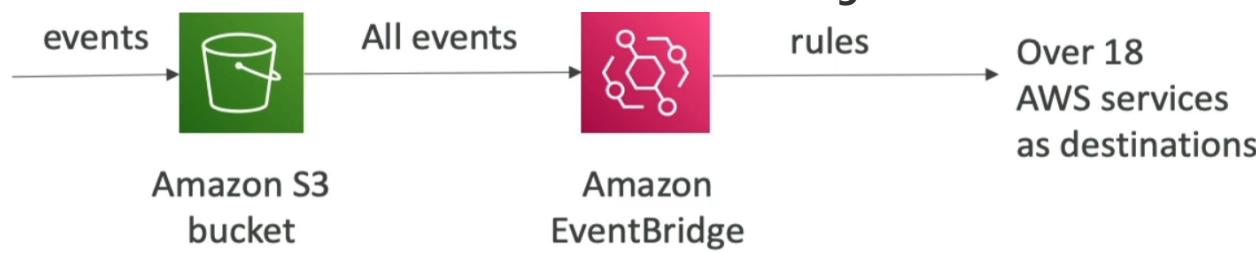


SAA-4

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

General configuration

Bucket name
demo-stephane-v3-event-notifications
Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region
EU (Ireland) eu-west-1

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)

Amazon S3 > Buckets > demo-stephane-v3-event-notifications

demo-stephane-v3-event-notifications [Info](#)

Objects [Properties](#) Permissions Metrics Management Access Points

Bucket overview

AWS Region EU (Ireland) eu-west-1	Amazon Resource Name (ARN) arn:aws:s3:::demo-stephane-v3-event-notifications	Creation date April 7, 2022, 11:37:12 (UTC+01:00)
--------------------------------------	---	--

Event notifications (0)
Send a notification when specific events occur in your bucket. [Learn more](#)

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				

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

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](#)

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

Event name can contain up to 255 characters.

Prefix - optional
Limit the notifications to objects with key starting with specified characters.

Suffix - optional
Limit the notifications to objects with key ending with specified characters.

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						
<input type="radio"/>	test	Standard	4/7/2022, 10:47:55 GMT+1	0	0	Disabled
Content-based deduplication						

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

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 <input type="text" value="30"/> Seconds ▾ <small>Should be between 0 seconds and 12 hours.</small>	Message retention period Info <input type="text" value="4"/> Days ▾ <small>Should be between 1 minute and 14 days.</small>
Delivery delay Info Maximum message size Info <input type="text" value="0"/> Seconds ▾ <input type="text" value="256"/> KB	

Access policy

Define who can access your queue. [Info](#)

```

2 "Id": "Policy1649328102124",
3 "Version": "2012-10-17",
4 "Statement": [
5   {
6     "Sid": "Stmt1649328100474",
7     "Action": [
8       "sns:SendMessage"
9     ],
10    "Effect": "Allow",
11    "Resource": "arn:aws:sns:eu-west-1:783768293452:DemoS3Notification",
12    "Principal": "*"
13  }
14 ]
15 
```

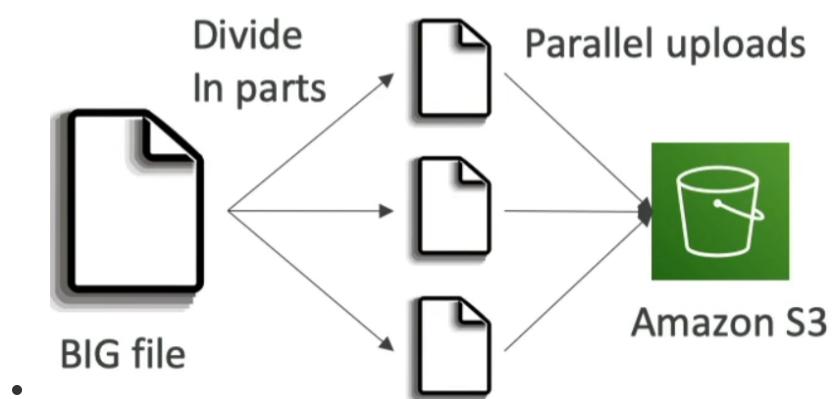
[Policy generator](#)

