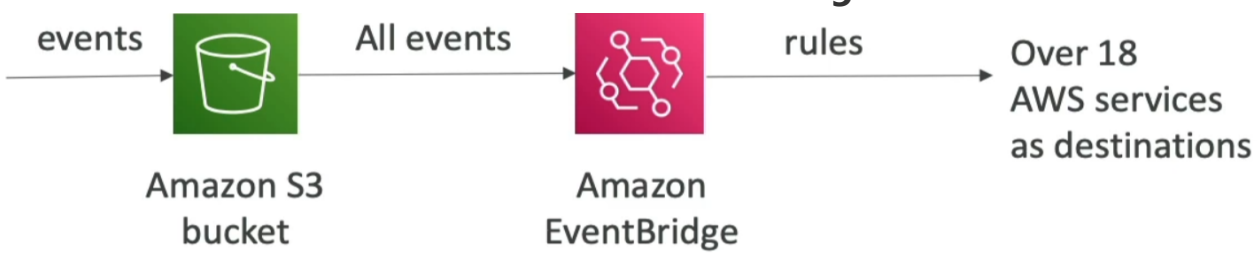
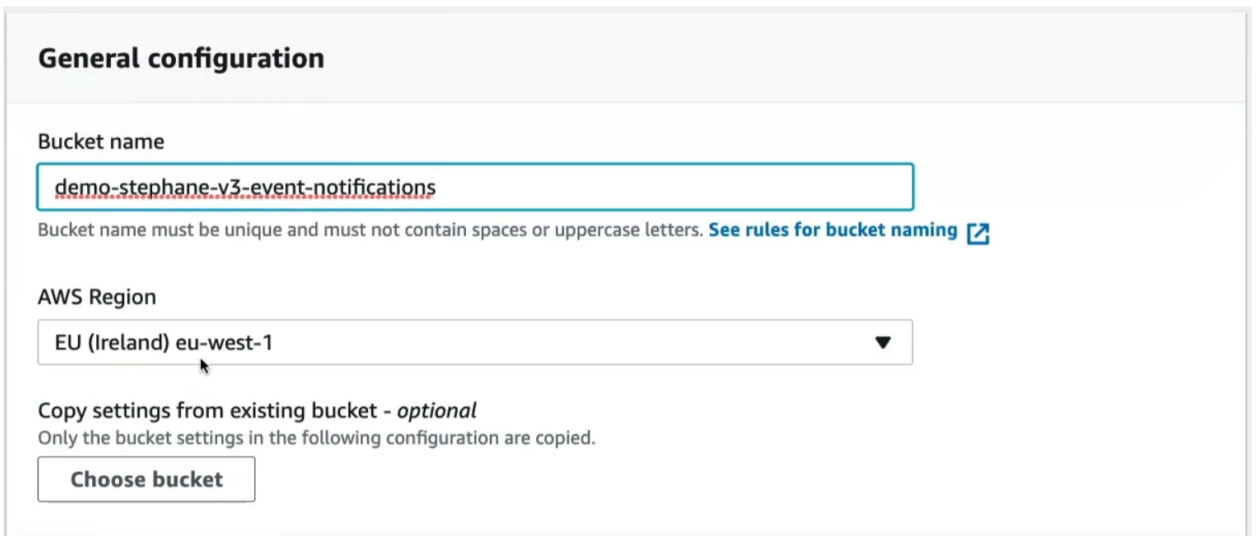
SAA-4

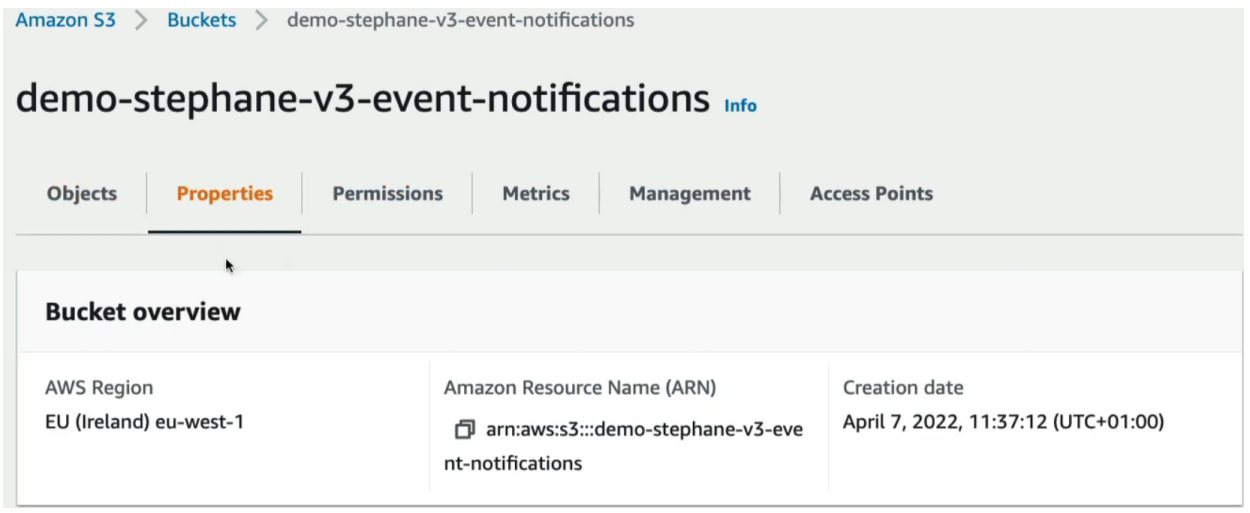
S3 Event Notifications with Amazon EventBridge

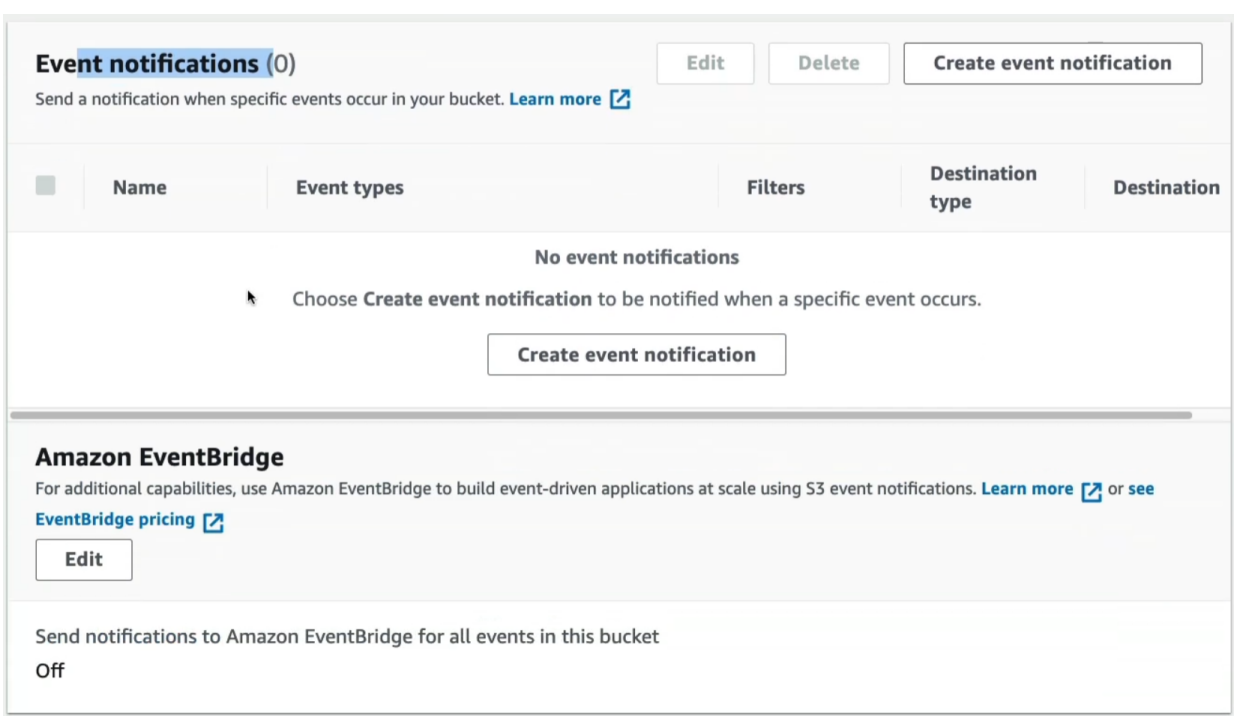


- **Advanced filtering** options with JSON rules (metadata, object size, name ...)
- **Multiple Destinations** - ex Step Functions, Kinesis Stream / Firehose
- **EventBridge Capabilities** -Archive, Replay Events, Reliable delivery

Hands on







Amazon EventBridge

For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. Learn more or see EventBridge pricing

Edit

Send notifications to Amazon EventBridge for all events in this bucket

Off

Edit Amazon EventBridge Info

Amazon EventBridge

For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. Learn more or see EventBridge pricing

Send notifications to Amazon EventBridge for all events in this bucket

- ○ Off
- ◉ On

Cancel | Save changes

Event notifications (0)

Send a notification when specific events occur in your bucket. Learn more

Edit | Delete | Create event notification

Name	Event types	Filters	Destination type	Destination

No event notifications

Choose **Create event notification** to be notified when a specific event occurs.

Create event notification

General configuration

Event name

DemoEventNotification

Event name can contain up to 255 characters.

Prefix - *optional*

Limit the notifications to objects with key starting with specified characters.

images/

Suffix - *optional*

Limit the notifications to objects with key ending with specified characters.

.jpg

Event types

Specify at least one event for which you want to receive notifications. For each group, you can choose an event type for all events, or you can choose one or more individual events.

Object creation

- ☑ All object create events
  s3:ObjectCreated:*
- ☐ Put
  s3:ObjectCreated:Put
- ☐ Post
  s3:ObjectCreated:Post
- ☐ Copy
  s3:ObjectCreated:Copy
- ☐ Multipart upload completed
  s3:ObjectCreated:CompleteMultipartUpload

Object removal

- ☐ All object removal events
  s3:ObjectRemoved:*
- ☐ Permanently deleted
  s3:ObjectRemoved:Delete
- ☐ Delete marker created
  s3:ObjectRemoved:DeleteMarkerCreated

Object restore

Destination

Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. Learn more

Destination
Choose a destination to publish the event. **Learn more**

- ○ **Lambda function**
  Run a Lambda function script based on S3 events.
- ○ **SNS topic**
  Send notifications to email, SMS, or an HTTP endpoint.
- ◉ **SQS queue**
  Send notifications to an SQS queue to be read by a server.

Specify SQS queue

- ◉ Choose from your SQS queues
- ○ Enter SQS queue ARN

SQS queue

Choose SQS queue ▼

Cancel | **Save changes**

Amazon SQS > Queues

Queues (1) — Edit | Delete | Send and receive messages | Actions | **Create queue**

Search queues by prefix — 1

Name	Type	Created	Messages available	Messages in flight	Encryption	Content-based deduplication
○ test	Standard	4/7/2022, 10:47:55 GMT+1	0	0	Disabled	-

◉ **Standard** Info
At-least-once delivery, message ordering isn't preserved
- At-least once delivery
- Best-effort ordering

○ **FIFO** Info
First-in-first-out delivery, message ordering is preserved
- First-in-first-out delivery
- Exactly-once processing

Name

DemoS3Notification

A queue name is case-sensitive and can have up to 80 characters. You can use alphanumeric characters, hyphens (-), and underscores (_).

Configuration

Set the maximum message size, visibility to other consumers, and message retention. Info

Visibility timeout Info — 30 — Seconds
Should be between 0 seconds and 12 hours.

Message retention period Info — 4 — Days
Should be between 1 minute and 14 days.

Delivery delay Info — 0 — Seconds

Maximum message size Info — 256 — KB

Access policy

Define who can access your queue. Info

```
  "Id": "Policy1649328102124",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1649328100474",
      "Action": [
        "sqs:SendMessage"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sqs:eu-west-1:783768293452:DemoS3Notification",
      "Principal": "*"
    }
  ]
}
```

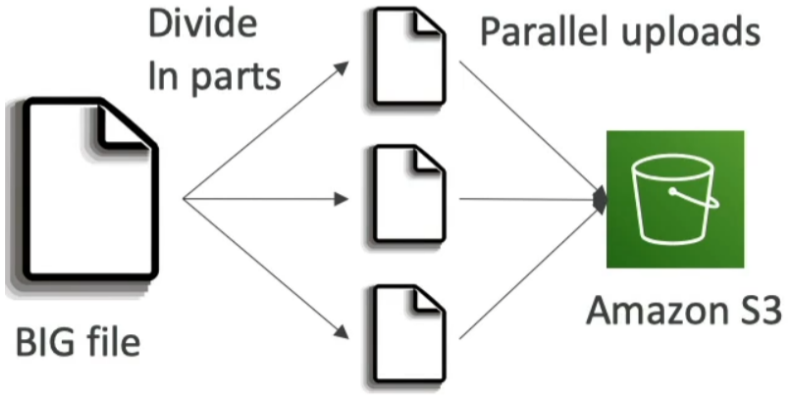
Policy generator

S3 - Baseline Performance

- Amazon S3 automatically scales to high request rates, latency 100-200 ms
- Your application can achieve at least **3500 PUT/COPY/POST/DELETE and 5500 GET/HEAD requests per second per prefix in a bucket**
- There are no limits to the number of prefixes in a bucket
- Example (object path => prefix):
  - bucket/folder1/sub1/file => /folder1/sub1/
  - bucket/folder1/sub2/file => /folder1/sub2/
  - bucket/1/file => /1/
  - bucket/2/file => /2/
- If you spread reads across all four prefixes evenly, you can achieve 22000 requests per second for GET and HEAD

S3 Performance

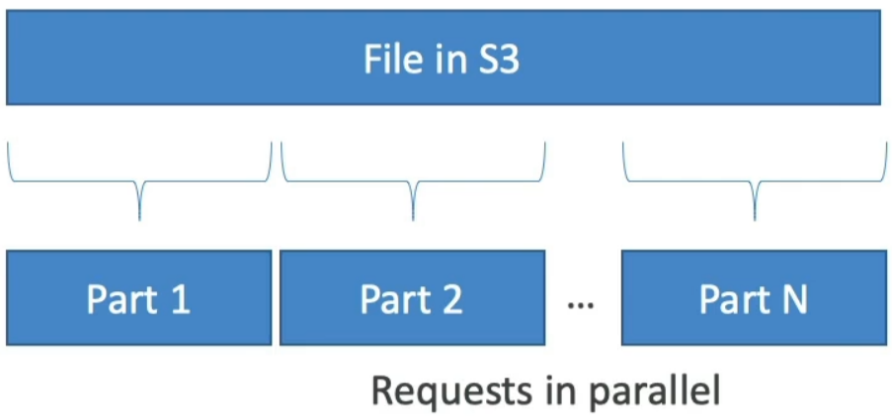
- Multi-Part upload:
  - recommended for files > 100MB,must use for files > 5GB
  - Can help parallelize uploads (speed up transfers)



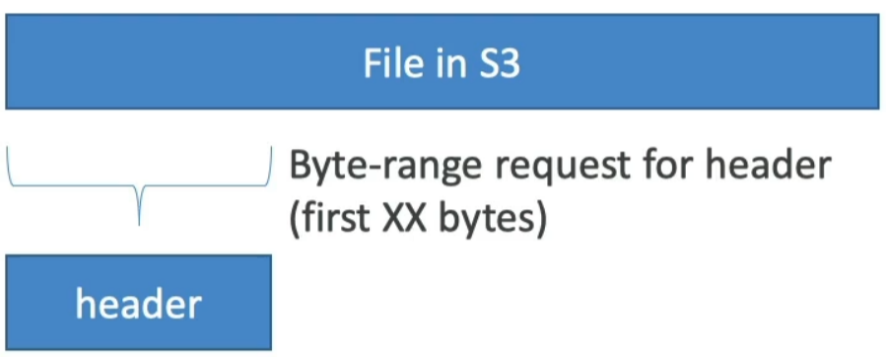
- S3 Transfer Acceleration
  - Increase transfer speed by transferring file to an AWS edge location which will forward the data to the S3 bucket in the target region
  - Compatible with multi-part upload

- S3 Byte-Range Fetches
  - Parallelize GETs by requesting specific byte ranges
  - Better resilience in case of failures

  Can be used to speed up downloads



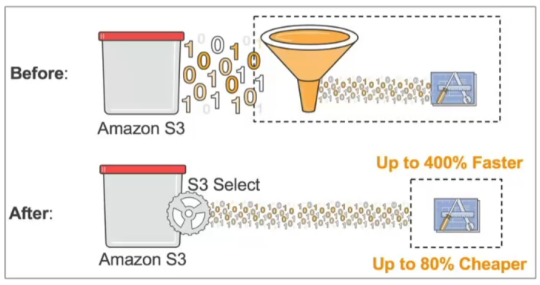
  Can be used to retrieve only partial data (for example the head of a file)



S3 Select & Glacier Select

- Retrieve less data using SQL by performing server-side filtering

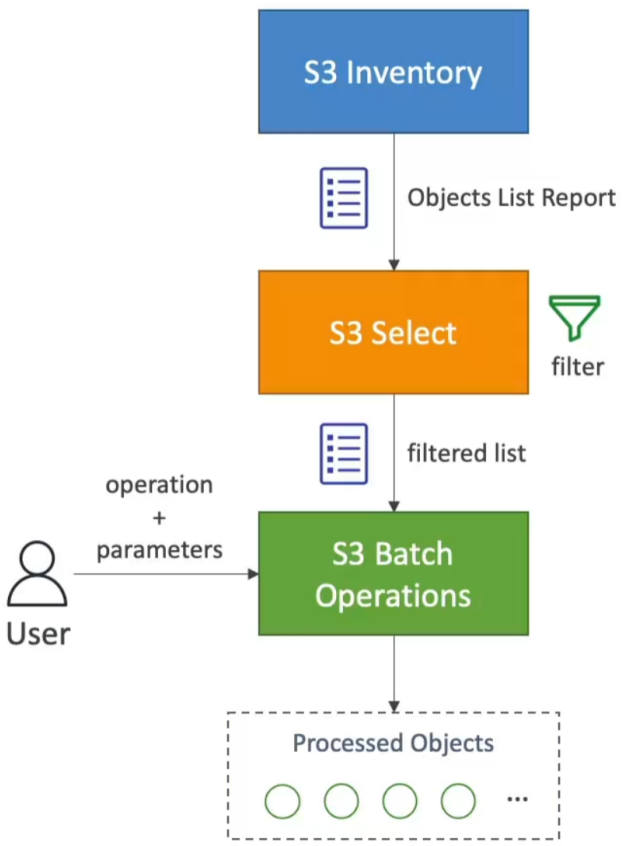
- Can filter by rows & columns (simple SQL statements)
- Less network transfer, less CPU cost client-side



https://aws.amazon.com/blogs/aws/s3-glacier-select/

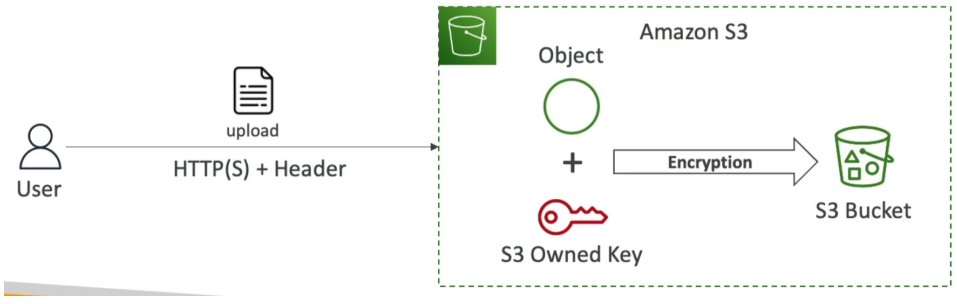
S3 Batch Operations

- Perform bulk operations on existing S3 objects with a single request,example:
  - Modify object metadata & properties
  - Copy objects between S3 buckets
  - Encrypt un-encrypted objects
  - Modify ACLs,tags
  - Restore objects from S3 Glacier
  - Invoke Lambda function to perform custom action on each object
- A job consists of a list of objects, the action to perform, and optional parameters
- S3 Batch Operations manages retries, tracks progress, sends completion notifications,generate reports ...
- **You can use S3 Inventory to get object list and use S3 Select to filter your objects**



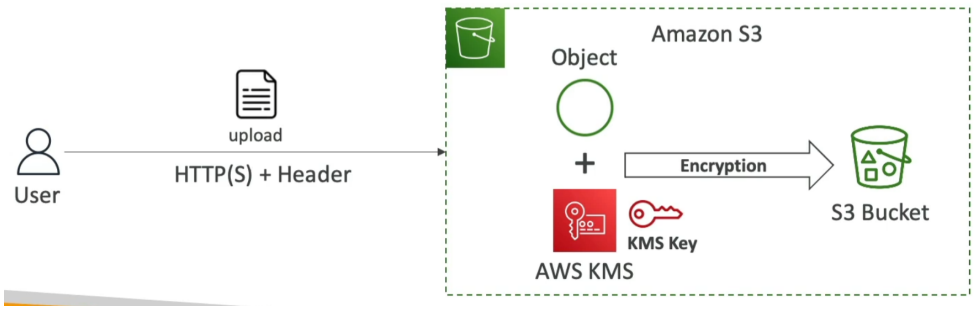
Amazon S3 - Object Encryption

- You can encrypt objects in S3 buckets using one of 4 methods
- **Server-Side Encryption (SSE)**
  - **Server-Side Encryption with Amazon S3 - Managed Keys (SSE-S3)**
    - Encrypts S3 objects using keys handled, managed, and owned by AWS
    - Object is encrypted server-side
    - Encryption type is AES-256
    - Must set header "x-amz-server-side-encryption":"AES256"

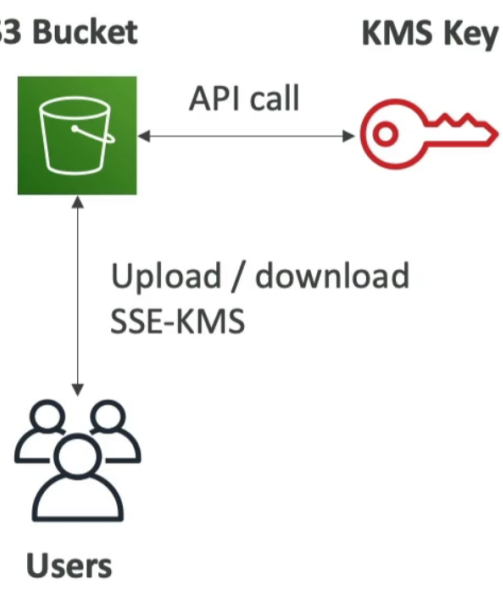


  - **Server-Side Encryption with KMS Keys stored in AWS KMS (SEE-KMS)**
    - Leverage AWS Key Management Service (AWS KMS) to manage encryption keys

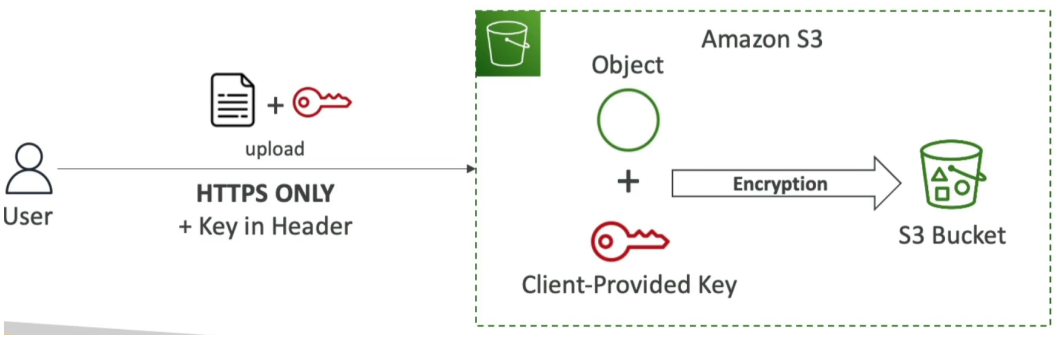
- Encryption using keys handled and managed by AWS KMS (Key Management Service)
- KMS advantages: user control + audit key usage using CloudTrail
- Object is encrypted server side
- Must set header **"x-amz-server-side-encryption":"aws:kms"**



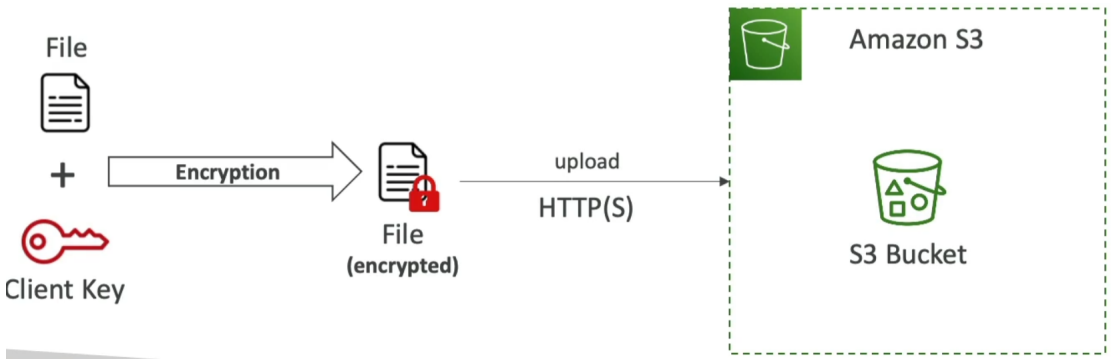
- **SSE-KMS Limitation**
  - If you use SSE-KMS, you may ve impacted by the KMS limits
  - When you upload, it calls the **GenerateDataKey** KMS API
  - when you download,it calls the Decrypt KMS API
  - Count towards the KMS quota per second (5500, 10000, 30000 req/s based on region)
  - You can request a quota increase using the Service Quotas Console



  - **Server-Side Encryption with Customer-Provided Keys (SSE-C)**
    - When you want to manage your own encryption keys
    - Server-Side Encryption using keys fully managed by the customer outside of AWS
    - Amazon S3 does **NOT** store the encryption key you provide
    - **HTTPS must be used**
    - Encryption key must provided in HTTP headers, for every HTTP request made



- **Client-Side Encryption**
  - Use client libraries such as **Amazon S3 Client-Side Encryption Library**
  - Client must encrypt data themselves before sending to Amazon S3
  - Client must decrypt data themselves when retrieving from Amazon S3
  - Customer fully manages the keys and encryption cycle

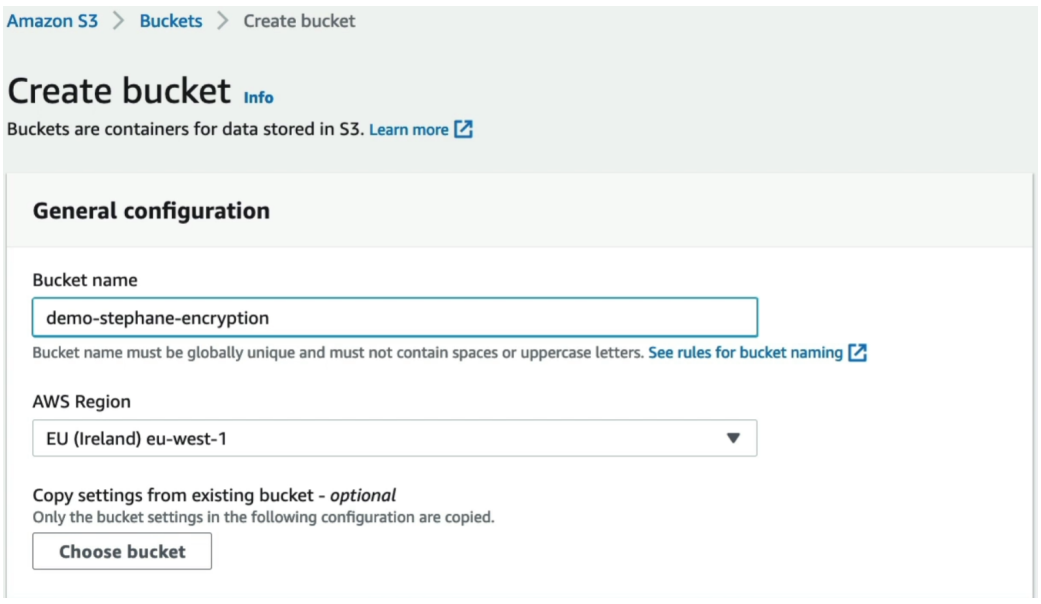


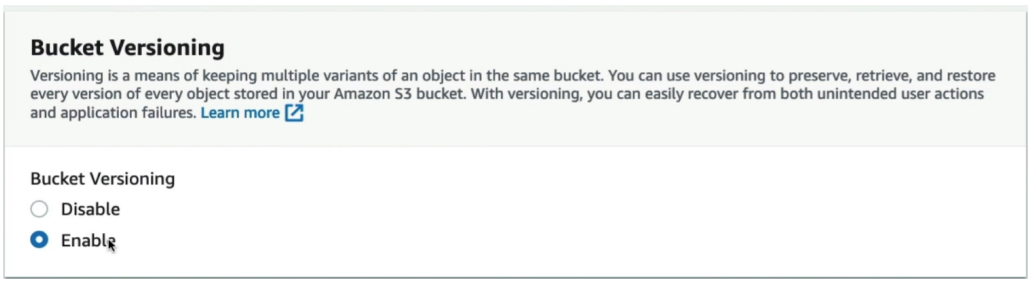
- It's important to understand which ones are for which situation for exam

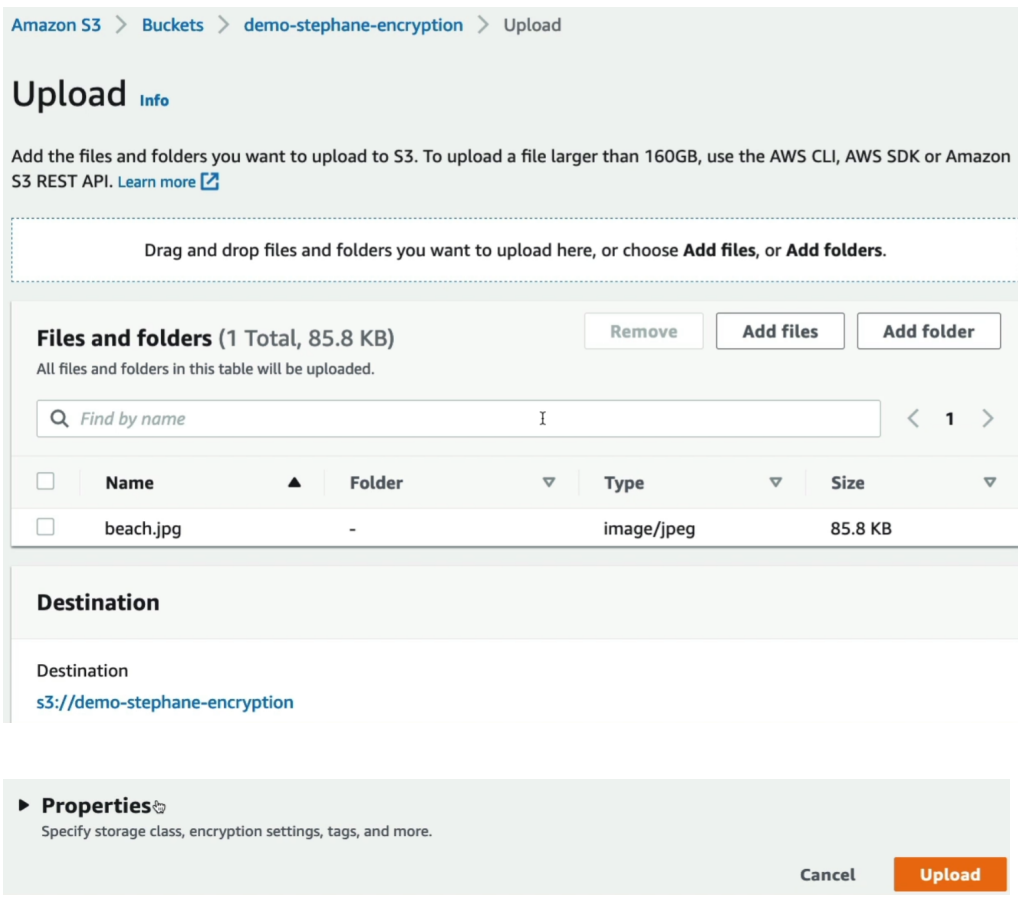
Amazon S3 - Encryption in transit (SSL/TLS)

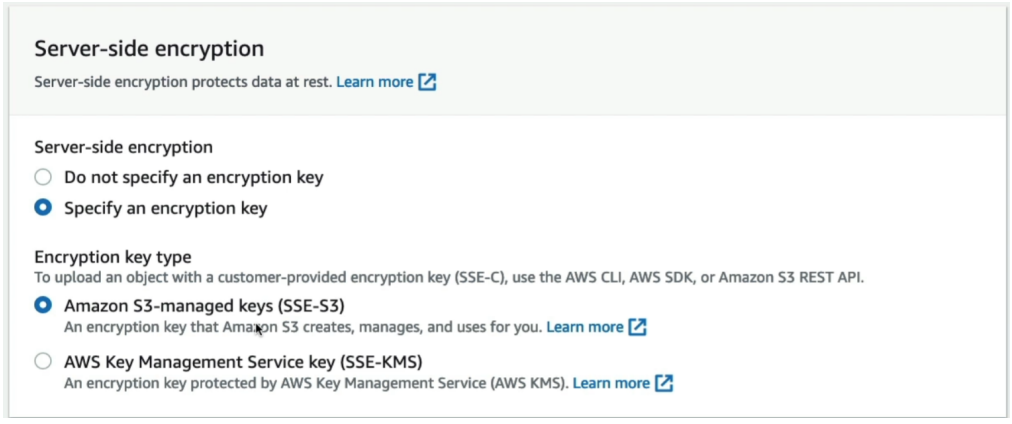
- Encryption in flight is also called SSL/TLS
- Amazon S3 exposes two endpoints:
  - HTTP Endpoint - non encrypted
  - HTTPS Endpoint - encryption in flight
- **HTTPS is recommended**
- **HTTPS is mandatory for SSE-C**
- Most clients would use the HTTPS endpoint by default

Hands on

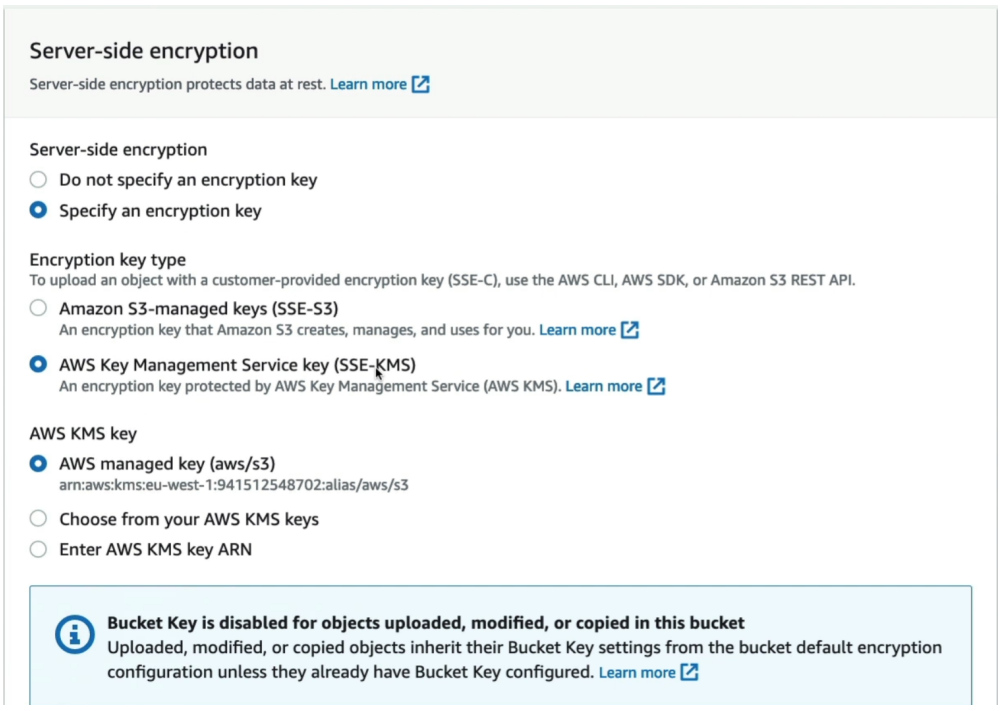


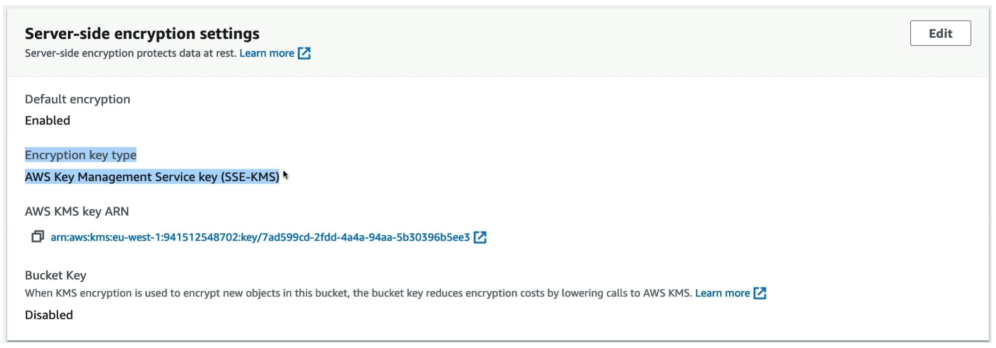




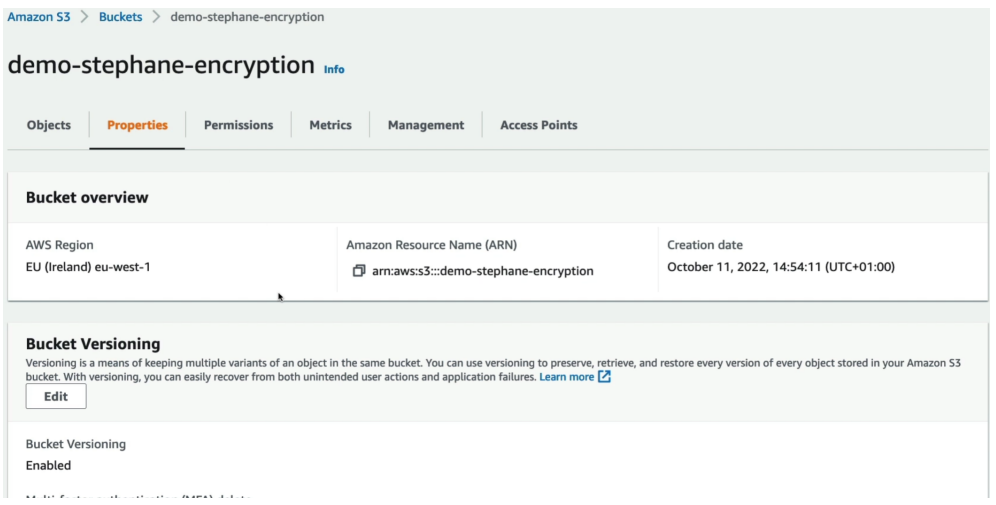


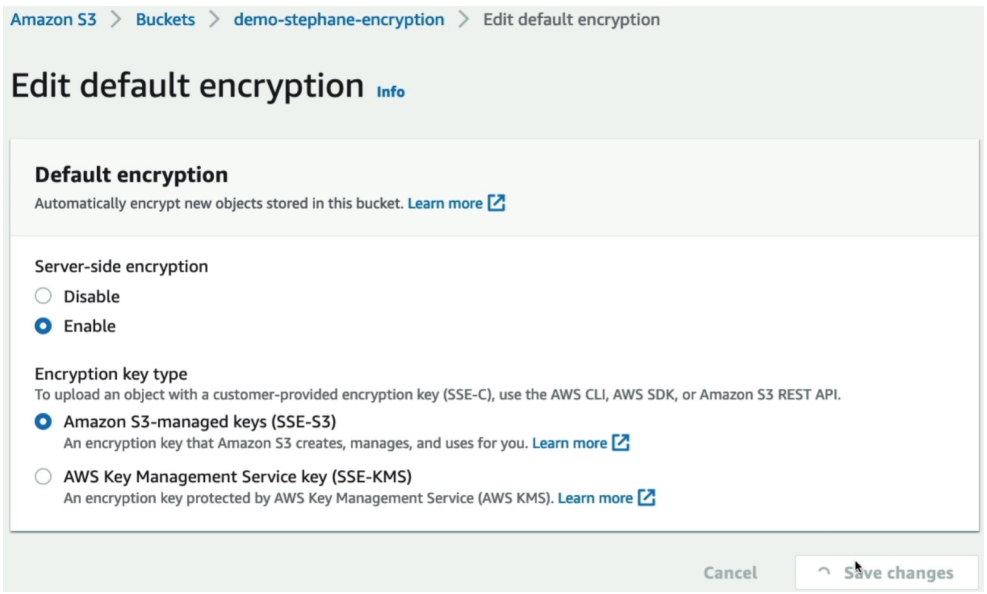
SEE-KMS





Edit with Properties





To upload an object with a **customer-provided encryption key (SSE-C)**, use the AWS CLI,AWS SDK,or Amazon S3 REST API

Amazon S3 - Default Encryption vs. Bucket Policies

- One way to "force encryption" is to use a bucket policy and refuse any API call to PUT an S3 object without encryption headers

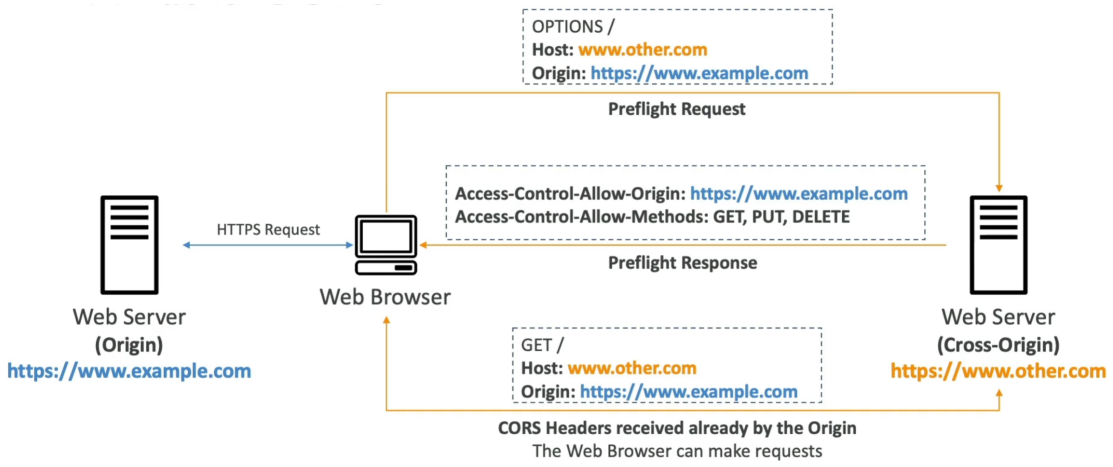
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyIncorrectDecryptionHeader",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [ "s3:PutObject" ],
            "Resource": [ "arn:aws:s3:::examplebucket/*" ],
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "AES256"
                }
            }
        }
    ]
}
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyUnencryptedObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [ "s3:PutObject" ],
            "Resource": [ "arn:aws:s3:::examplebucket/*" ],
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption": true
                }
            }
        }
    ]
}
```

- Another way is to use the "default encryption" option in S3
- **Note: Bucket Policies are evaluated before "default encryption"**

What is CORS?

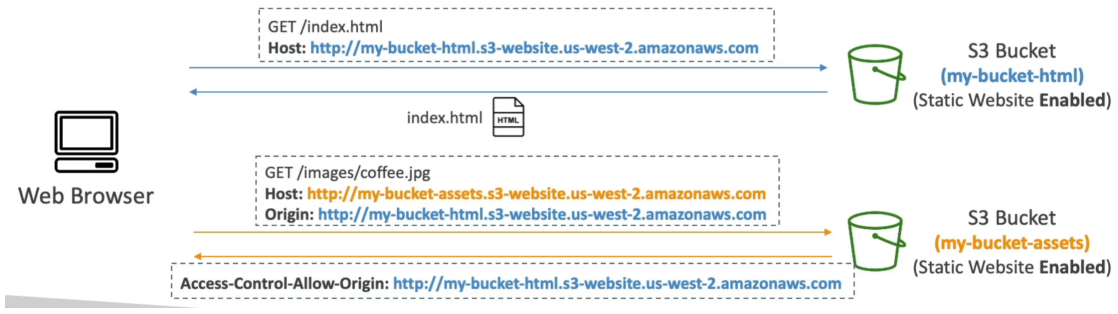
- **Cross-Origin Resource Sharing(CORS)**
- **Origin = scheme(protocol) + host (domain) + port**
- example:https://www.example.com (implied port is 443 for HTTPS, 80 for HTTP)
- **Web Browser** based mechanism to allow requests to other origins while visiting the main origin
- Same origin: http://example.com/app1 & http://other.example.com/app2
- Different origins:http://example.com& http://other.example.com
- The requests won't be fulfilled unless the other origin allows for the requests,using CORS Headers(example: **Access-Control-Allow-Origin**)



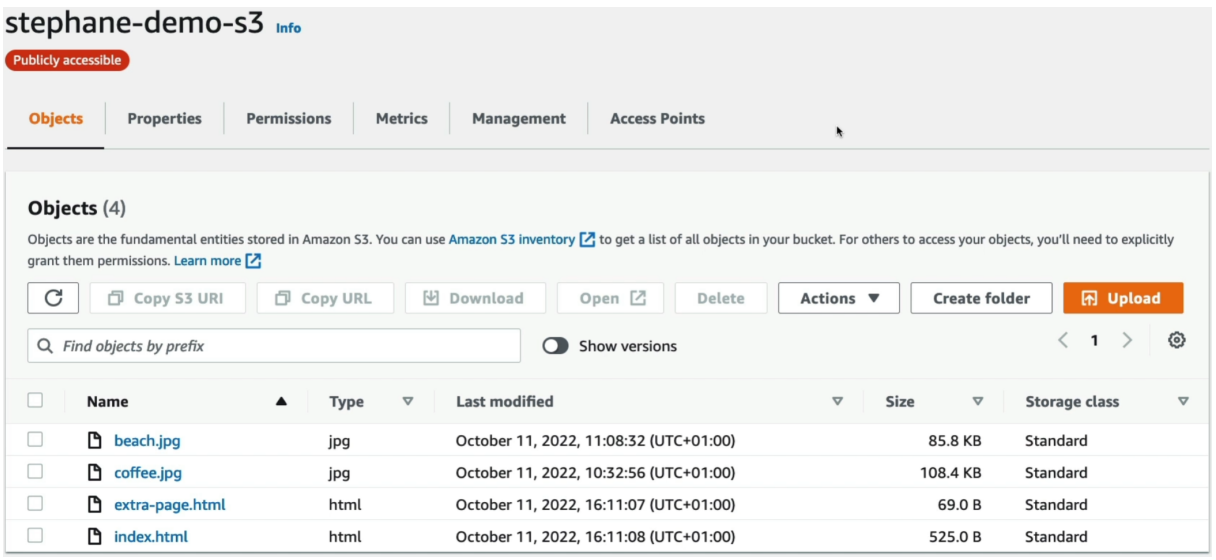
Amazon S3 - CORS

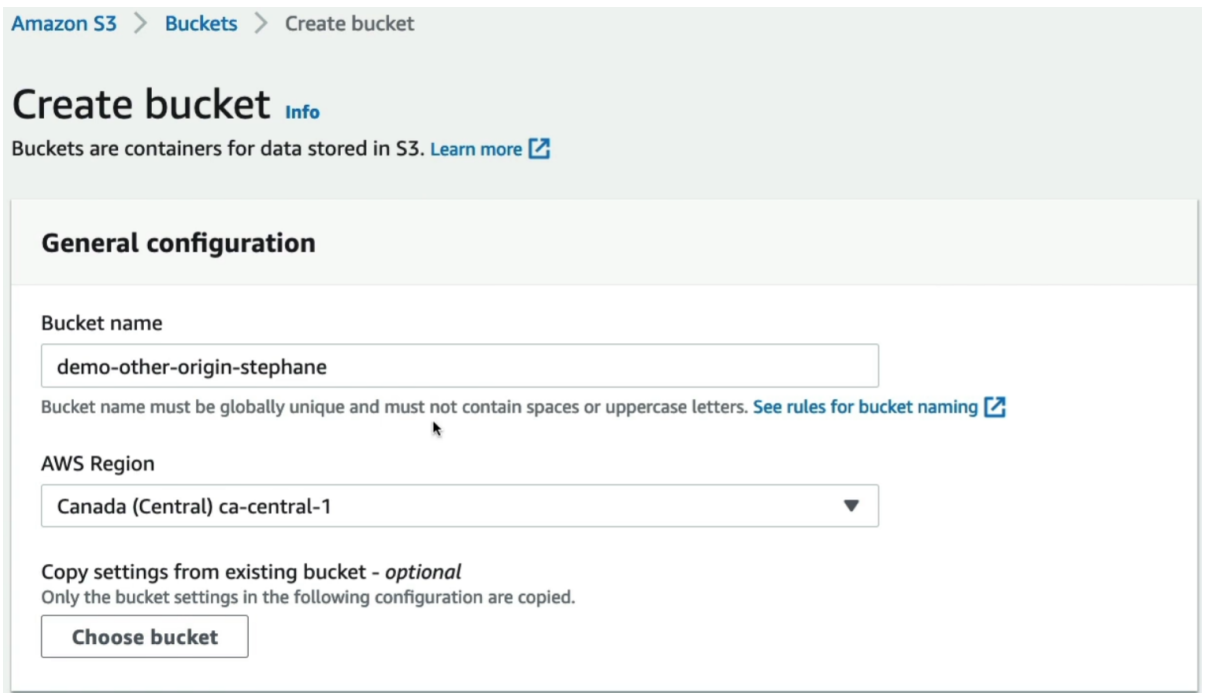
- If a client makes a cross-origin request on our S3 bucket, we need to enable the correct CORS headers
- It's a popular exam question

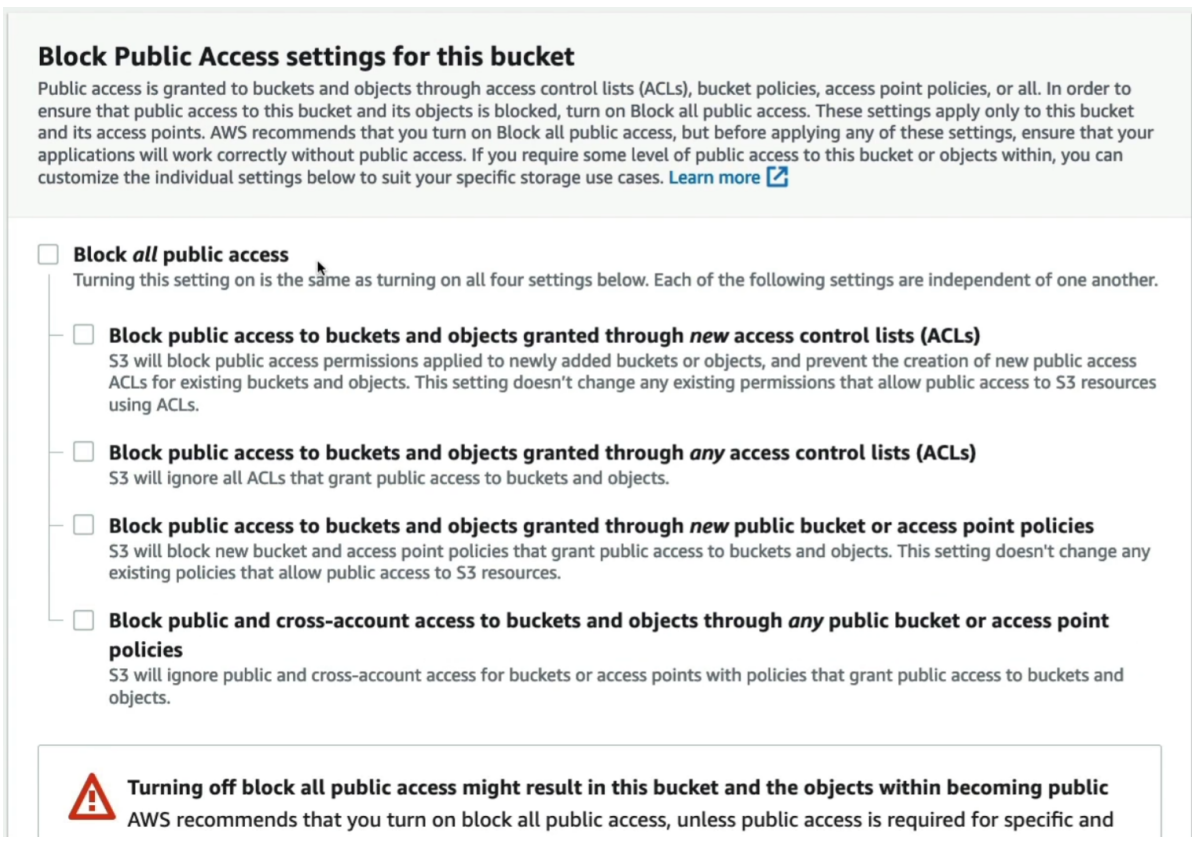
- You can allow for a specific origin or for * (all origins)



Hands on







Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

demo-other-origin-stephane Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Bucket overview

AWS Region	Amazon Resource Name (ARN)	Creation date
Canada (Central) ca-central-1	arn:aws:s3:::demo-other-origin-stephane	October 11, 2022, 16:13:24 (UTC+01:00)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Edit

Bucket Versioning
Disabled

Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Edit

Static website hosting
Disabled

Edit static website hosting Info

Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

- ○ Disable
- ◉ Enable

Hosting type

- ◉ Host a static website
  Use the bucket endpoint as the web address. Learn more
- ○ Redirect requests for an object
  Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

Amazon S3 > Buckets > demo-other-origin-stephane

demo-other-origin-stephane Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Permissions overview

Access

Objects can be public

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

Edit

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

Policy examples | Policy generator

Bucket ARN

arn:aws:s3:::demo-other-origin-stephane

Policy

```
{
    "Version": "2012-10-17",
    "Id": "Policy1665482300144",
    "Statement": [
        {
            "Sid": "Stmt1665482297957",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::stephane-demo-s3/*"
        }
    ]
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

Files and folders (1 Total, 69.0 B)

Remove | Add files | Add folder

All files and folders in this table will be uploaded.

Find by name

1

Name	Folder	Type	Size
extra-page.html	-	text/html	69.0 B

Destination

Destination

s3://demo-other-origin-stephane

▶ **Destination details**

Bucket settings that impact new objects stored in the specified destination.

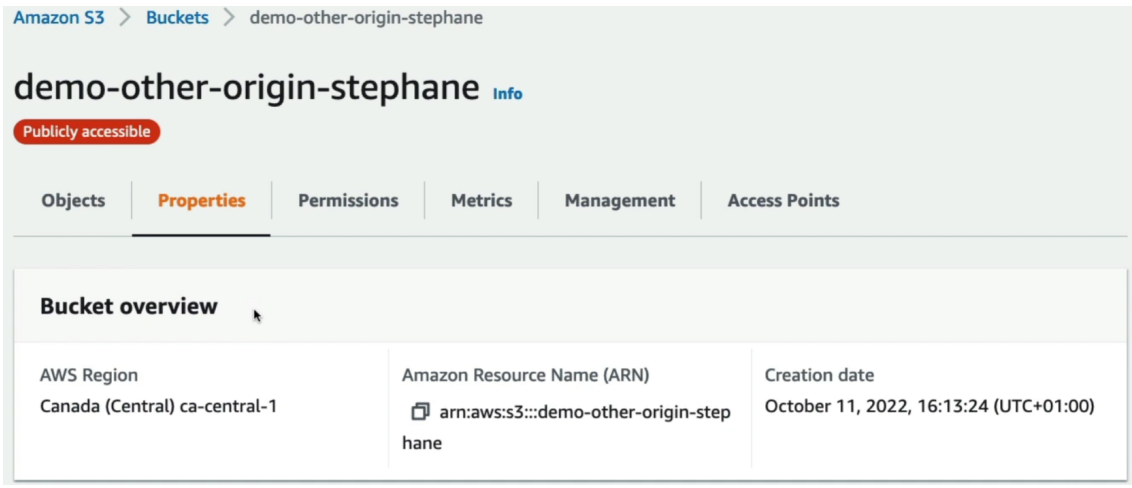
▶ **Permissions**

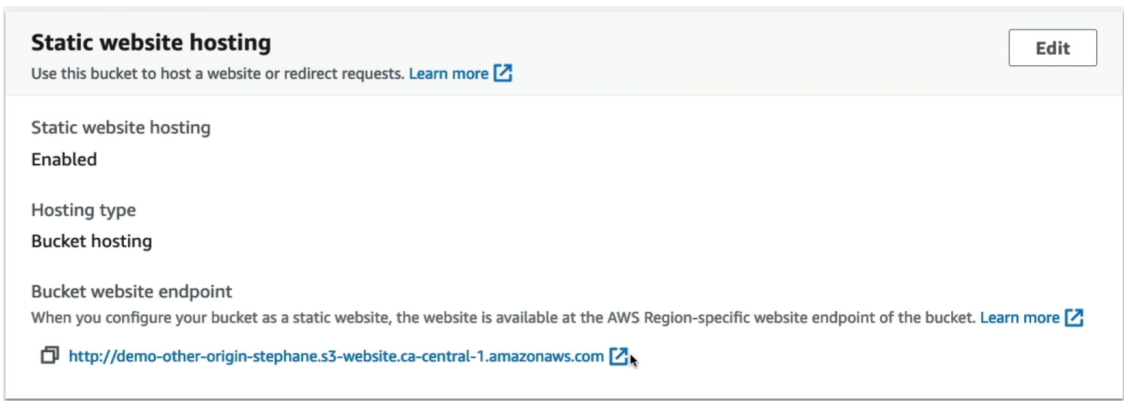
Grant public access and access to other AWS accounts.

▶ **Properties**

Specify storage class, encryption settings, tags, and more.

Cancel | Upload



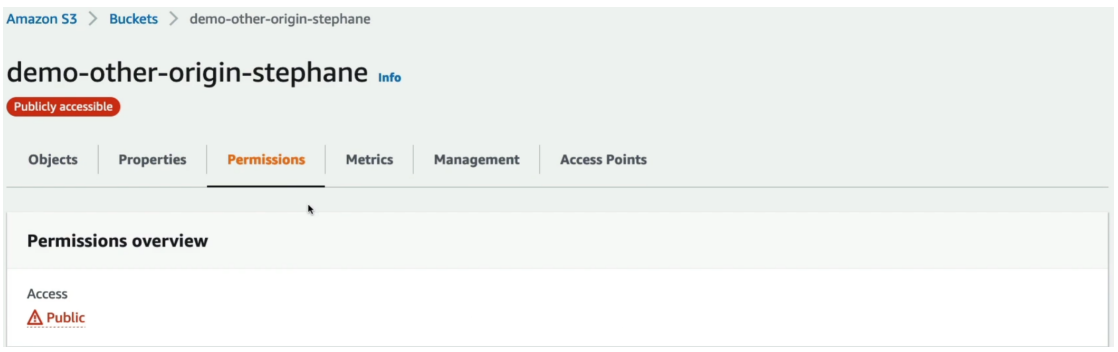


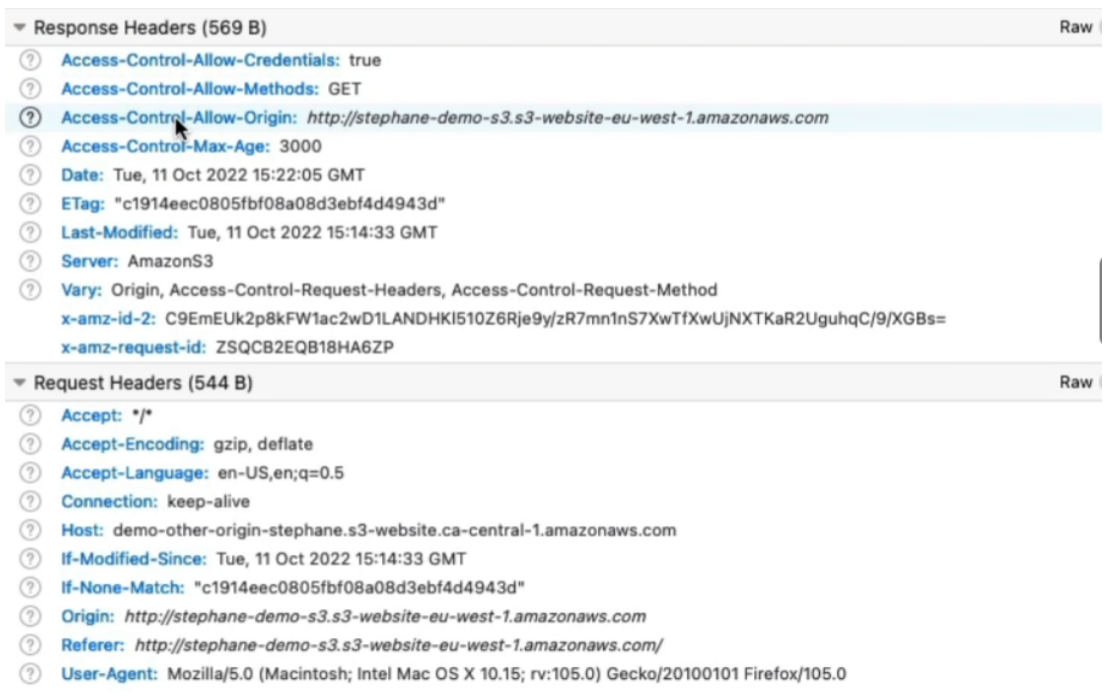
origin bucket index.html

index.html

```
<html>
    <head>
        <title>My First Webpage</title>
    </head>
    <body>
        <h1>I love coffee</h1>
        <p>Hello world!</p>
    </body>

    <img src="coffee.jpg" width=500/>

    <!-- CORS demo -->
    <div id="tofetch"/>
    <script>
        var tofetch = document.getElementById("tofetch");

        fetch('http://demo-other-origin-stephane.s3-website.ca-central-1.amazonaws.com/extra-page.html')
        .then((response) => {
            return response.text();
        })
        .then((html) => {
            tofetch.innerHTML = html
        });
    </script>
</html>
```

Edit other bucket's cross-origin resource sharing

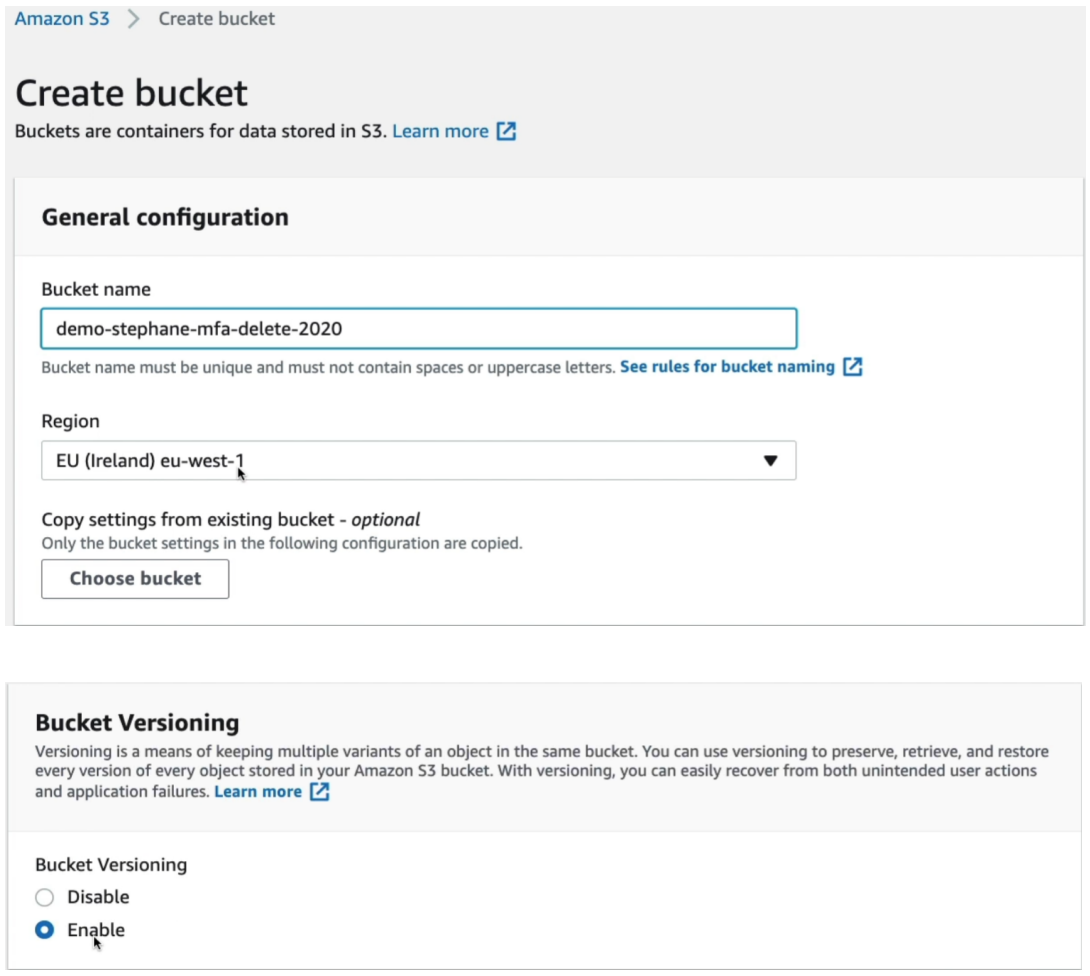


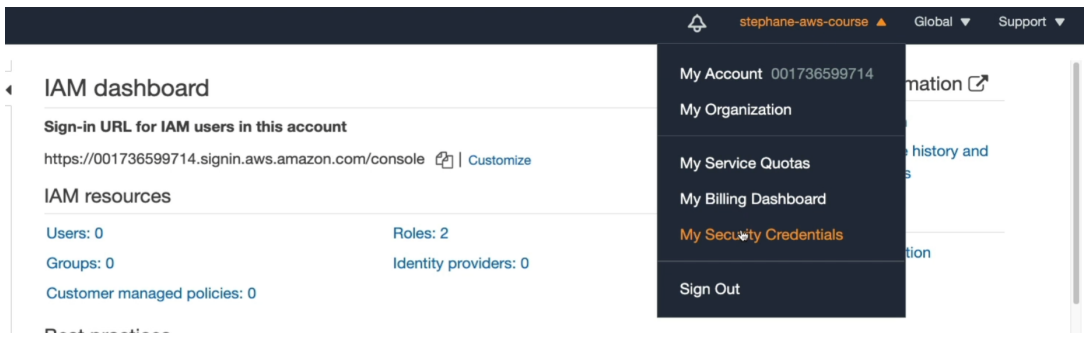


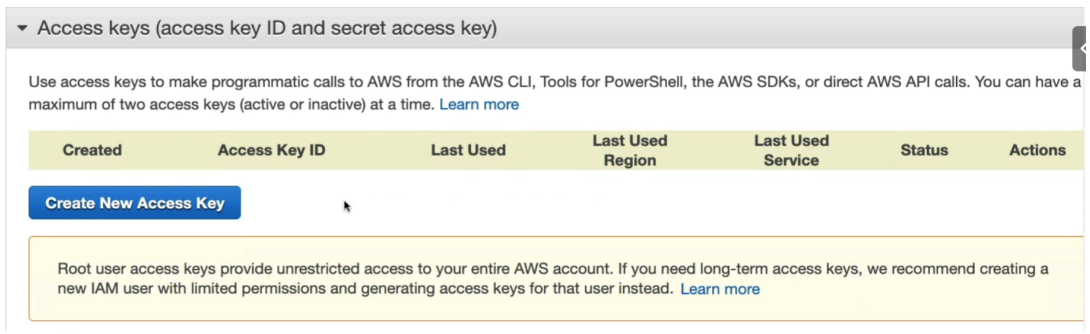
Amazon S3 - MFA Delete

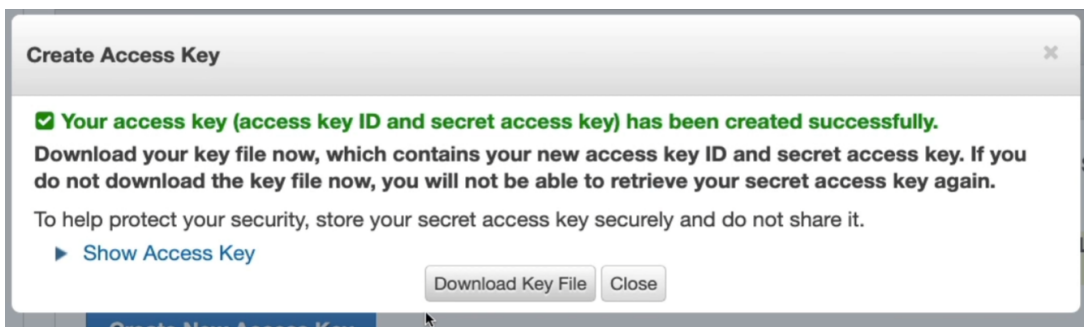
- **MFA (Multi-Factor Authentication)** - force users to generate a code on a device (usually a mobile phone or hardware) before doing important operations on S3
- MFA will be required to :
  - Permanently delete an object version
  - Suspend Versioning on the bucket
- MFA won't be required to:
  - Enable Versioning
  - List deleted versions
- To use MFA Delete, **Versioning must be enable** on the bucket
- **Only the bucket owner(root account) can enable/disable MFA Delete**

Hands on





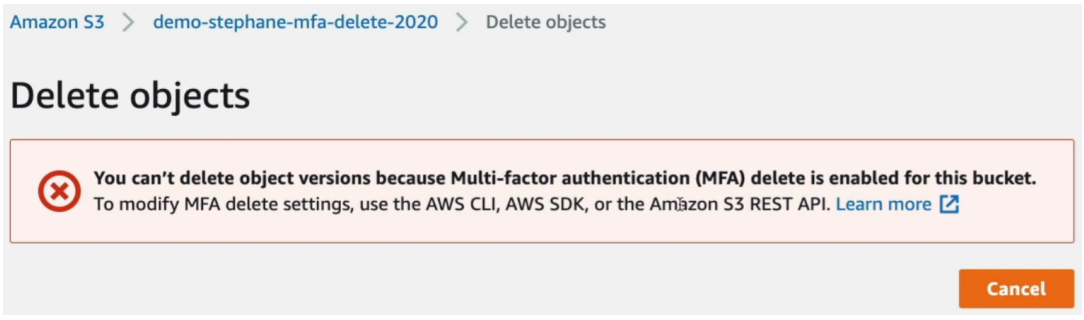


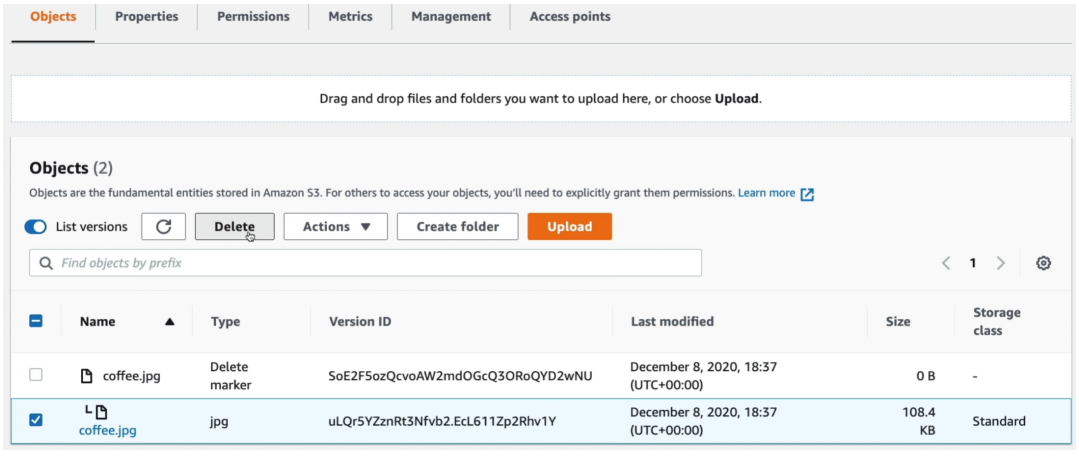



```
Last login: Tue Dec  1 19:08:49 on ttys000
~ aws configure --profile root-mfa-delete-demo
AWS Access Key ID [None]: AKIAIBDXM4UJBGAQNVDA
AWS Secret Access Key [None]: 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
Default region name [None]: eu-west-1
Default output format [None]:
~ aws s3 ls
```

MFADelete=Enabled

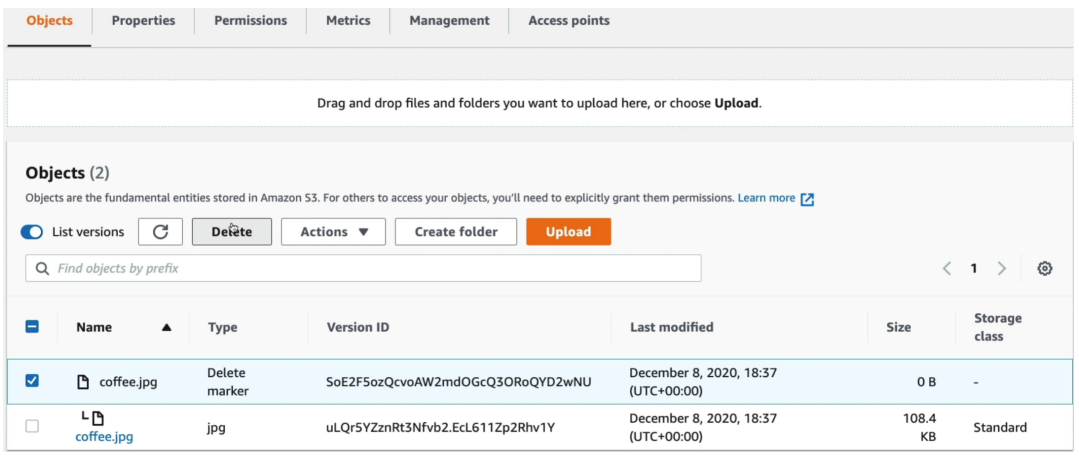
```
~ aws s3 ls --profile root-mfa-delete-demo
2020-12-08 18:17:54 demo-stephane-cors-2020
2020-12-08 18:29:50 demo-stephane-mfa-delete-2020
2020-12-08 18:06:10 demo-stephane-s3-bucket-2020
~ aws s3api put-bucket-versioning --bucket demo-stephane-mfa-delete-2020 --versioning-configuration Status=Enabled,MFADelete=Enabled
--mfa "arn:aws:iam::001736599714:mfa/root-account-mfa-device 710343" --profile root-mfa-delete-demo

An error occurred (TokenCodeInvalidError) when calling the PutBucketVersioning operation: The serial number arn:aws:iam::001736599714:mf
a/root-account-mfa-device and/or token code 710343 you provided is not valid
~ aws s3api put-bucket-versioning --bucket demo-stephane-mfa-delete-2020 --versioning-configuration Status=Enabled,MFADelete=Enab
led --mfa "arn:aws:iam::001736599714:mfa/root-account-mfa-device 797879" --profile root-mfa-delete-demo
```

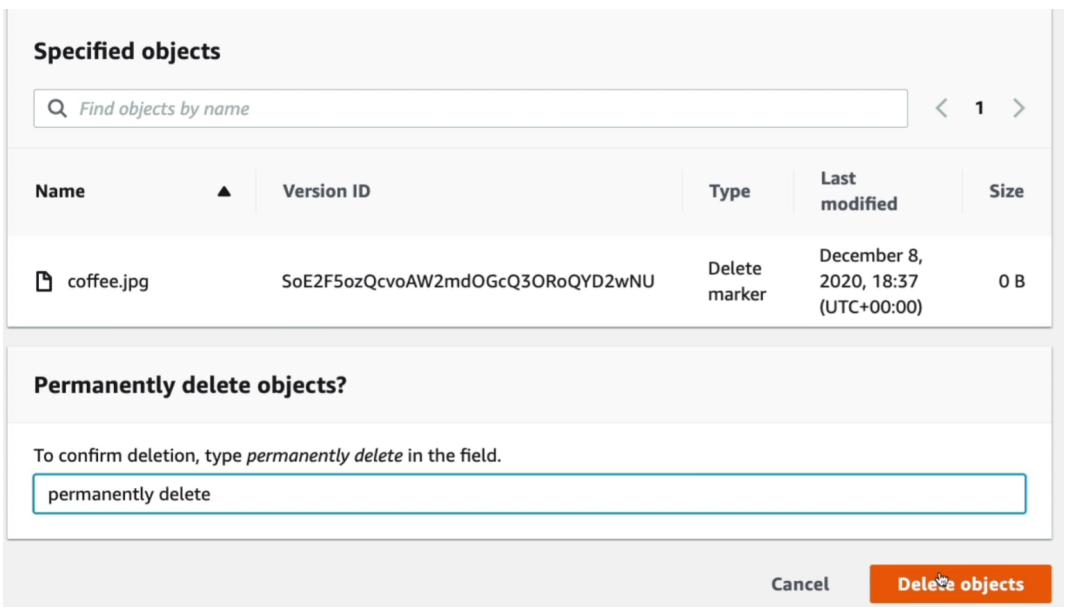




MFADelete=Disabled

```
aws s3api put-bucket-versioning --bucket demo-stephane-mfa-delete-2020 --versioning-configuration Status=Enabled,MFADelete=Disabled
--mfa "arn:aws:iam::001736599714:mfa/root-account-mfa-device 880189" --profile root-mfa-delete-demo
```

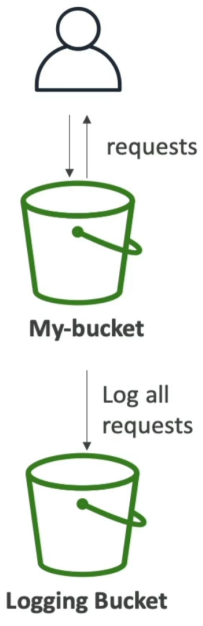




S3 Access Logs

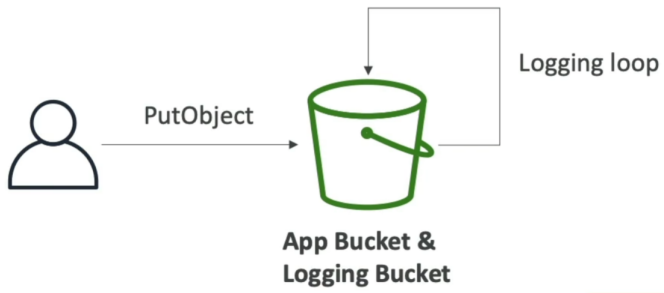
- For audit purpose, you may want to log all access to S3 buckets
- Any request made to S3, from any account,authorized or denied,will be logged into another S3 bucket
- That data can be analyzed using data analysis tools...
- The target logging bucket must be in the same AWS region

- The log format is at:
  https://docs.aws.amazon.com/AmazonS3/latest/devf/LogFormat.html



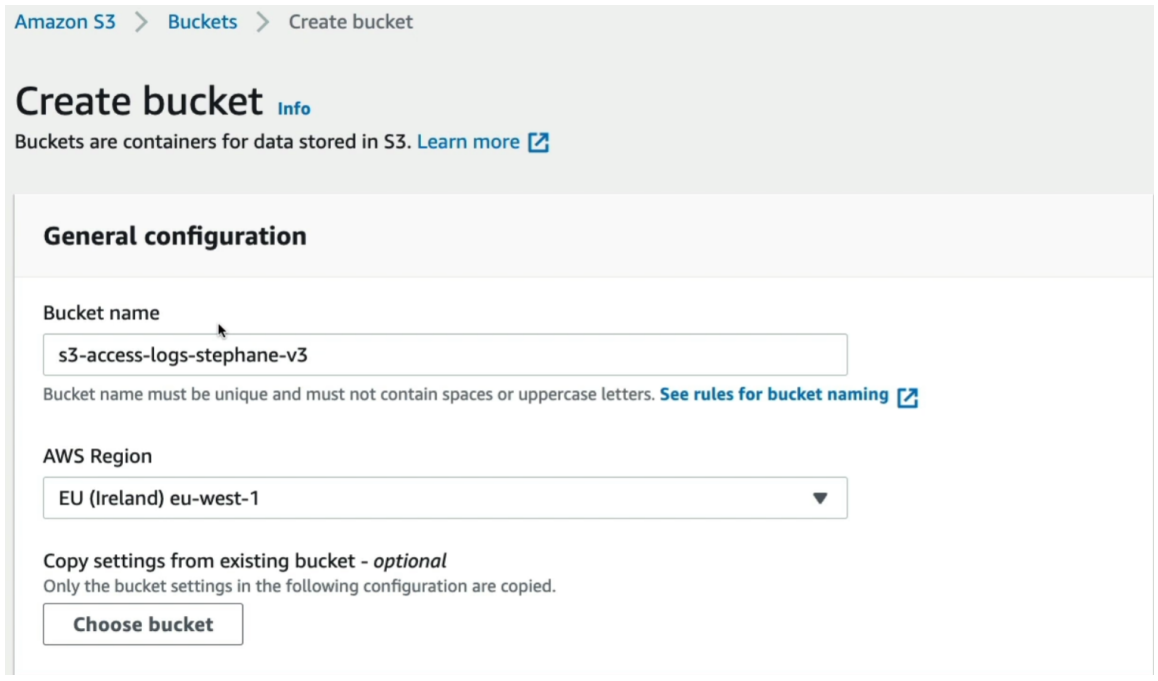
S3 Access Logs: Warning

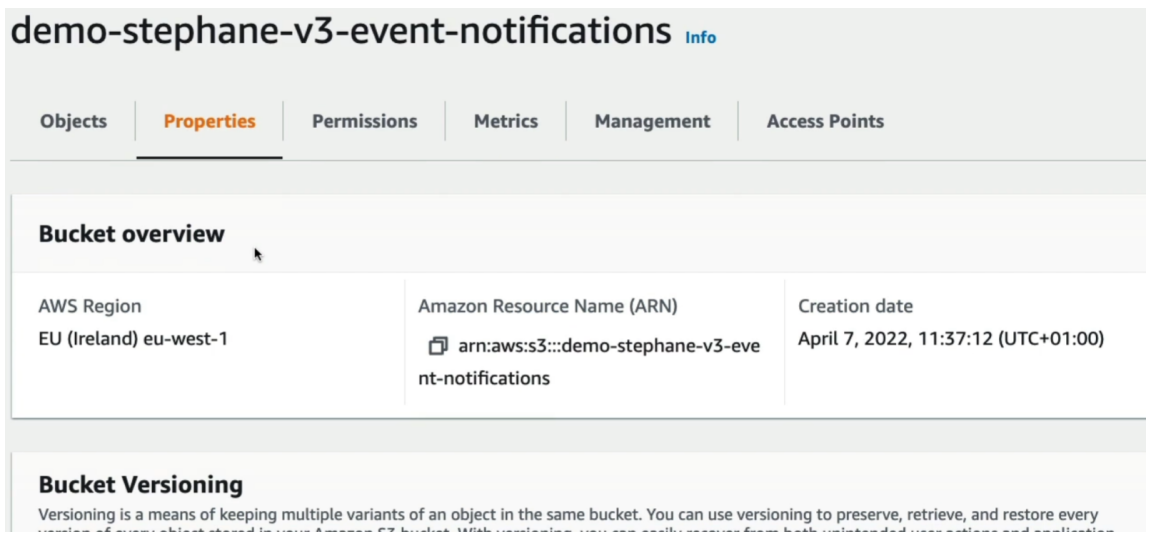
- Do not set your logging bucket to be the monitored bucket
- It will create a logging loop,and **your bucket will grow exponentially**

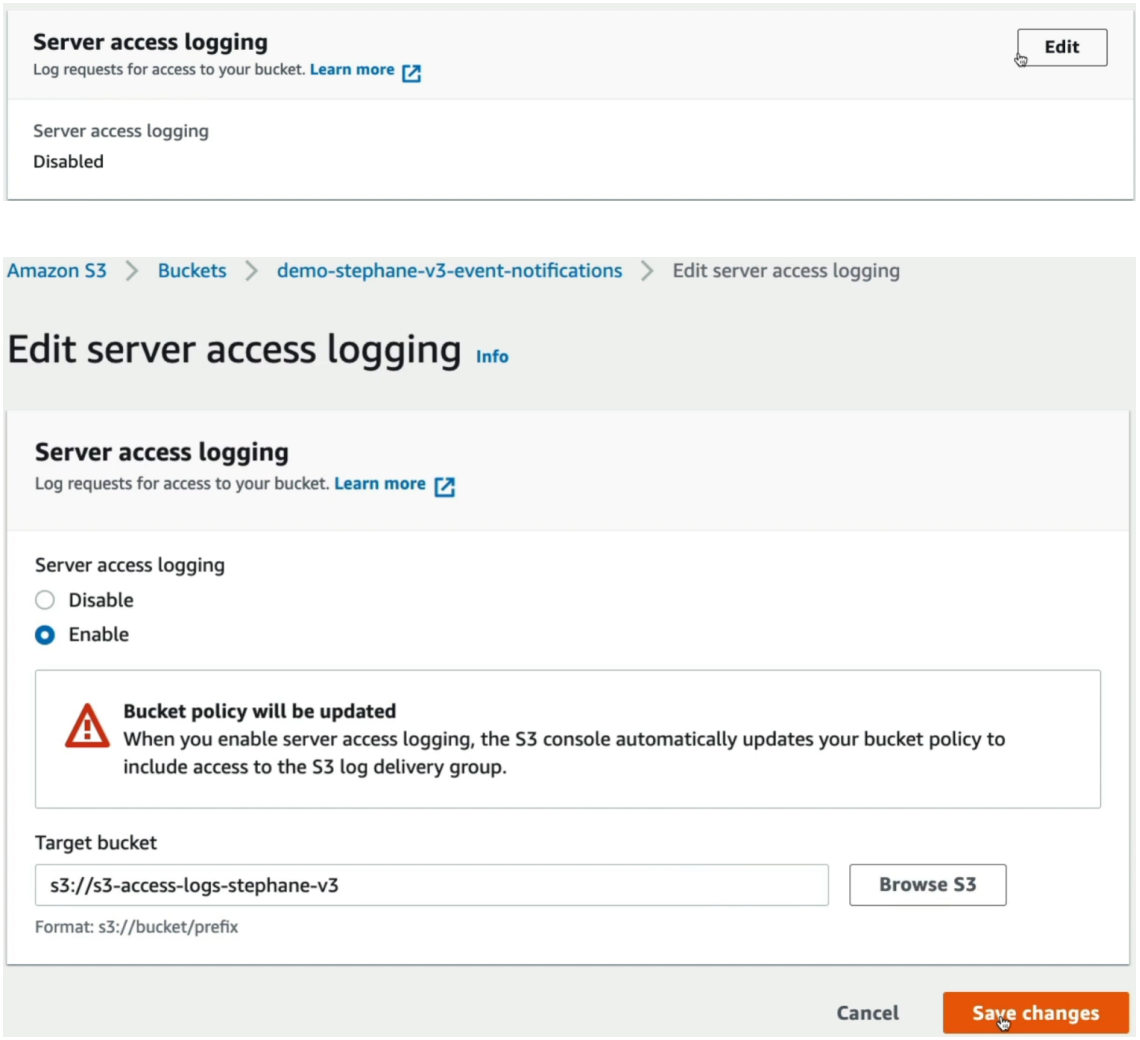


Do not try this at home ☺

Hands on

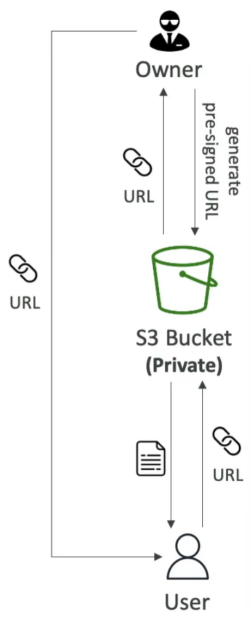




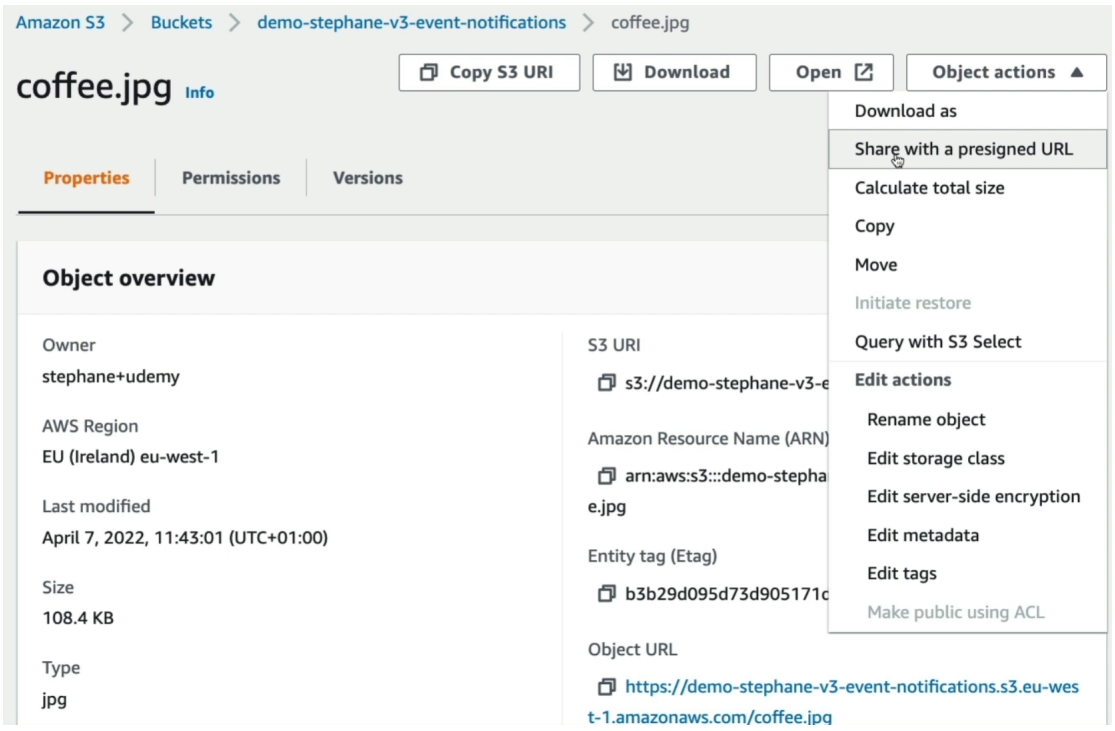


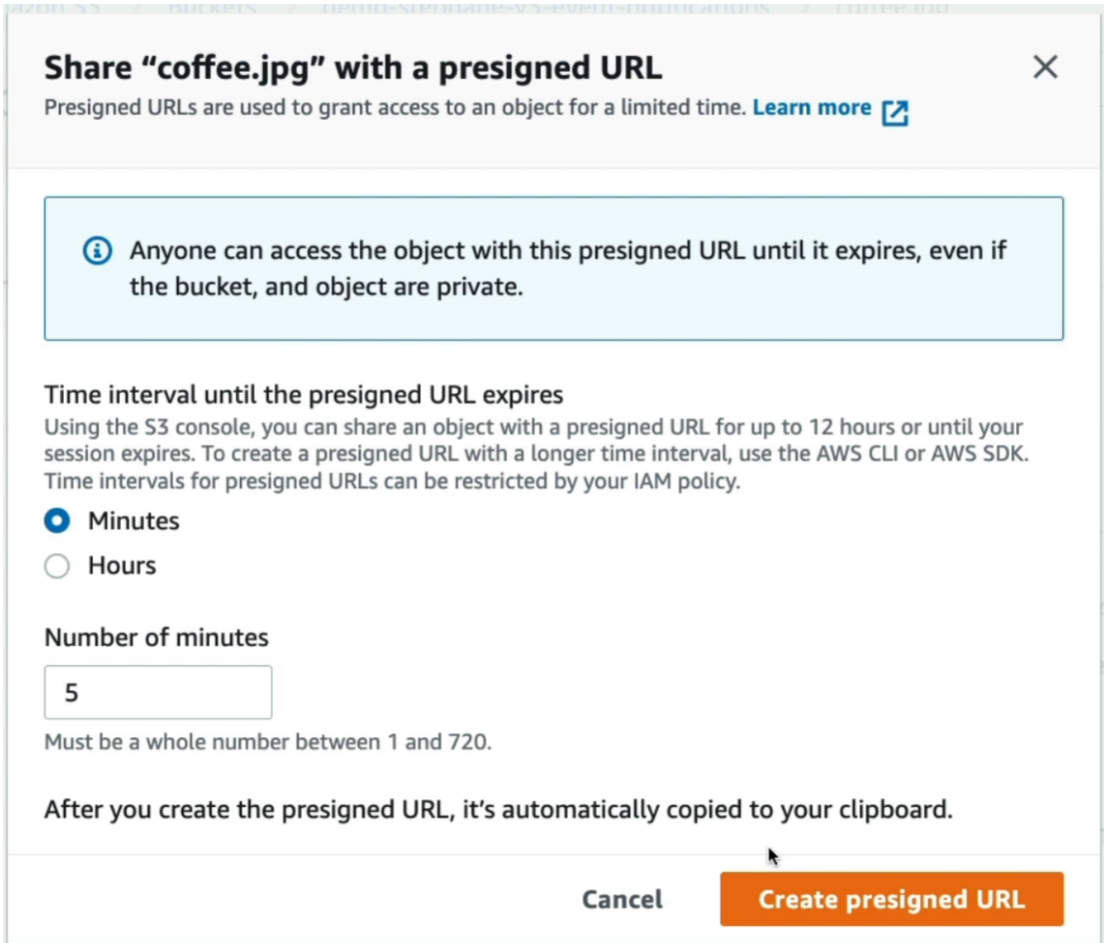
Amazon S3 - Pre-Signed URLs

- Generate pre-signed URLs using the **S3 Console,AWS CLI or SDK**
- **URL Expiration**
  - **S3 Console** - 1 min up to 720 mins (12 hours)
  - **AWS CLI** - configure expiration with - expires-in parameter in seconds(default 36000 secs, max. 604800 secs ~ 168 hours)
- Users given a pre-signed URL inherit the permissions of the user that generated the URL for GET/PUT
- Examples:
  - Allow only logged-in users to download a premium video from your S3 bucket
  - Allow an ever-changing list of users to download files by generating URLs dynamically
  - Allow temporarily a user to upload a file to a precise location in your S3 bucket



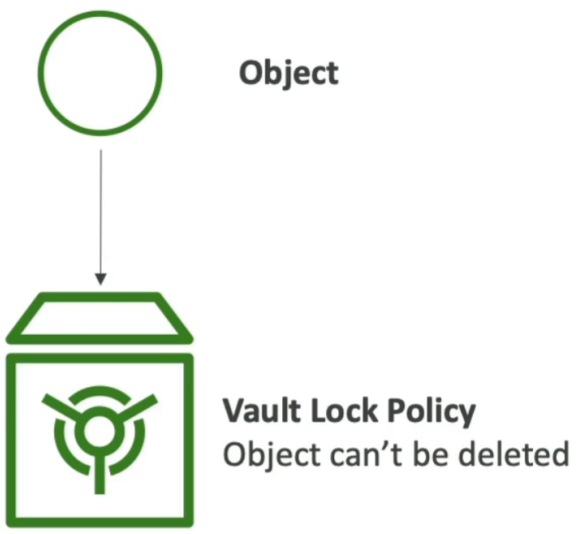
Hands on





S3 Glacier Vault Lock

- Adopt a WORM (Write Once Read Many) model
- Create a Vault Lock Policy
- Lock the Policy for future edits (can no longer be changed or deleted)
- Helpful for compliance and data retention

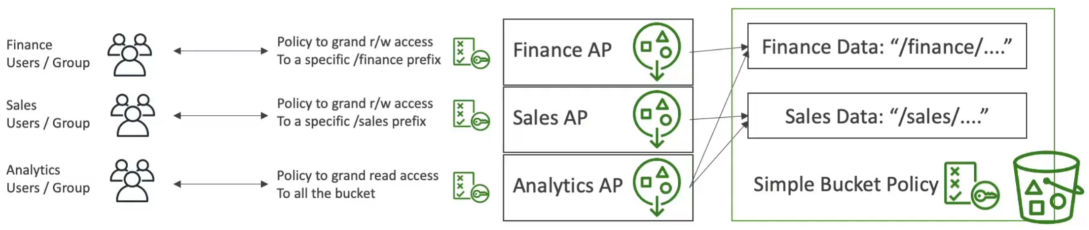


S3 Object Lock(versioning must be enabled)

- Adopt a WORM (Write Once Read Many) model
- Block an object version deletion for a specified amount of time

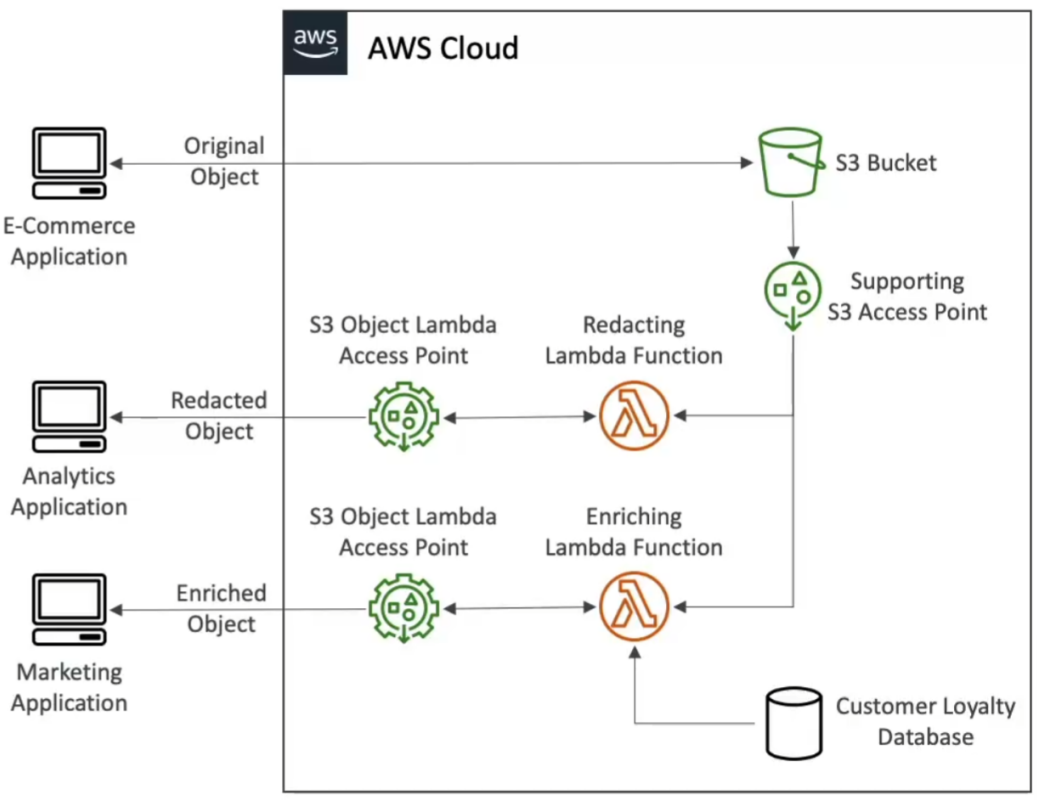
- Retention mode - Compliance:
  - Object versions can't be overwritten or deleted by any user, including the root user
  - Object retention modes can't be changed, and retention periods can't be shortened
- Retention mode - Governance:
  - Most user can't overwrite or delete an object version or alter its lock settings
  - Some user have special permissions to change the retention or delete the object
- Retention Period: protect the object for a fixed period, it can be extended
- Legal Hold:
  - protect the object indefinitely, independent from retention period
  - can be freely placed and removed using the s3:PutObjectLegalHold IAM permission

S3 - Access Points

- Each Access Point gets its own DNS and policy to limit who can access it
  - A specific IAM user / group
  - One policy per Access Point => Easier to manage than complex bucket policies
- 

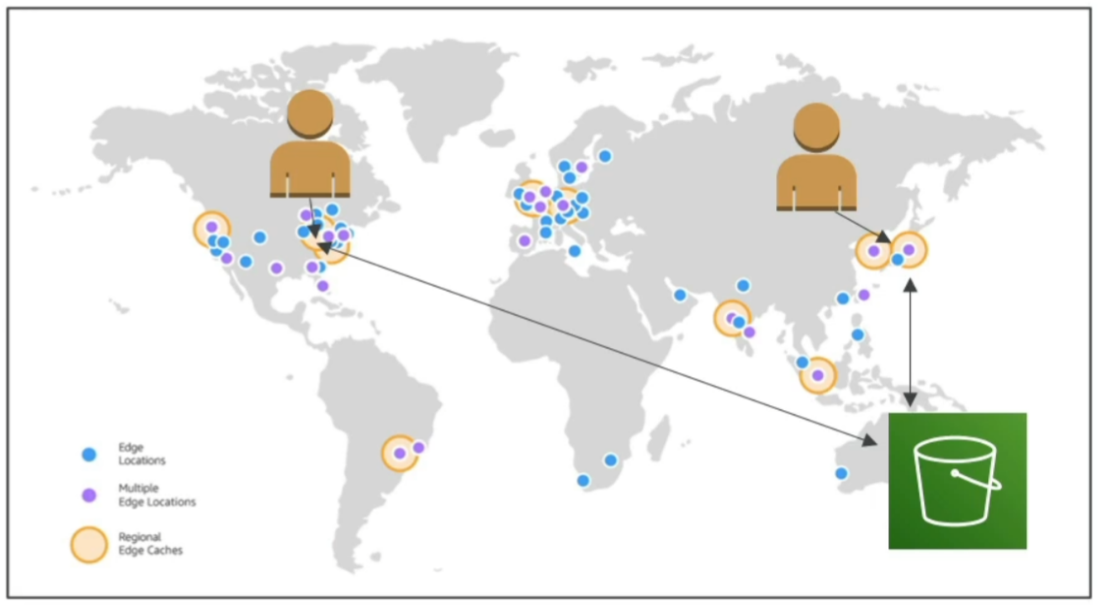
S3 Object Lambda

- Use AWS Lambda Functions to change the object before it is retrieved by the caller application
- Only one S3 bucket is needed, on top of which we create **S3 Access Point and S3 Object Lambda Access Points**.
- Use Cases:
  - Redacting personally identifiable information for analytics or non-production environments.
  - Converting across data formats, such as converting XML to JSON
  - Resizing and watermarking images on the fly using caller-specific details, such as the user who requested the object.



AWS CloudFront

- **Content Delivery Network (CDN)**
- **Improves read performance, content is cached at the edge**
- Improves users experience
- 216 Point of Presence globally (edge locations)
- **DDoS protection (because worldwide), integration with Shield, AWS Web Application Firewall**



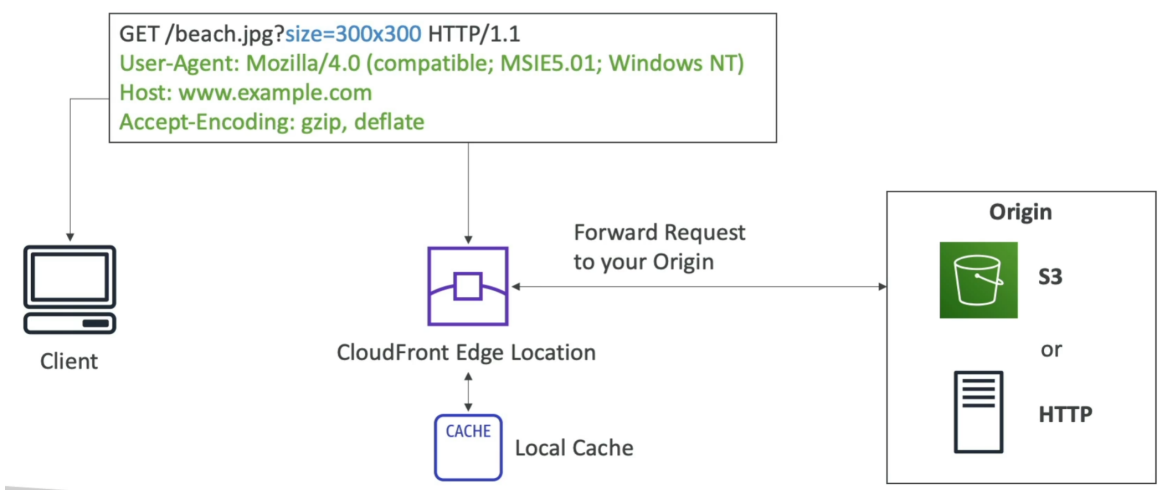
Source: https://aws.amazon.com/cloudfront/features/?nc=sn&loc=2

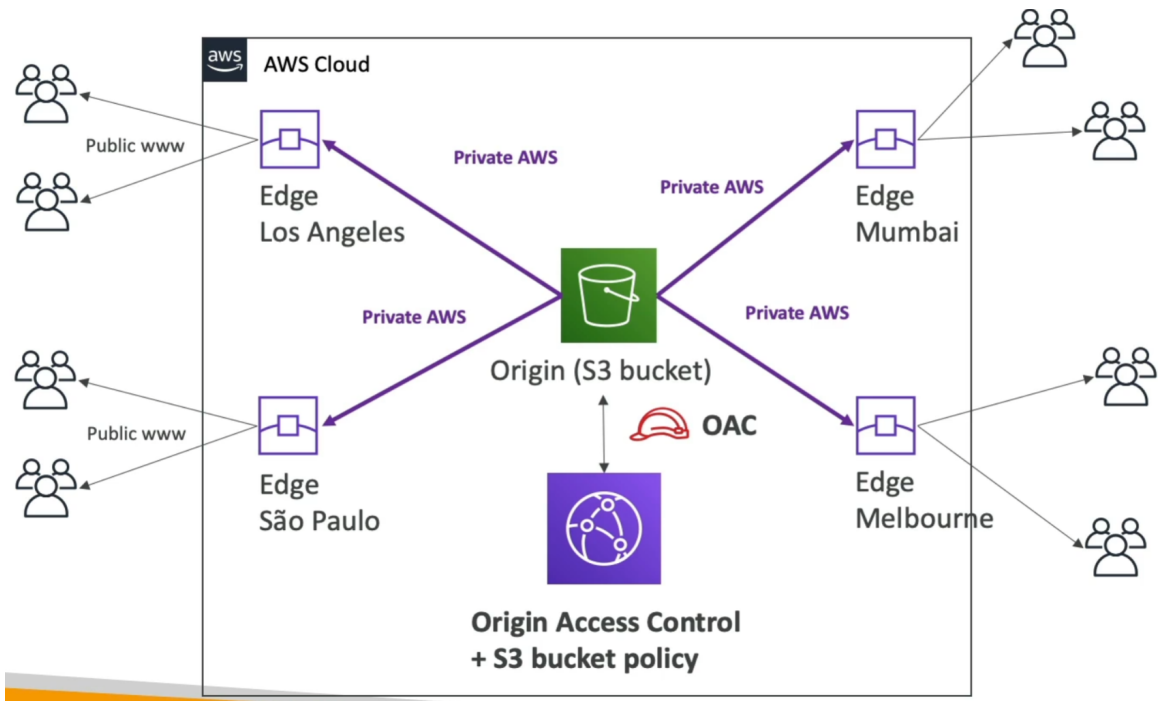
CloudFront - Origins

- **S3 bucket**
  - For distributing files and cashing them at the edge
  - Enhanced security with CloudFront **Origin Access Control (OAC)**
  - OAC is replacing Origin Access Identity (OAI)
  - CloudFront can be used as an ingress (to upload files to S3)

- **Custom Origin (HTTP)**
  - Application Load Balancer
  - EC2 instance
  - S3 website (must first enable the bucket as a static S3 website)
  - Any HTTP backend you want

CloudFront at a high level



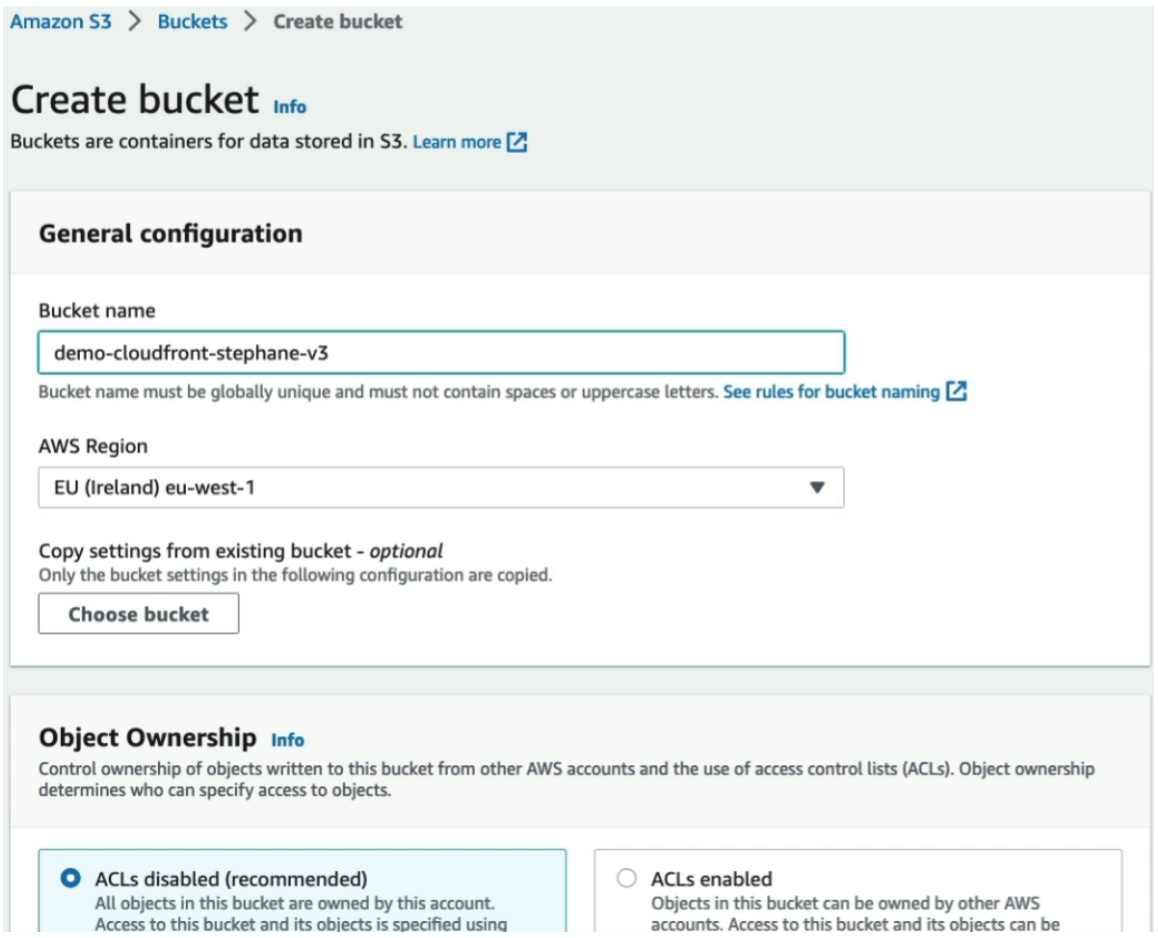


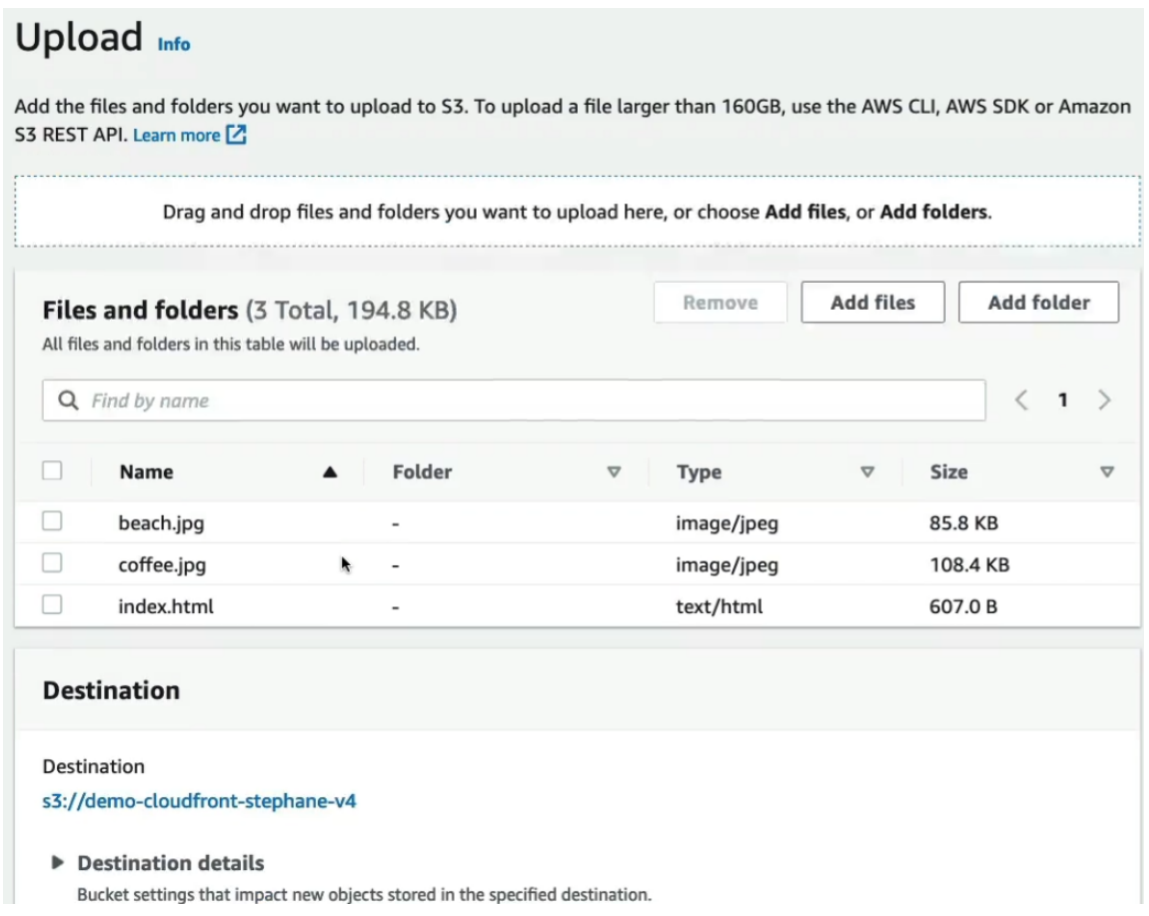
- CloudFront:

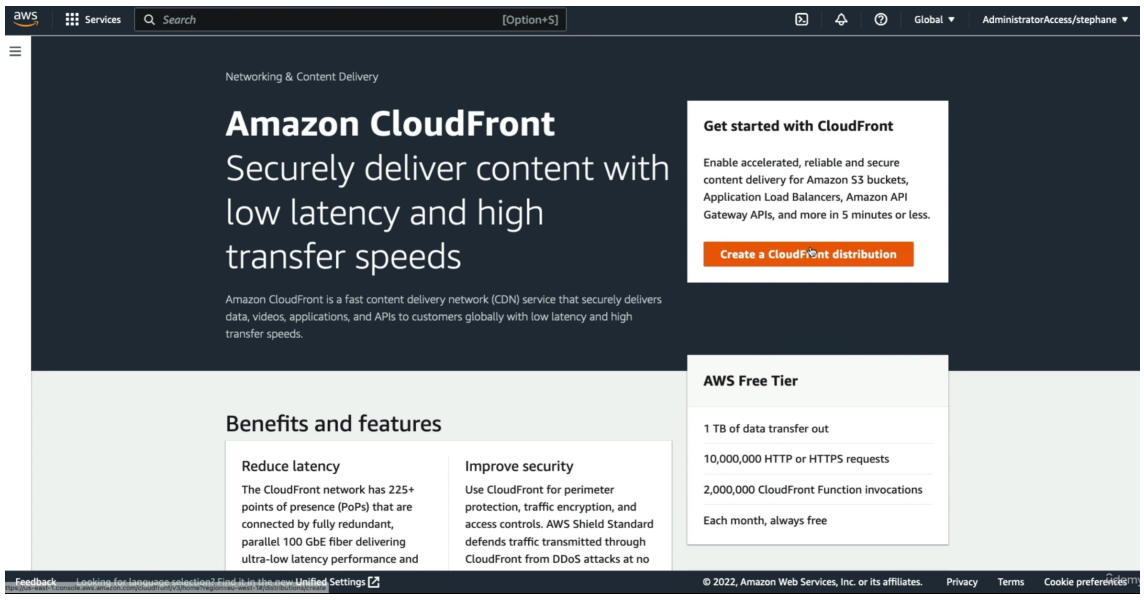
    - Global Edge network
    - Files are cached for a TTL (maybe a day)
    - **Greate for static content that must be available everywhere**

- S3 Cross Region Replication:
    - Must be setup for each region you want replication to happen
    - Files are updated in near real-time
    - Read only
    - **Great for dynamic content that needs to be available at low-latency in few regions**

Hands on






Services
Search
[Option+S]
Global
AdministratorAccess/stephane
Networking & Content Delivery
Amazon CloudFront
Securely deliver content with low latency and high transfer speeds
Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.
Get started with CloudFront
Enable accelerated, reliable and secure content delivery for Amazon S3 buckets, Application Load Balancers, Amazon API Gateway APIs, and more in 5 minutes or less.
Create a CloudFront distribution
AWS Free Tier
1 TB of data transfer out
10,000,000 HTTP or HTTPS requests
2,000,000 CloudFront Function invocations
Each month, always free
Benefits and features
Reduce latency
The CloudFront network has 225+ points of presence (PoPs) that are connected by fully redundant, parallel 100 GbE fiber delivering ultra-low latency performance and
Improve security
Use CloudFront for perimeter protection, traffic encryption, and access controls. AWS Shield Standard defends traffic transmitted through CloudFront from DDoS attacks at no
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences