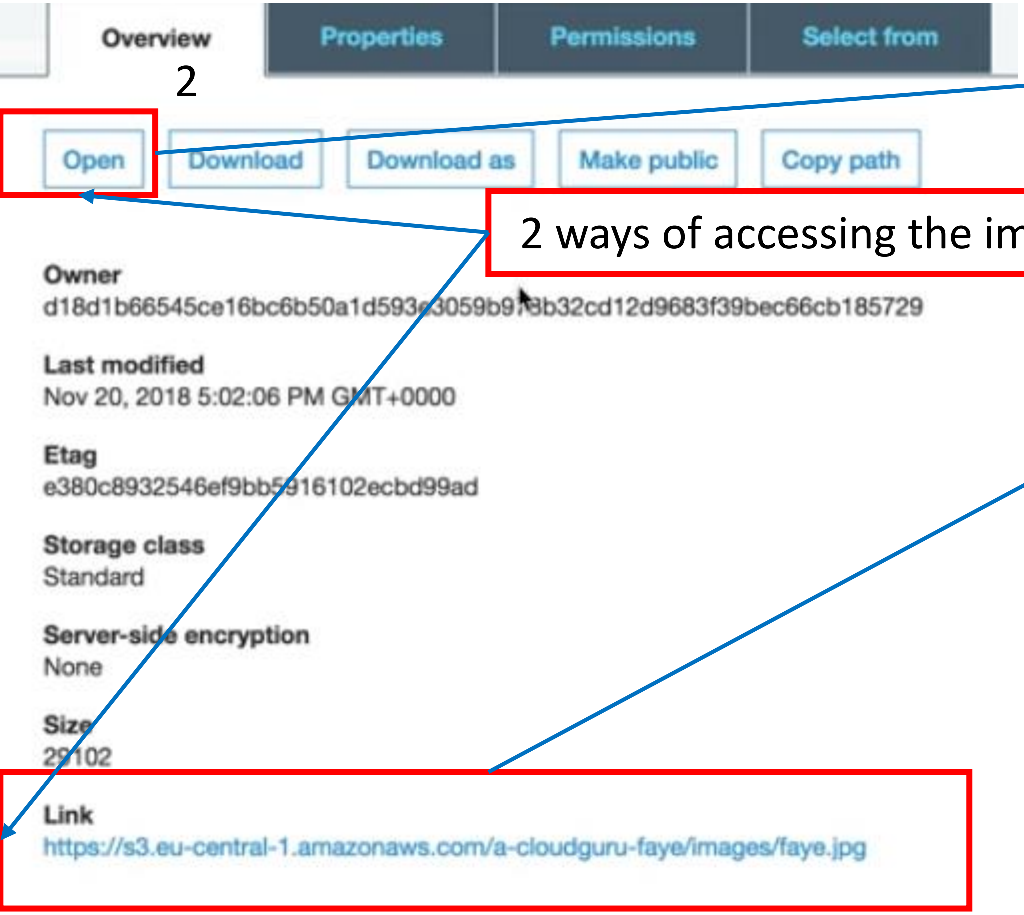
Tag Dept Dev

Previous Upload

Accessing the Bucket contents



Name	Last modified	Size	Storage class
faye.jpg	Nov 20, 2018 5:02:06 PM GMT+0000	28.4 KB	Standard



Owner
d18d1b66545ce16bc6b50a1d593e3059b978b32cd12d9683f39bec66cb185729

Last modified
Nov 20, 2018 5:02:06 PM GMT+0000

Etag
e380c8932546ef9bb5916102ecbd99ad

Storage class
Standard

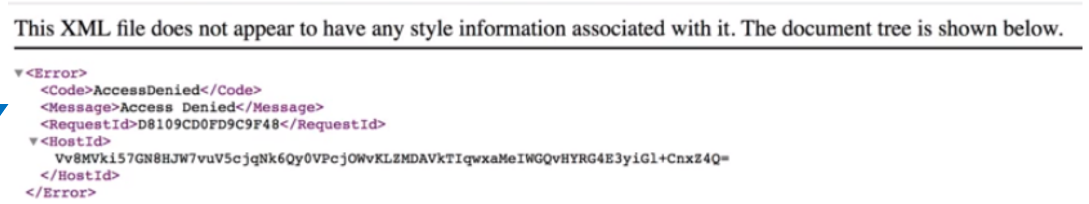
Server-side encryption
None

Size
29102

Link
https://s3.eu-central-1.amazonaws.com/a-cloudguru-faye/images/faye.jpg

Opens the image in new tab

2 ways of accessing the image

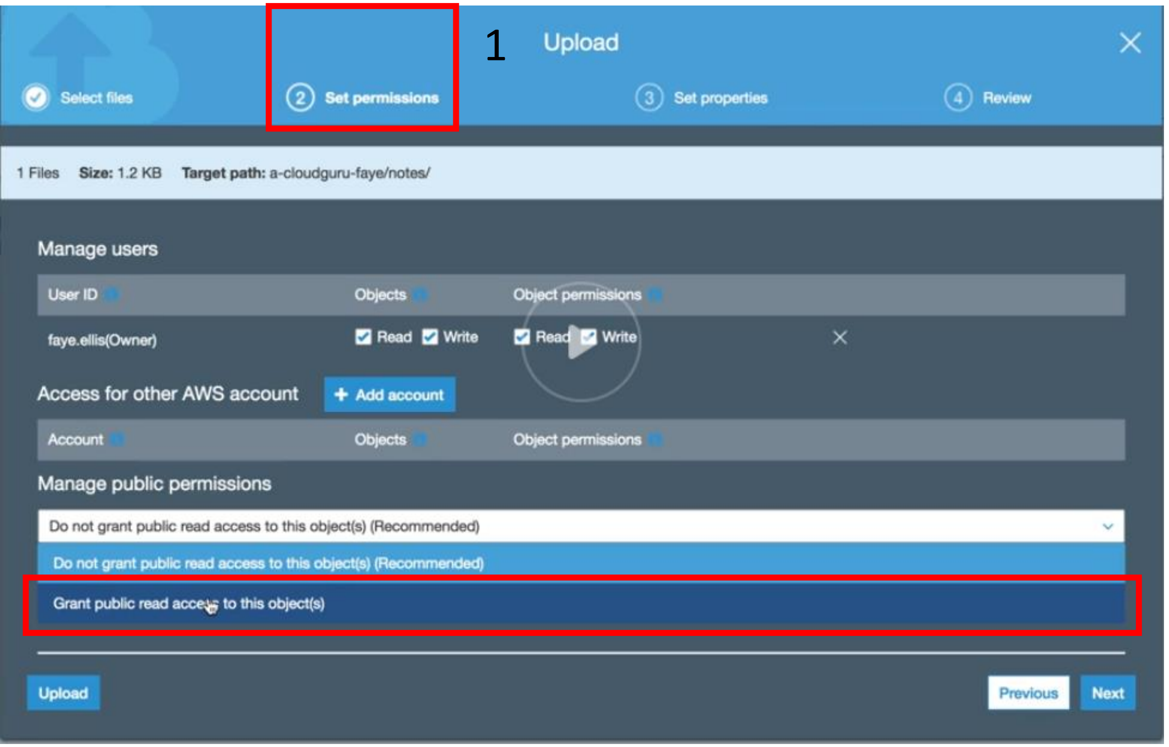


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>D8109CD0FD9C9F48</RequestId>
  ▼<HostId>
     Vv8MVki57GN8HJW7vuV5cjqNk6Qy0VPcjOWvKLZMDAVkTIqwxaMeIWGQvHYRG4E3yiGl+CnxZ4Q=
   </HostId>
 </Error>
```

We get access denied when we try to open image via link. This is because, all s3 bucket contents are not publicly available by default.

This is treated as anonymous request



1

1 Files **Size:** 1.2 KB **Target path:** a-cloudguru-faye/notes/

Manage users

User ID	Objects	Object permissions
faye.ellis(Owner)	☑ Read ☑ Write	☑ Read ☑ Write

Access for other AWS account

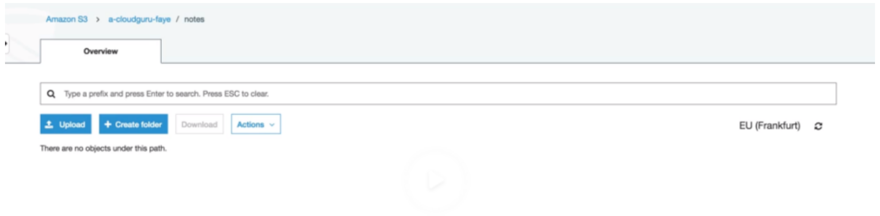
Account	Objects	Object permissions

Manage public permissions

Do not grant public read access to this object(s) (Recommended)

Do not grant public read access to this object(s) (Recommended)

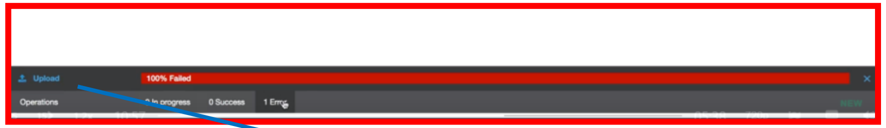
Grant public read access to this object(s)

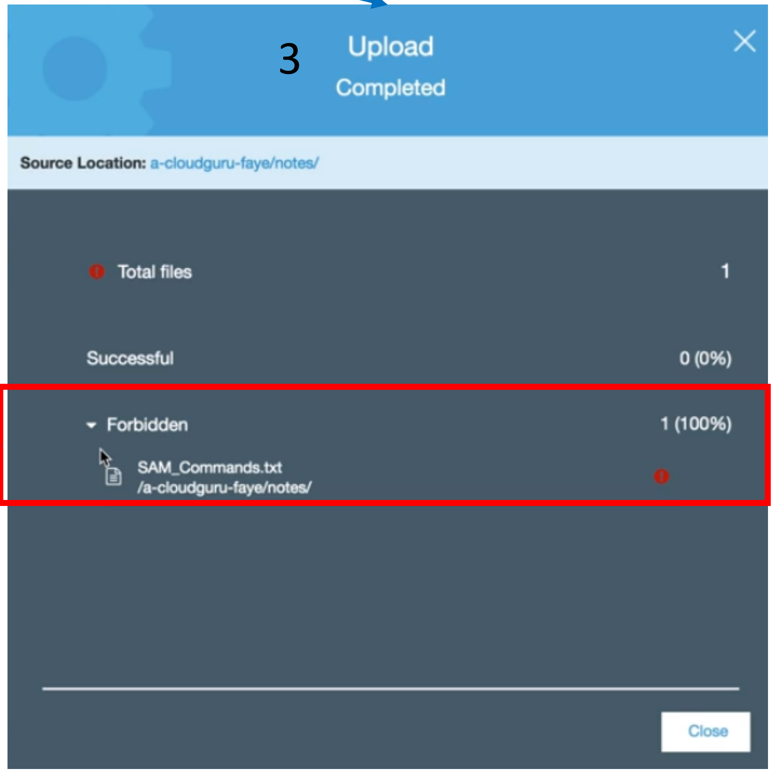


Amazon S3 > a-cloudguru-faye / notes
Overview
Type a prefix and press Enter to search. Press ESC to clear.
Upload
+ Create folder
Download
Actions
EU (Frankfurt)

There are no objects under this path.

2





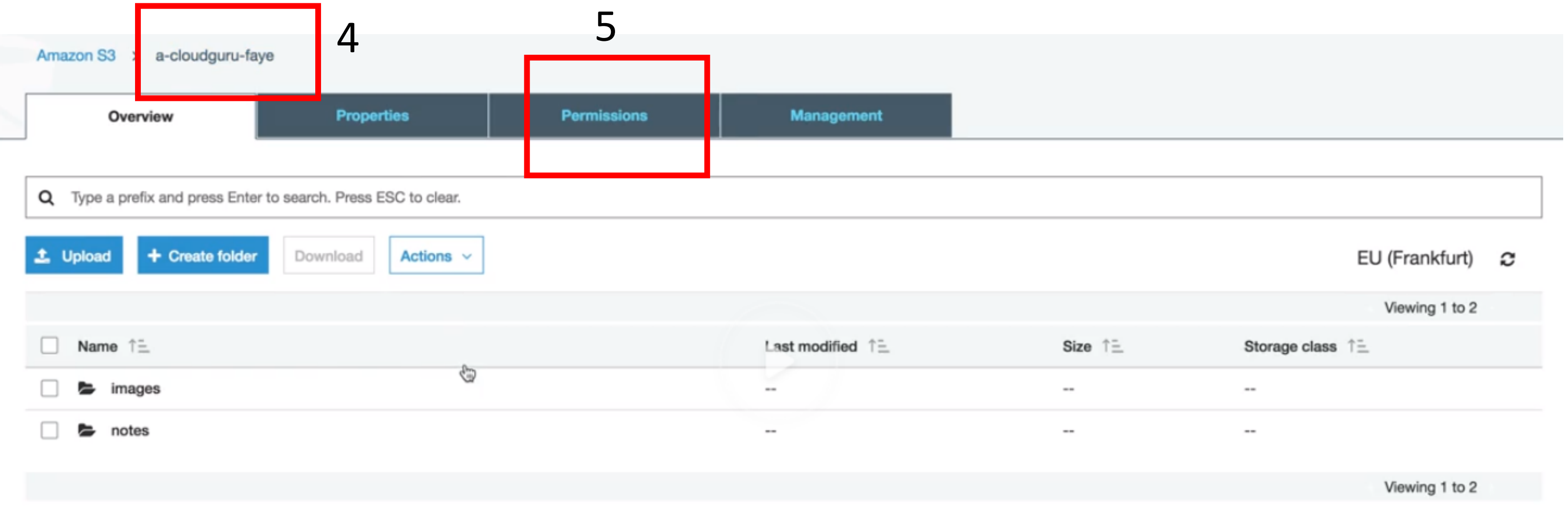
3

Upload Completed

Source Location: a-cloudguru-faye/notes/

Total files	1
Successful	0 (0%)
Forbidden	1 (100%)
SAM_Commands.txt /a-cloudguru-faye/notes/	

Uploading files that are publicly available is not the bucket policy by default and hence we get the forbidden error

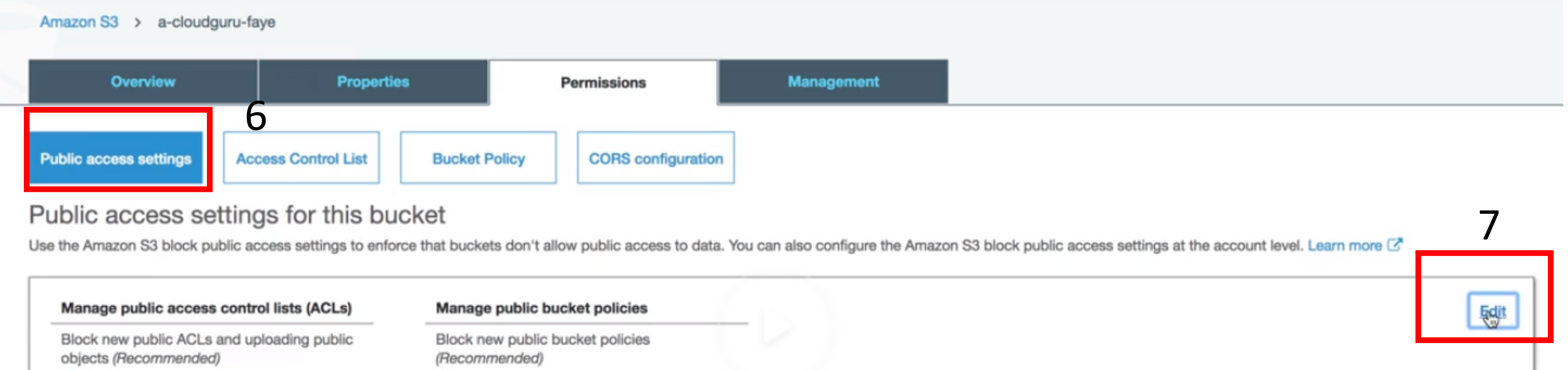


Type a prefix and press Enter to search. Press ESC to clear.

Viewing 1 to 2

	Name	Last modified	Size	Storage class
□	images	--	--	--
□	notes	--	--	--

Viewing 1 to 2



Public access settings for this bucket

Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. Learn more

Manage public access control lists (ACLs)

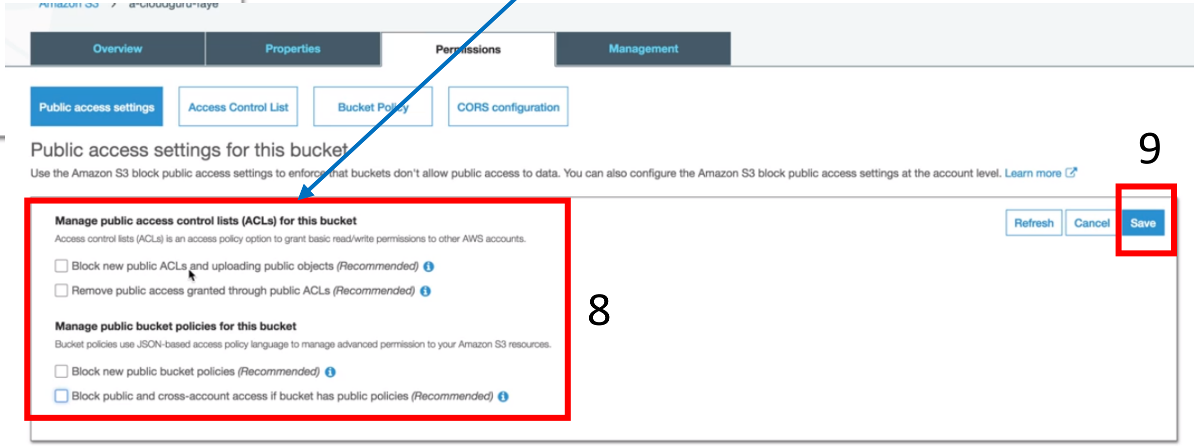
Block new public ACLs and uploading public objects *(Recommended)*
True

Remove public access granted through public ACLs *(Recommended)*
True

Manage public bucket policies

Block new public bucket policies *(Recommended)*
True

Block public and cross-account access if bucket has public policies *(Recommended)*
True



Public access settings for this bucket

Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. Learn more

Manage public access control lists (ACLs) for this bucket

Access control lists (ACLs) is an access policy option to grant basic read/write permissions to other AWS accounts.

□ Block new public ACLs and uploading public objects *(Recommended)*

□ Remove public access granted through public ACLs *(Recommended)*

Manage public bucket policies for this bucket

Bucket policies use JSON-based access policy language to manage advanced permission to your Amazon S3 resources.

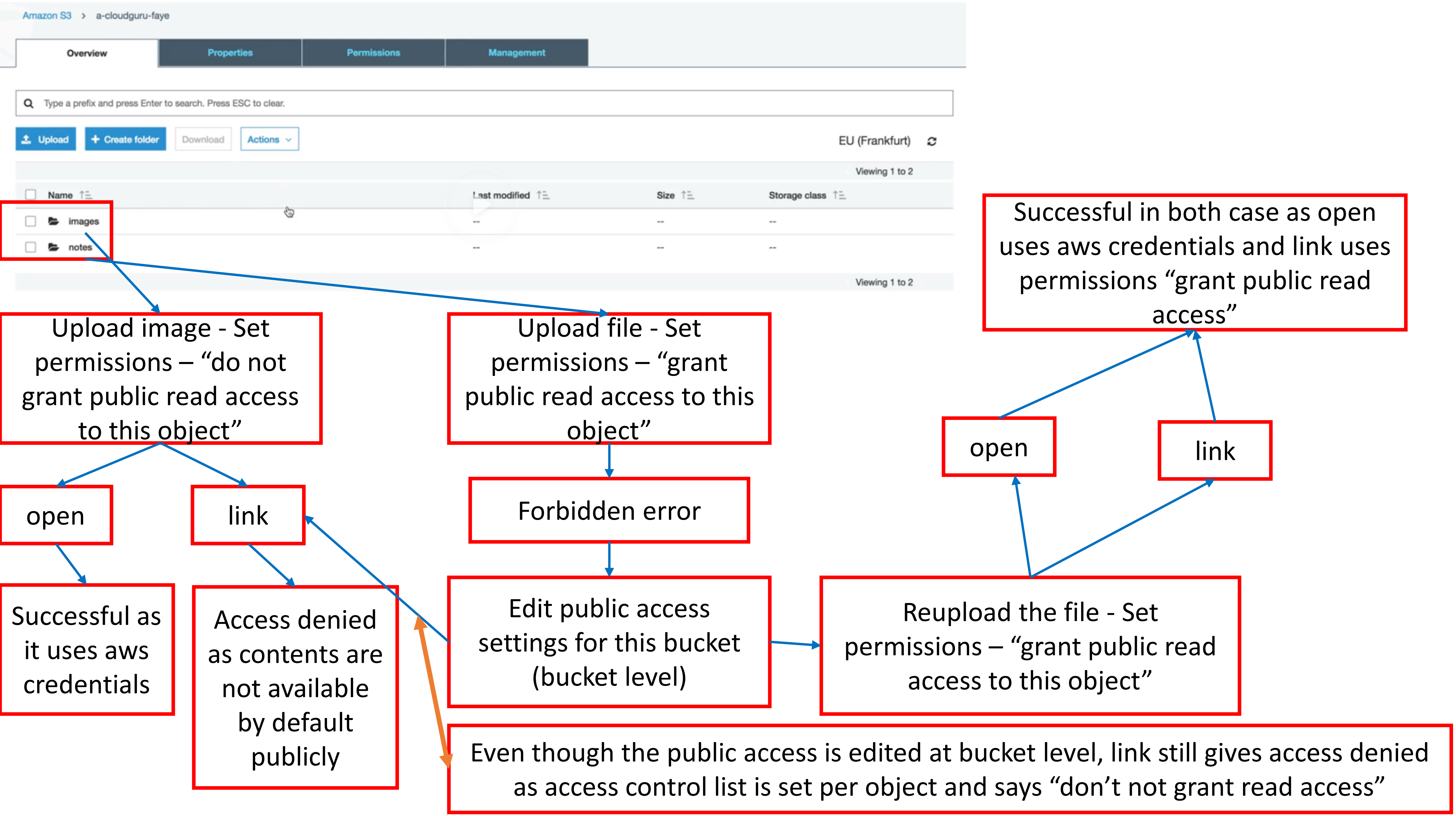
□ Block new public bucket policies *(Recommended)*

□ Block public and cross-account access if bucket has public policies *(Recommended)*

Deselect the checkboxes and save

Try uploading the file with “grant public read access to the object” and this leads to successful upload

When the content is opened with “open”, it uses aws login credentials



Type a prefix and press Enter to search. Press ESC to clear.

EU (Frankfurt)

Viewing 1 to 2

Name	Last modified	Size	Storage class
images	--	--	--
notes	--	--	--

Viewing 1 to 2

Upload image - Set permissions – “do not grant public read access to this object”

open

Successful as it uses aws credentials

link

Access denied as contents are not available by default publicly

Upload file - Set permissions – “grant public read access to this object”

Forbidden error

Edit public access settings for this bucket (bucket level)

Even though the public access is edited at bucket level, link still gives access denied as access control list is set per object and says “don’t not grant read access”

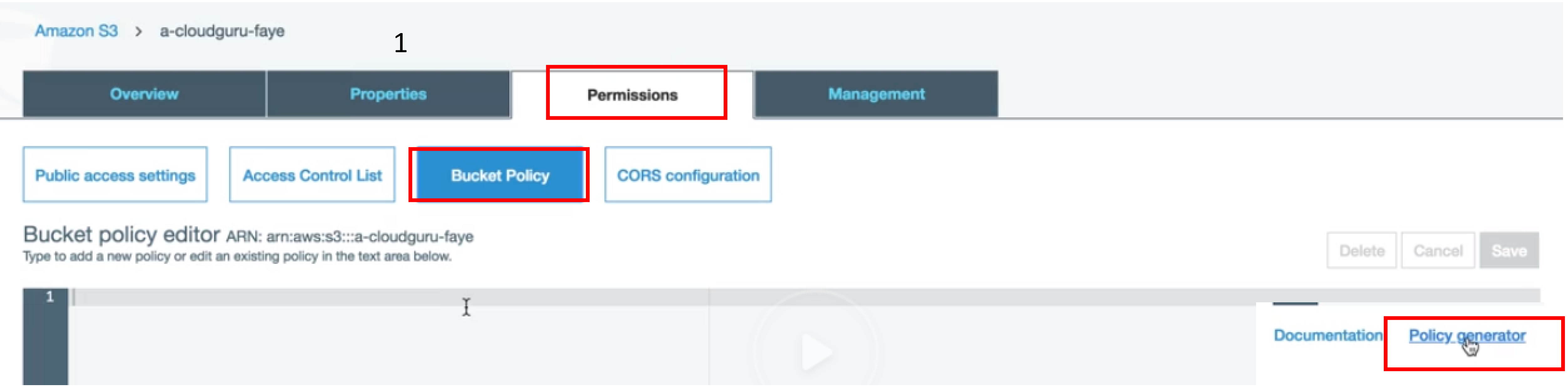
Reupload the file - Set permissions – “grant public read access to this object”

open

link

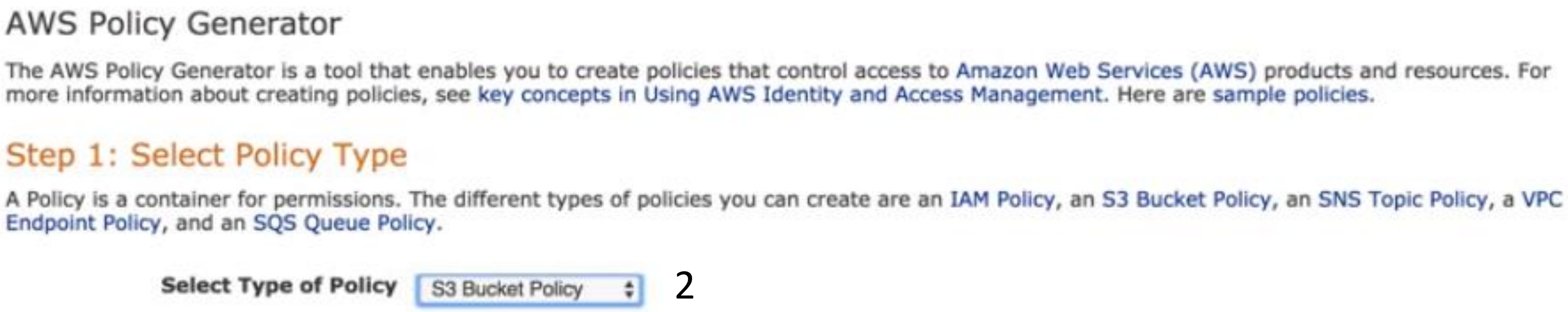
Successful in both case as open uses aws credentials and link uses permissions “grant public read access”

1



Bucket policy editor ARN: arn:aws:s3:::a-cloudguru-faye

Type to add a new policy or edit an existing policy in the text area below.



AWS Policy Generator

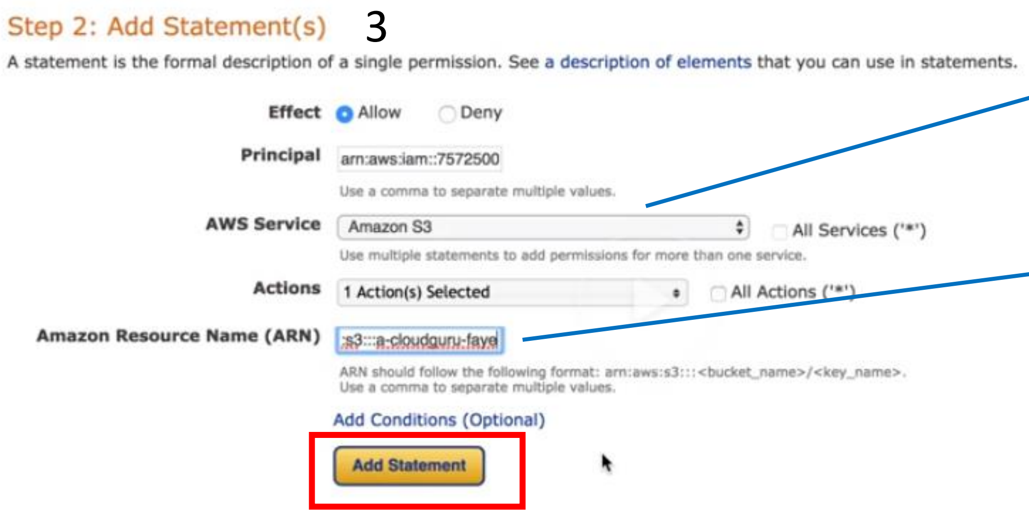
The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy

2



Step 2: Add Statement(s) 3

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect ● Allow ○ Deny

Principal arn:aws:iam::7572500

Use a comma to separate multiple values.

AWS Service Amazon S3 □ All Services ('*')

Use multiple statements to add permissions for more than one service.

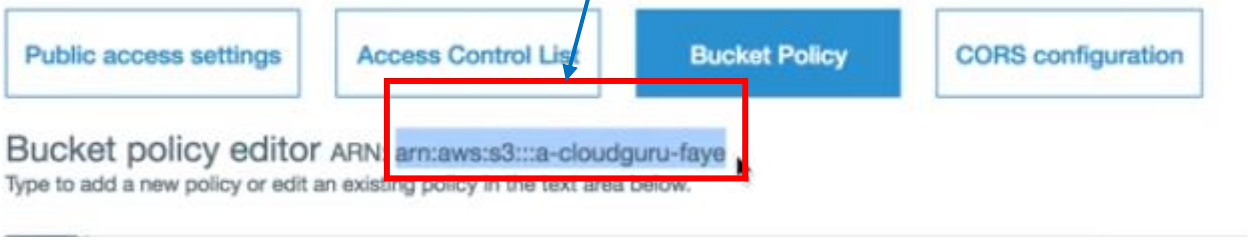
Actions 1 Action(s) Selected □ All Actions ('*')

Amazon Resource Name (ARN) :s3:::a-cloudguru-faye

ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>.
Use a comma to separate multiple values.

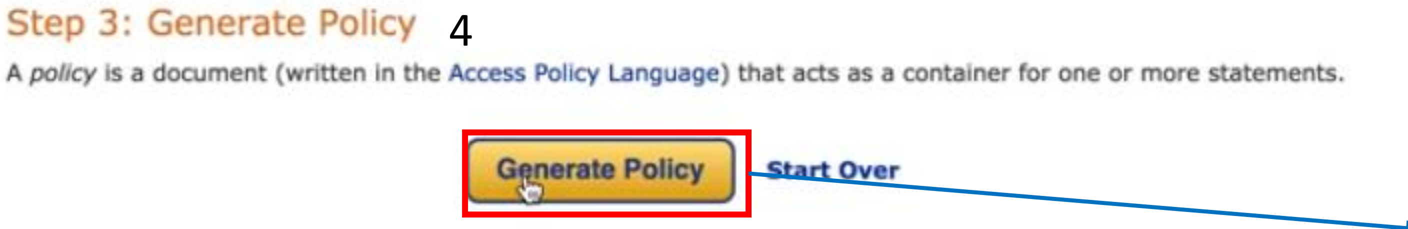
Services → IAM → users → copy the user ARN of the particular user – we are applying bucket policy to this user

We are applying permissions to -



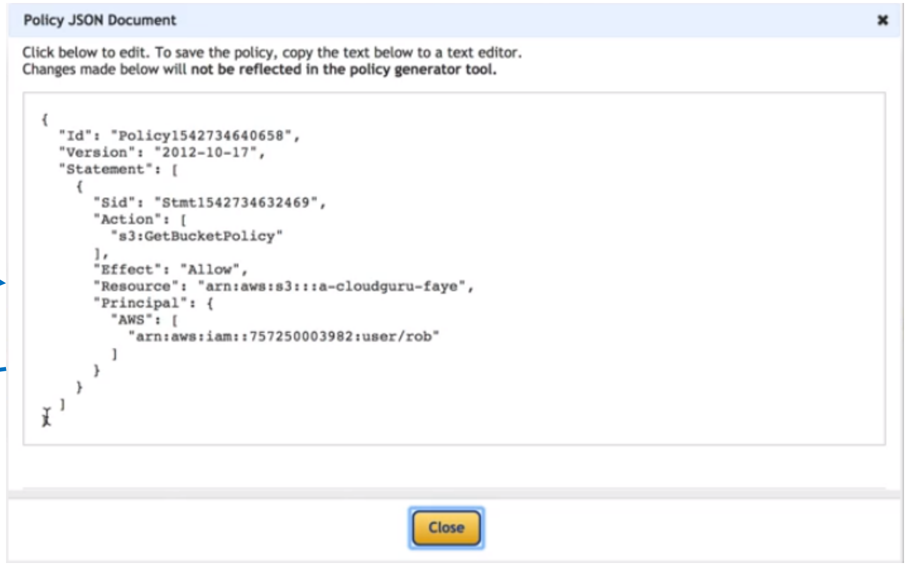
Bucket policy editor ARN: arn:aws:s3:::a-cloudguru-faye

Type to add a new policy or edit an existing policy in the text area below.



Step 3: Generate Policy 4

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.



Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```
{
  "Id": "Policy1542734640658",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1542734632469",
      "Action": [
        "s3:GetBucketPolicy"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::a-cloudguru-faye",
      "Principal": {
        "AWS": [
          "arn:aws:iam::757250003982:user/rob"
        ]
      }
    }
  ]
}
```

Copy paste the generated json into bucket policy editor