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

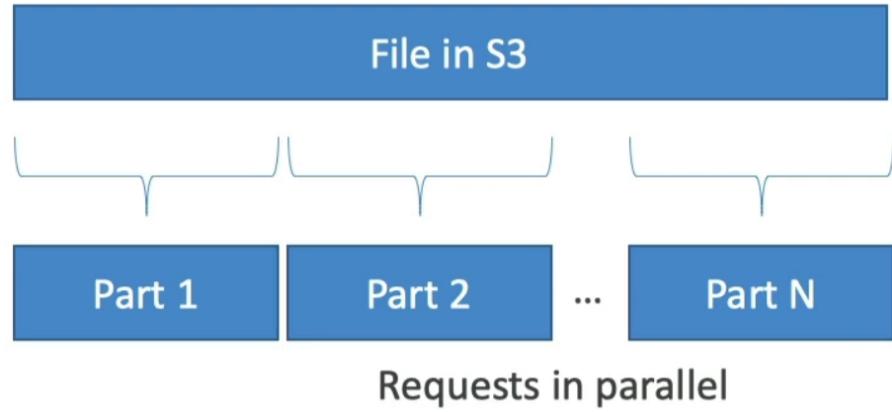
S3 Performance

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

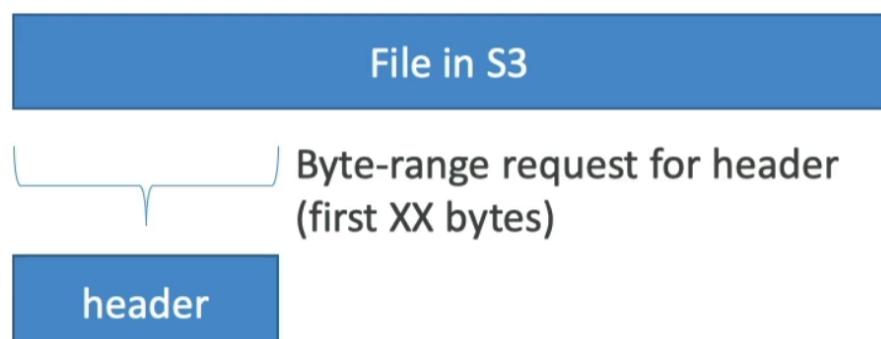


- S3 Transfer Acceleration
 - Increase transfer speed by transferring file to an AWS edge location which will forward the data to the S3 bucket in the target region
 - Compatible with multi-part upload
 - S3 Byte-Range Fetches
 - Parallelize GETs by requesting specific byte ranges
 - Better resilience in case of failures

Can be used to speed up downloads



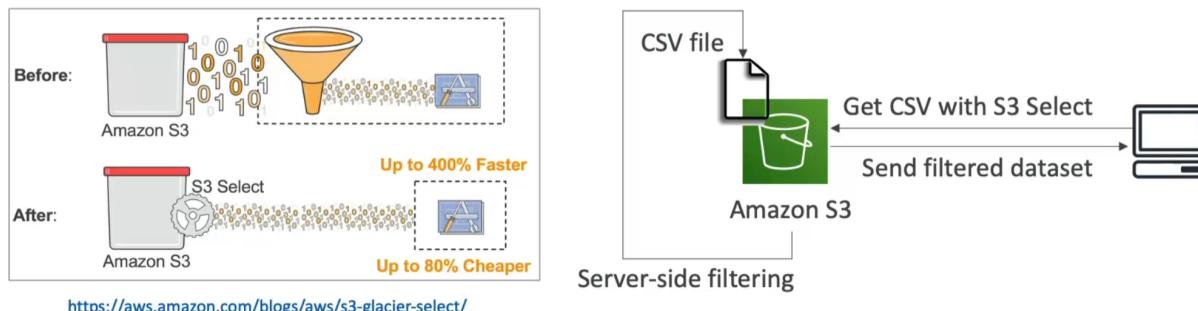
Can be used to retrieve only partial data (for example the head of a file)



S3 Select & Glacier Select

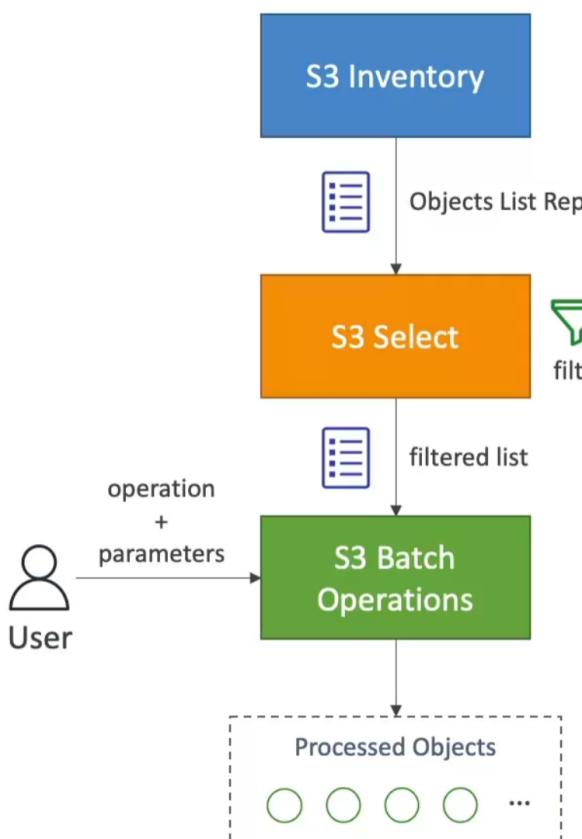
- Retrieve less data using SQL by performing server-side filtering

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



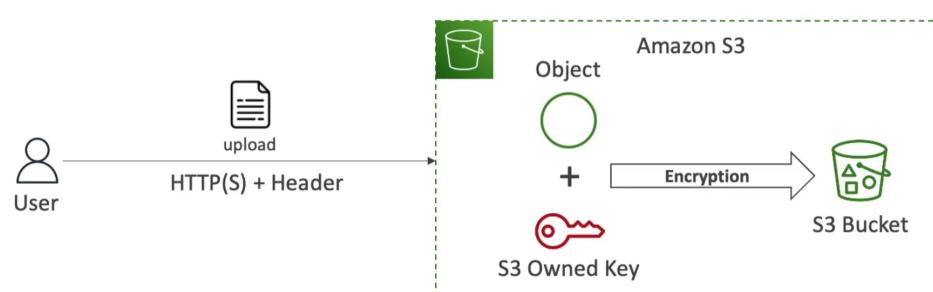
S3 Batch Operations

- 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**



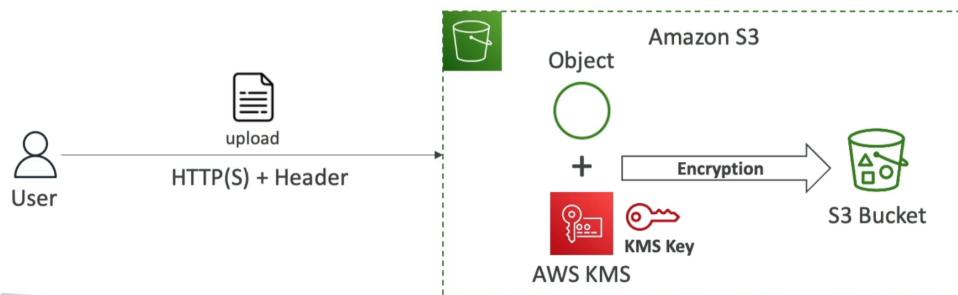
Amazon S3 - Object Encryption

- 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"



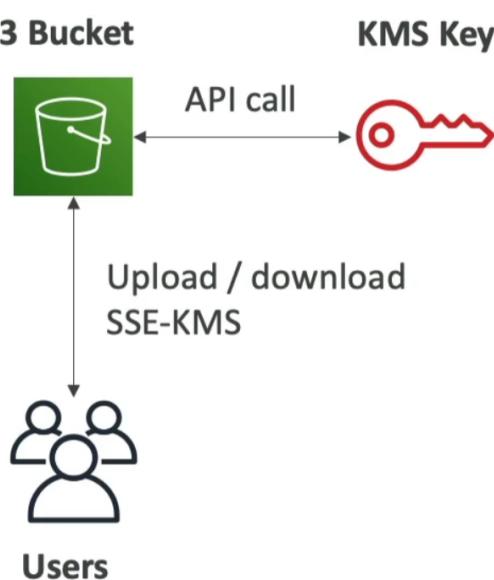
- **Server-Side Encryption with KMS Keys stored in AWS KMS (SEE-KMS)**
 - Leverage AWS Key Management Service (AWS KMS) to manage encryption keys

- 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"**



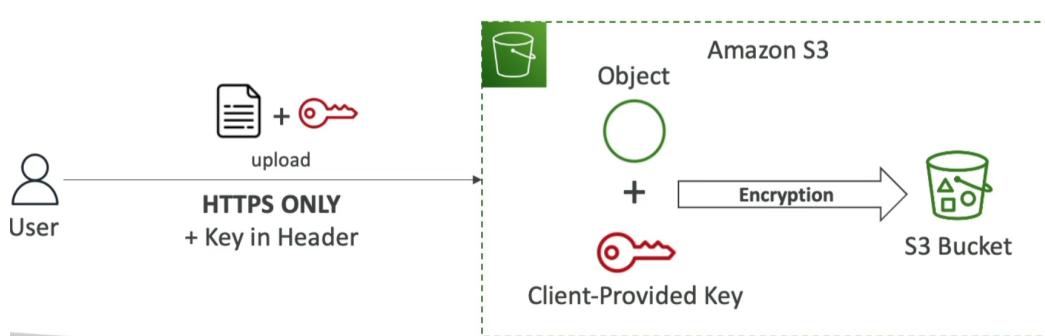
▪ SSE-KMS Limitation

- If you use SSE-KMS, you may be 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



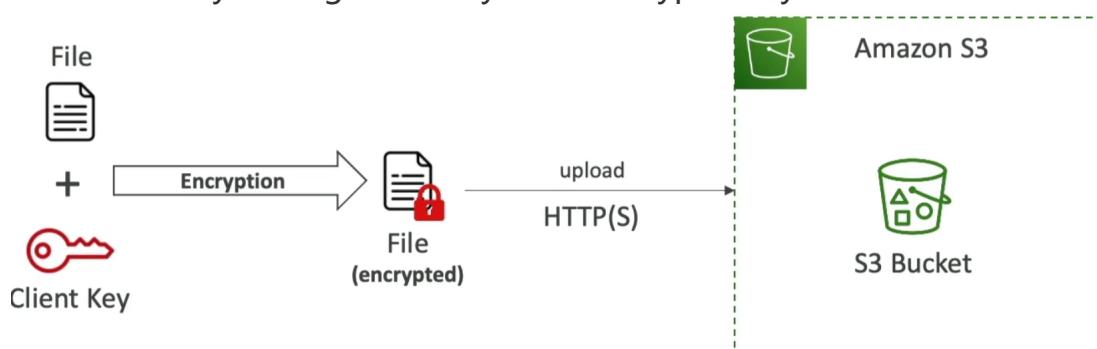
◦ Server-Side Encryption with Customer-Provided Keys (SSE-C)

- 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 be 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

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name: demo-stephane-encryption

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region: EU (Ireland) eu-west-1

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

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](#)

Bucket Versioning

Disable
 Enable

Amazon S3 > Buckets > demo-stephane-encryption > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (1 Total, 85.8 KB)					
All files and folders in this table will be uploaded.					
Remove Add files Add folder					
<input type="text"/> Find by name I < 1 >					
Name	Folder	Type	Size		
beach.jpg	-	image/jpeg	85.8 KB		

Destination

Destination: s3://demo-stephane-encryption

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

[Cancel](#) [Upload](#)

Server-side encryption

Server-side encryption protects data at rest. [Learn more](#)

Server-side encryption

- Do not specify an encryption key
- Specify an encryption key

Encryption key type

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-managed keys (SSE-S3)**
An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)
- AWS Key Management Service key (SSE-KMS)**
An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

SEE-KMS

Server-side encryption

Server-side encryption protects data at rest. [Learn more](#)

Server-side encryption

- Do not specify an encryption key
- Specify an encryption key

Encryption key type

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-managed keys (SSE-S3)**
An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)
- AWS Key Management Service key (SSE-KMS)**
An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

AWS KMS key

- AWS managed key (aws/s3)**
arn:aws:kms:eu-west-1:941512548702:alias/aws/s3
- Choose from your AWS KMS keys
- Enter AWS KMS key ARN

Bucket Key is disabled for objects uploaded, modified, or copied in this bucket

Uploaded, modified, or copied objects inherit their Bucket Key settings from the bucket default encryption configuration unless they already have Bucket Key configured. [Learn more](#)

Server-side encryption settings

Server-side encryption protects data at rest. [Learn more](#)

Default encryption

Enabled

Encryption key type

AWS Key Management Service key (SSE-KMS)*

AWS KMS key ARN

arn:aws:kms:eu-west-1:941512548702:key/7ad599cd-2fdd-4a4a-94aa-5b30396b5ee3

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

Disabled

Edit with Properties

Amazon S3 > Buckets > demo-stephe-ne-encryption

demo-stephe-ne-encryption [Info](#)

[Edit](#)

Properties

Bucket overview

AWS Region EU (Ireland) eu-west-1	Amazon Resource Name (ARN) arn:aws:s3:::demo-stephe-ne-encryption	Creation date October 11, 2022, 14:54:11 (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
Enabled

Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

[Edit](#)

Default encryption
Disabled

Amazon S3 > Buckets > demo-stephane-encryption > Edit default encryption

Edit default encryption [Info](#)

Default encryption
Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption
 Disable
 Enable

Encryption key type
 Amazon S3-managed keys (SSE-S3)
 An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)
 AWS Key Management Service key (SSE-KMS)
 An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

[Cancel](#) [Save changes](#)

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

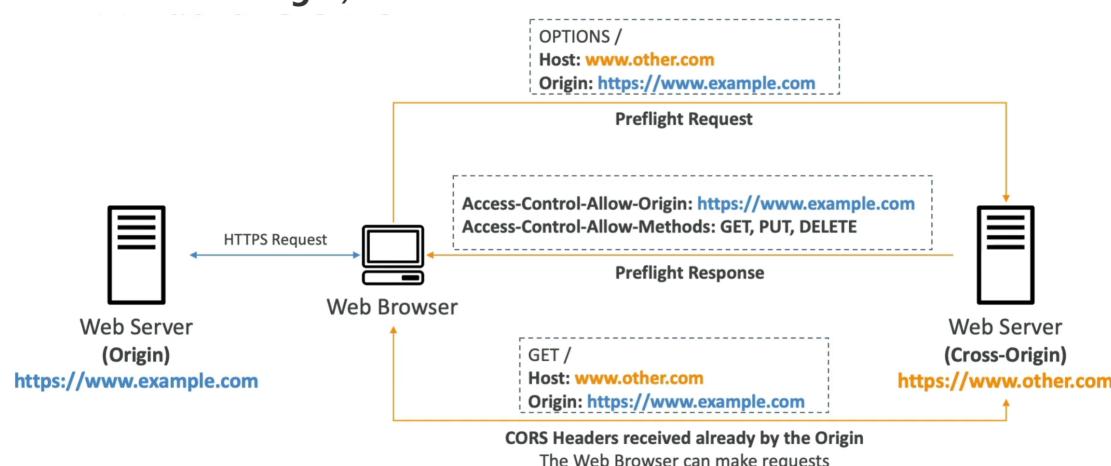
- One way to "force encryption" is to use a bucket policy and refuse any API call to PUT an S3 object without encryption headers

```
{
  "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?

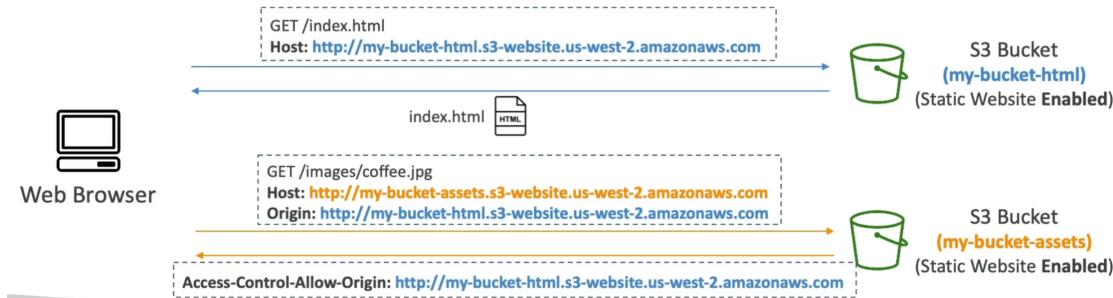
- Cross-Origin Resource Sharing(CORS)**
- Origin = scheme(protocol) + host (domain) + port**
- example:<https://www.example.com> (implied port is 443 for HTTPS, 80 for HTTP)
- Web Browser** based mechanism to allow requests to other origins while visiting the main origin
- Same origin: <http://example.com/app1> & <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

stephane-demo-s3 [Info](#)

Publicly accessible

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

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](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	beach.jpg	jpg	October 11, 2022, 11:08:32 (UTC+01:00)	85.8 KB	Standard
<input type="checkbox"/>	coffee.jpg	jpg	October 11, 2022, 10:32:56 (UTC+01:00)	108.4 KB	Standard
<input type="checkbox"/>	extra-page.html	html	October 11, 2022, 16:11:07 (UTC+01:00)	69.0 B	Standard
<input type="checkbox"/>	index.html	html	October 11, 2022, 16:11:08 (UTC+01:00)	525.0 B	Standard

[C](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Q Find objects by prefix Show versions < 1 > [@](#)

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

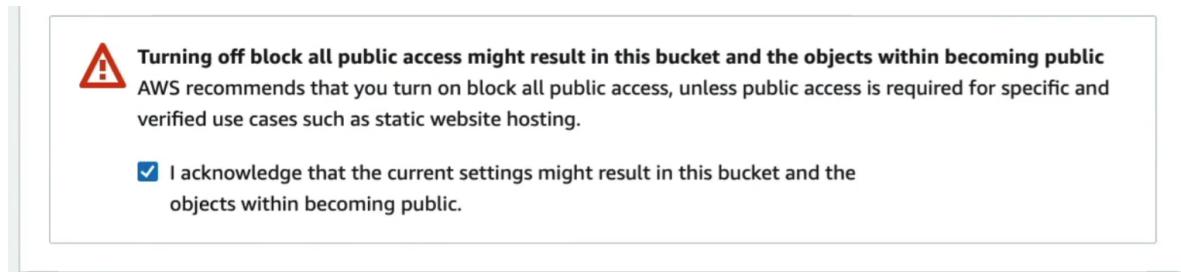
Block Public Access settings for this bucket

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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)** S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)** S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies** S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies** S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

⚠️ 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



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

demo-other-origin-stephe [Info](#)

Objects [Properties](#) Permissions Metrics Management Access Points

Bucket overview

AWS Region Canada (Central) ca-central-1	Amazon Resource Name (ARN) arn:aws:s3:::demo-other-origin-stephe	Creation date 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](#)

[Edit](#)

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](#)

Info 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

```

1  {
2    "Version": "2012-10-17",
3    "Id": "Policy1665482300144",
4    "Statement": [
5      {
6        "Sid": "Stmt1665482297957",
7        "Effect": "Allow",
8        "Principal": "*",
9        "Action": "s3:GetObject",
10       "Resource": "arn:aws:s3:::stephane-demo-s3/*"
11     }
12   ]
13 }
```

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)

All files and folders in this table will be uploaded.

	Name	Folder	Type	Size
<input type="checkbox"/>	extra-page.html	-	text/html	69.0 B

[Remove](#) [Add files](#) [Add folder](#)

Find by name

< 1 >

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](#)

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

demo-other-origin-stephane [Info](#)

Publicly accessible

Objects Properties Permissions Metrics Management Access Points

Bucket overview

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

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

[http://demo-other-origin-stephane.s3-website.ca-central-1.amazonaws.com](#)

origin bucket index.html

```
index.html X
index.html > html > script
1 <html>
2   <head>
3     <title>My First Webpage</title>
4   </head>
5   <body>
6     <h1>I love coffee</h1>
7     <p>Hello world!</p>
8   </body>
9
10  
11
12  <!-- CORS demo -->
13  <div id="tofetch"/>
14  <script>
15    var tofetch = document.getElementById("tofetch");
16
17    fetch('http://demo-other-origin-stephane.s3-website.ca-central-1.amazonaws.com/
18      extra-page.html')
19      .then((response) => {
20        return response.text();
21      })
22      .then((html) => {
23        tofetch.innerHTML = html
24      });
25  </script>
</html>
```

Edit other bucket's cross-origin resource sharing

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

demo-other-origin-stephane [Info](#)

Publicly accessible

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access
[Public](#)

Edit cross-origin resource sharing (CORS)

Cross-origin resource sharing (CORS)

The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. [Learn more](#)

```
1 [  
2 {  
3   "AllowedHeaders": [  
4     "Authorization"  
5   ],  
6   "AllowedMethods": [  
7     "GET"  
8   ],  
9   "AllowedOrigins": [  
10    "http://stephane-demo-s3.s3-website-eu-west-1.amazonaws.com"  
11  ],  
12  "ExposeHeaders": [],  
13  "MaxAgeSeconds": 3000  
14 }  
15 ]
```

Response Headers (569 B)

Raw

① **Access-Control-Allow-Credentials:** true
① **Access-Control-Allow-Methods:** GET
① **Access-Control-Allow-Origin:** http://stephane-demo-s3.s3-website-eu-west-1.amazonaws.com
① **Access-Control-Max-Age:** 3000
① **Date:** Tue, 11 Oct 2022 15:22:05 GMT
① **ETag:** "c1914eec0805fbf08a08d3ebf4d4943d"
① **Last-Modified:** Tue, 11 Oct 2022 15:14:33 GMT
① **Server:** AmazonS3
① **Vary:** Origin, Access-Control-Request-Headers, Access-Control-Request-Method
x-amz-id-2: C9EmEUk2p8kFW1ac2wD1LANDHKI510Z6Rje9y/zR7mn1nS7XwTfXwUjNXTKaR2UguhqC/9/XGBs=
x-amz-request-id: ZSQCB2EQB18HA6ZP

Request Headers (544 B)

Raw

① **Accept:** */*
① **Accept-Encoding:** gzip, deflate
① **Accept-Language:** en-US,en;q=0.5
① **Connection:** keep-alive
① **Host:** demo-other-origin-stephane.s3-website.ca-central-1.amazonaws.com
① **If-Modified-Since:** Tue, 11 Oct 2022 15:14:33 GMT
① **If-None-Match:** "c1914eec0805fbf08a08d3ebf4d4943d"
① **Origin:** http://stephane-demo-s3.s3-website-eu-west-1.amazonaws.com
① **Referer:** http://stephane-demo-s3.s3-website-eu-west-1.amazonaws.com/
① **User-Agent:** Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:105.0) Gecko/20100101 Firefox/105.0

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**



Google Authenticator



MFA Hardware Device

Hands on

Amazon S3 > Create bucket

Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

General configuration	
Bucket name	<input type="text" value="demo-stephane-mfa-delete-2020"/>
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming	
Region	EU (Ireland) eu-west-1
Copy settings from existing bucket - <i>optional</i> Only the bucket settings in the following configuration are copied.	
Choose bucket	

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](#)

Bucket Versioning	
<input type="radio"/> Disable	
<input checked="" type="radio"/> Enable	

stephane-aws-course ▲ Global ▾ Support ▾

- IAM dashboard
- Sign-in URL for IAM users in this account
<https://001736599714.signin.aws.amazon.com/console> | Customize
- IAM resources

Users: 0	Groups: 0	Roles: 2	Identity providers: 0
Customer managed policies: 0			
- My Account 001736599714
- My Organization
- My Service Quotas
- My Billing Dashboard
- My Security Credentials
- Sign Out

▼ Access keys (access key ID and secret access key)

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

Created	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
Create New Access Key						

Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we recommend creating a new IAM user with limited permissions and generating access keys for that user instead. [Learn more](#)

Create Access Key

Your access key (access key ID and secret access key) has been created successfully.

Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

To help protect your security, store your secret access key securely and do not share it.

[Show Access Key](#)

[Download Key File](#) [Close](#)

```
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:mfa/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=Enabled
--mfa "arn:aws:iam::001736599714:mfa/root-account-mfa-device 797879" --profile root-mfa-delete-demo
```

Amazon S3 > demo-stephane-mfa-delete-2020 > Delete objects

Delete objects

You can't delete object versions because Multi-factor authentication (MFA) delete is enabled for this bucket.
To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

[Cancel](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access points](#)

Drag and drop files and folders you want to upload here, or choose [Upload](#).

Objects (2)
Objects are the fundamental entities stored in Amazon S3. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[List versions](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

[Find objects by prefix](#)

Name	Type	Version ID	Last modified	Size	Storage class
<input type="checkbox"/> coffee.jpg	Delete marker	SoE2F5ozQcvoAW2mdOGcQ3ORoQYD2wNU	December 8, 2020, 18:37 (UTC+00:00)	0 B	-
<input checked="" type="checkbox"/> coffee.jpg	jpg	uLQr5YZznRt3Nfvb2.EcL611Zp2Rhv1Y	December 8, 2020, 18:37 (UTC+00:00)	108.4 KB	Standard

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
```

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access points](#)

Drag and drop files and folders you want to upload here, or choose [Upload](#).

Objects (2)
Objects are the fundamental entities stored in Amazon S3. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[List versions](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

[Find objects by prefix](#)

Name	Type	Version ID	Last modified	Size	Storage class
<input checked="" type="checkbox"/> coffee.jpg	Delete marker	SoE2F5ozQcvoAW2mdOGcQ3ORoQYD2wNU	December 8, 2020, 18:37 (UTC+00:00)	0 B	-
<input type="checkbox"/> coffee.jpg	jpg	uLQr5YZznRt3Nfvb2.EcL611Zp2Rhv1Y	December 8, 2020, 18:37 (UTC+00:00)	108.4 KB	Standard

Specified objects

[Find objects by name](#)

Name	Version ID	Type	Last modified	Size
<input checked="" type="checkbox"/> coffee.jpg	SoE2F5ozQcvoAW2mdOGcQ3ORoQYD2wNU	Delete marker	December 8, 2020, 18:37 (UTC+00:00)	0 B

Permanently delete objects?

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

[Cancel](#) [Delete objects](#)

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**



Hands on

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

demo-stephane-v3-event-notifications Info

[Objects](#) | **Properties** | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Bucket overview

AWS Region EU (Ireland) eu-west-1	Amazon Resource Name (ARN) arn:aws:s3:::demo-stephane-v3-event-notifications	Creation date April 7, 2022, 11:37:12 (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

Server access logging
Log requests for access to your bucket. [Learn more](#)

Server access logging
Disabled

Amazon S3 > Buckets > demo-stephane-v3-event-notifications > Edit server access logging

Edit server access logging Info

Server access logging
Log requests for access to your bucket. [Learn more](#)

Server access logging
 Disable
 Enable

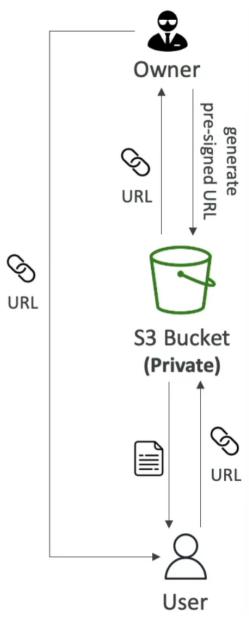
⚠ Bucket policy will be updated
When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery group.

Target bucket
 [Browse S3](#)
Format: s3://bucket/prefix

[Cancel](#) [Save changes](#)

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

Amazon S3 > Buckets > demo-stephane-v3-event-notifications > coffee.jpg

coffee.jpg Info

Properties **Permissions** **Versions**

Object overview

Owner stephane+udemy	S3 URI s3://demo-stephane-v3-e
AWS Region EU (Ireland) eu-west-1	Amazon Resource Name (ARN) arn:aws:s3:::demo-stephane-v3-e/coffee.jpg
Last modified April 7, 2022, 11:43:01 (UTC+01:00)	Entity tag (Etag) b3b29d095d73d905171c
Size 108.4 KB	Object URL https://demo-stephane-v3-event-notifications.s3.eu-west-1.amazonaws.com/coffee.jpg
Type jpg	

Object actions ▾

- Download as
- Share with a presigned URL** ✓
- Calculate total size
- Copy
- Move
- Initiate restore
- Query with S3 Select
- Edit actions**
- Rename object
- Edit storage class
- Edit server-side encryption
- Edit metadata
- Edit tags
- Make public using ACL

Share "coffee.jpg" with a presigned URL

Presigned URLs are used to grant access to an object for a limited time. [Learn more](#)

Anyone can access the object with this presigned URL until it expires, even if the bucket, and object are private.

Time interval until the presigned URL expires
Using the S3 console, you can share an object with a presigned URL for up to 12 hours or until your session expires. To create a presigned URL with a longer time interval, use the AWS CLI or AWS SDK. Time intervals for presigned URLs can be restricted by your IAM policy.

Minutes

Hours

Number of minutes
5

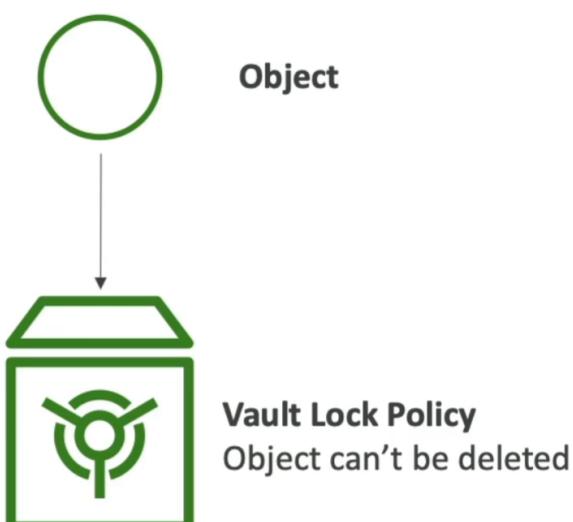
Must be a whole number between 1 and 720.

After you create the presigned URL, it's automatically copied to your clipboard.

[Cancel](#) **Create presigned URL**

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



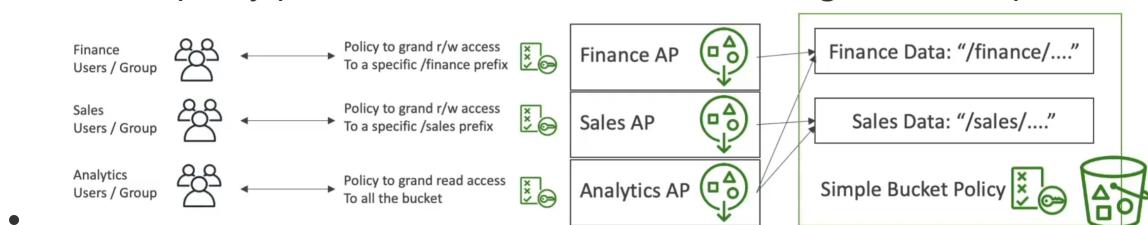
S3 Object Lock(versioning must be enabled)

- 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 users can't overwrite or delete an object version or alter its lock settings
 - Some users 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

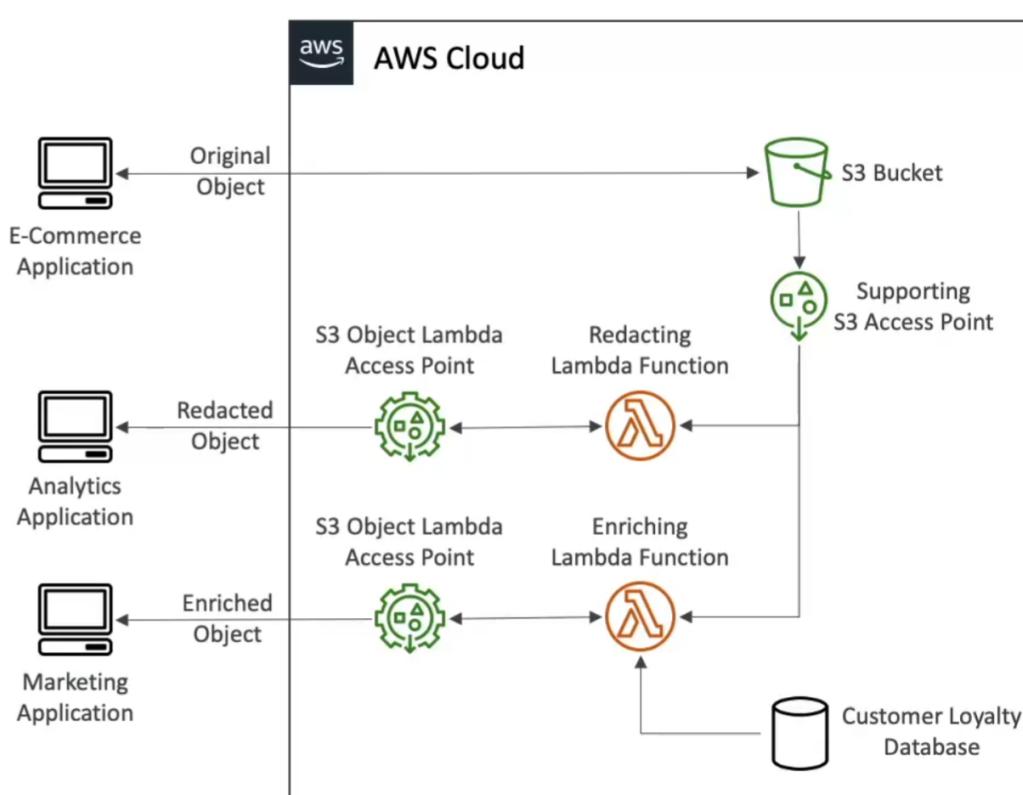
S3 - Access Points

- 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



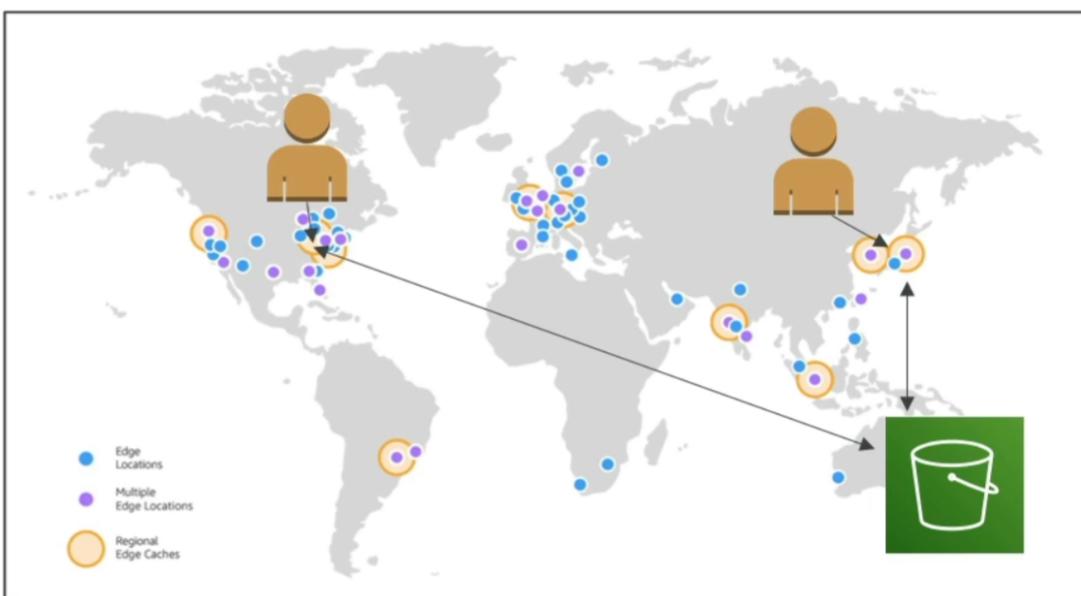
S3 Object Lambda

- 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

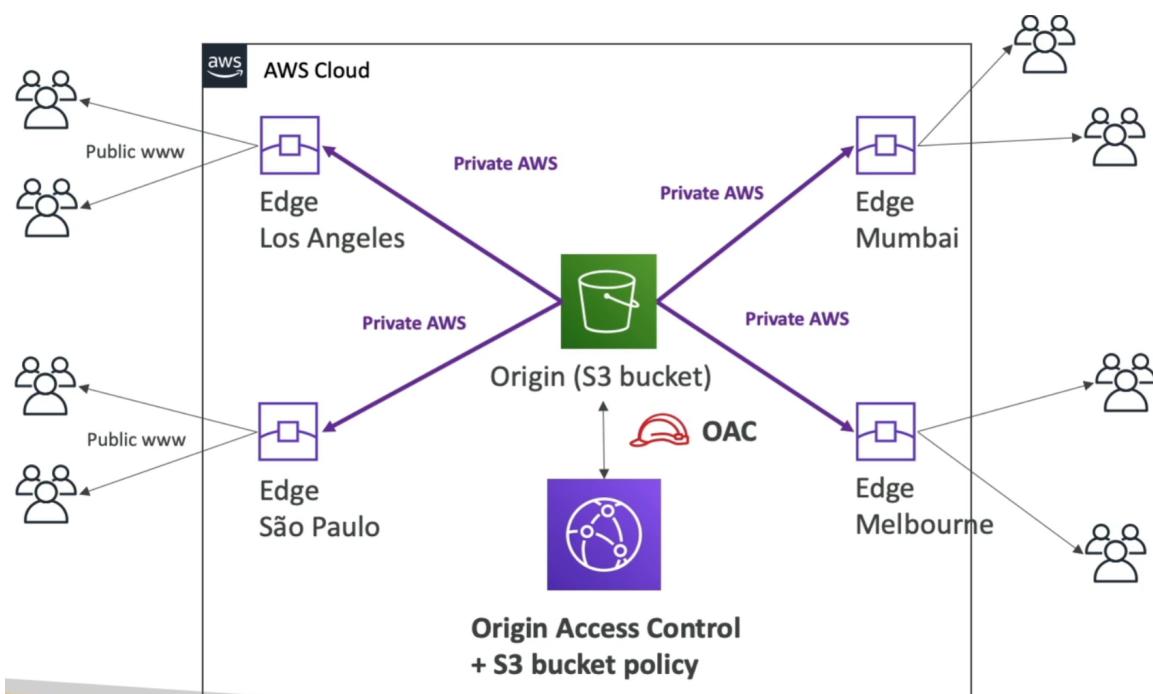
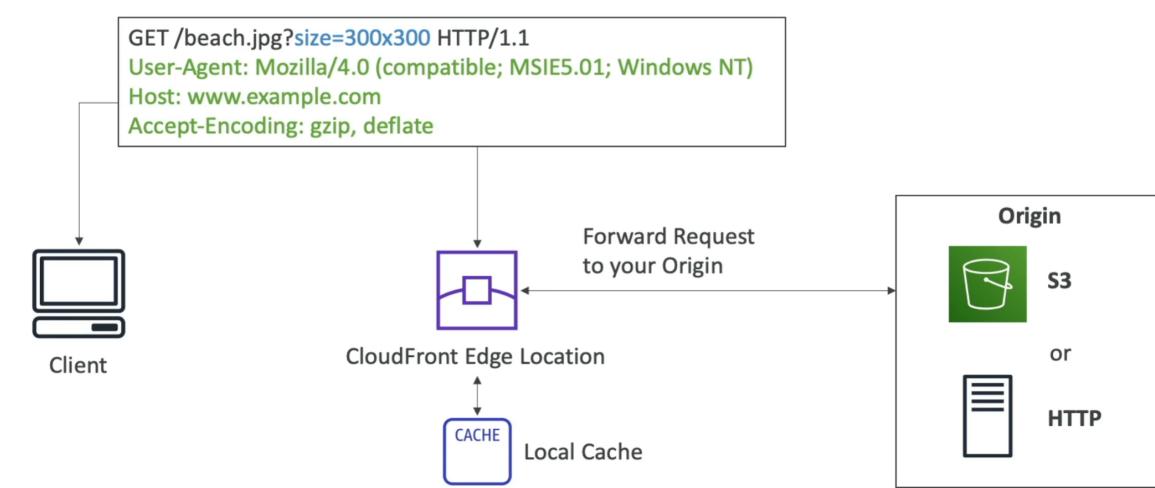


Source: <https://aws.amazon.com/cloudfront/features/?nc=sn&loc=2>

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)
 - **Create 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

Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)
All objects in this bucket are owned by this account.
Access to this bucket and its objects is specified using

ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (3 Total, 194.8 KB)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	beach.jpg	-	image/jpeg	85.8 KB
<input type="checkbox"/>	coffee.jpg	-	image/jpeg	108.4 KB
<input type="checkbox"/>	index.html	-	text/html	607.0 B

Destination

Destination

<s3://demo-cloudfront-stephane-v4>

► **Destination details**

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

Servicess 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](#)

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
---	---

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

Feedback Looking for language selection? Find it in the new Unified Settings. © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences