



## **Project Report - Manual Exercises (Bac +2)**

### **LAB 03**

**Submitted by:** ALAGO CHIEMELA VICTOR  
KHANH NGUYEN TRAN  
DUC-TIN NGUYEN

**Projects Dates:** 13<sup>th</sup> March 2024 to 19<sup>h</sup> March 2024.

Completed in partial fulfillment of the requirements for the course:  
**CLOUD COMPUTING**

At:

**EPITA, SCHOOL OF ENGINEERING AND COMPUTER SCIENCE**

**Academic Year:** 2023/2024

**Paris, 19<sup>th</sup> March 2024.**

## LAB 03 – AWS S3 Bucket

### *Introduction:*

The lab is structured into three main parts, each designed to progressively introduce users to more complex functionalities of S3, starting with the basics of bucket creation and object upload, advancing to hosting static websites, and finally, exploring version control of stored objects.

Part 1 focuses on the initial setup, guiding users through creating an S3 bucket and uploading different types of objects. This section provides step-by-step instructions on how to navigate the AWS Console, configure the bucket settings to ensure security and privacy, and successfully upload files.

Part 2 expands on the utility of S3 buckets by demonstrating how to use them for static website hosting. It introduces the concept of lifecycle rules to manage storage costs and ensure efficient data handling. This includes transitioning objects to more cost-effective storage classes after a certain period and setting up rules for automatic expiration.

Part 3 delves into enabling versioning for the S3 bucket, a crucial feature for maintaining data integrity and facilitating the recovery of previous versions of files. This section covers the re-upload of files to test and confirm the versioning feature is working as intended.

Throughout the lab, detailed guidelines and illustrations support the theoretical explanations, ensuring that users can follow along and apply the concepts in a practical, hands-on manner.

# 1. Create a bucket

AWS Region  
Europe (Ireland) eu-west-1

Bucket name [Info](#)  
kntranbucket2

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

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

[Choose bucket](#)

Format: s3://bucket/prefix

**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 only policies.

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

Object Ownership  
Bucket owner enforced

Figure 1.a. Setup 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.

Figure 1.b. Setup 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

---

## Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#) 

No tags associated with this bucket.

Add tag

---

## Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type | [Info](#)

- ☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
- Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [AWS console](#).

Figure 1.c. Setup bucket versioning

### There are many reasons why creating a bucket is very crucial:

- Buckets provide a unique namespace on the internet for your data. The bucket name is unique globally across all AWS regions, ensuring that your data's storage location is distinct and accessible via a unique DNS address.
- With buckets, you can implement security features such as encryption, both at rest and in transit, to protect sensitive information.

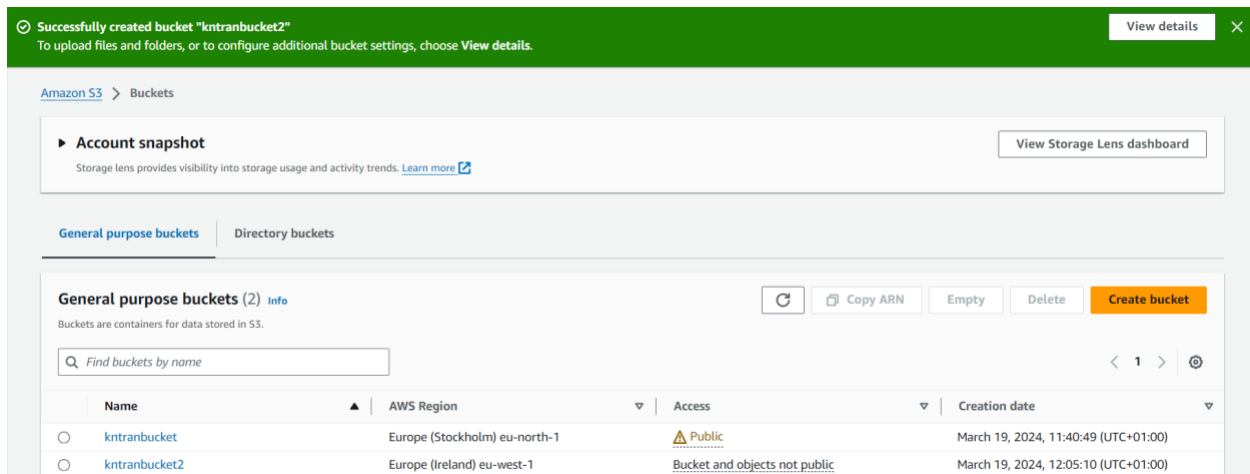


Figure 1.d. Finished setting up bucket

## 2. Upload files to S3

The advantages of uploading files to Amazon S3 (Simple Storage Service) span various aspects of data management, storage, security, and integration.

S3 offers comprehensive security features that help protect your data. This includes server-side encryption for data at rest, the option to use AWS Key Management Service (KMS) for managing encryption keys, and secure data transfer over SSL/TLS.

S3 provides a suite of management features to automate data transfers, set lifecycle policies for automatic archiving or deletion, and monitor and log access requests.

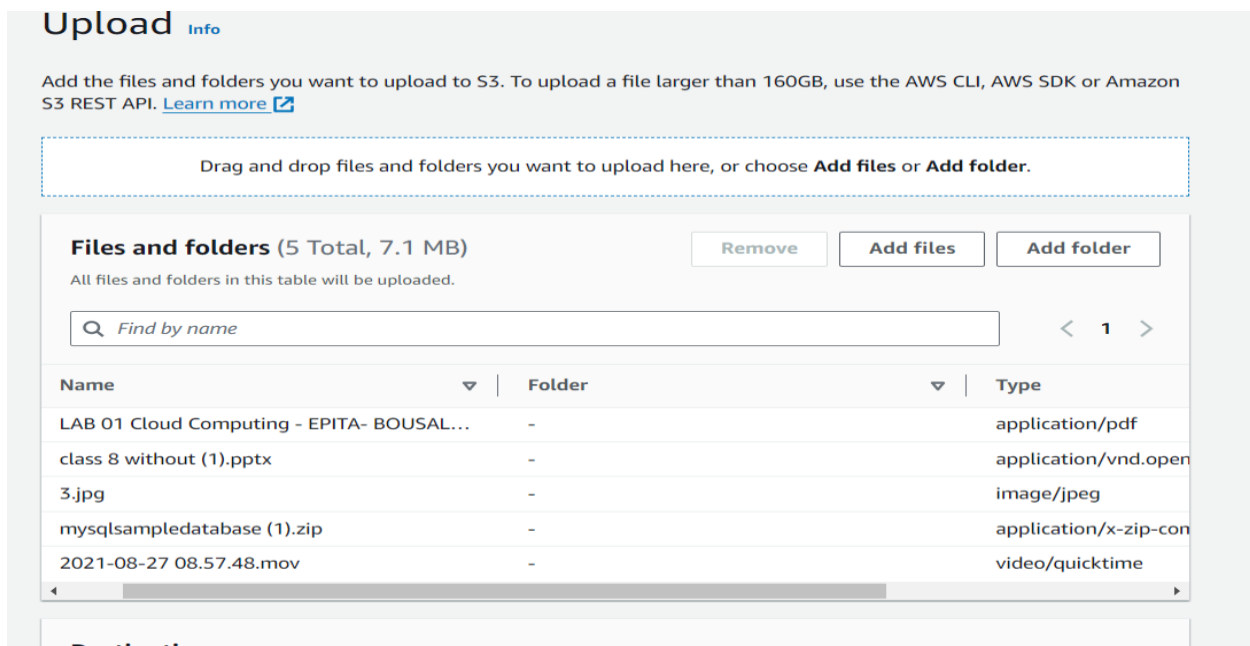


Figure 2.a. Uploading different files

Upload succeeded  
View details below.

### Summary

Destination s3://kntranbucket2	Succeeded 5 files, 7.1 MB (100.00%)	Failed 0 files, 0 B (0%)
-----------------------------------	--	-----------------------------

Files and folders

Configuration

### Files and folders (5 Total, 7.1 MB)

< 1 >

Name	Folder	Type	Size	Status	Error
LAB 01 Clou...	-	application/...	2.9 MB	Succeeded	-
class 8 with...	-	application/...	2.3 MB	Succeeded	-
3.jpg	-	image/jpeg	26.9 KB	Succeeded	-
mysqlsaml...	-	application/...	53.1 KB	Succeeded	-
2021-08-27...	-	video/quickt...	1.9 MB	Succeeded	-

Figure 2.b. Successfully uploaded files

## 3. Static website hosting

### 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](#)

#### Index document

Specify the home or default page of the website.

index.html

#### Error document - optional

This is returned when an error occurs.

error.html

#### Redirection rules – optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

Figure 3.a. Enable web hosting and specify document

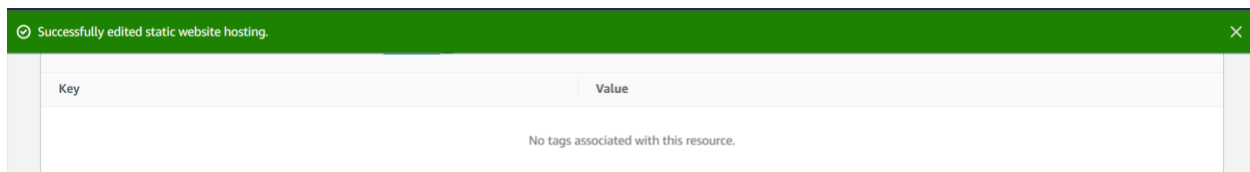


Figure 3.b. Successfully enabled web hosting

### Benefits of hosting a static website on AWS:

- Amazon S3 automatically scales to handle high traffic loads, ensuring that your website remains available and performs well, even during peak times.

## Edit Block public access (bucket settings) [Info](#)

### 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](#)

#### ☐ 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.

Cancel

Save changes

Figure 4.a. Make the bucket public

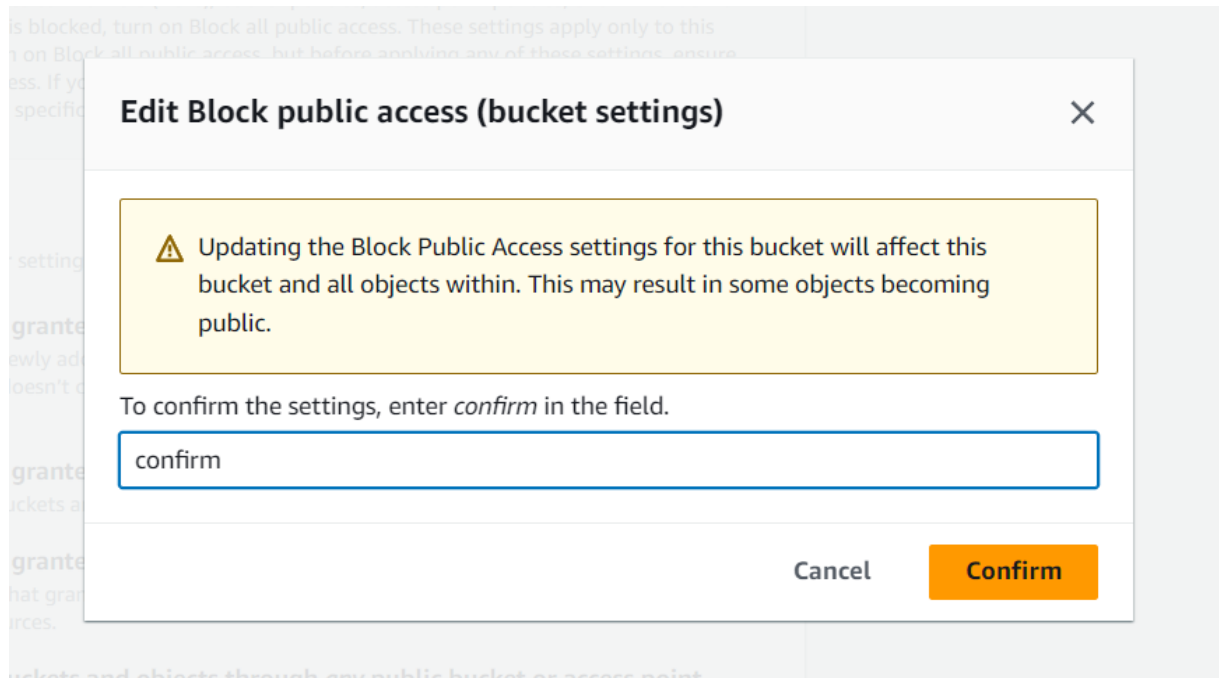


Figure 4.b. Confirm the settings

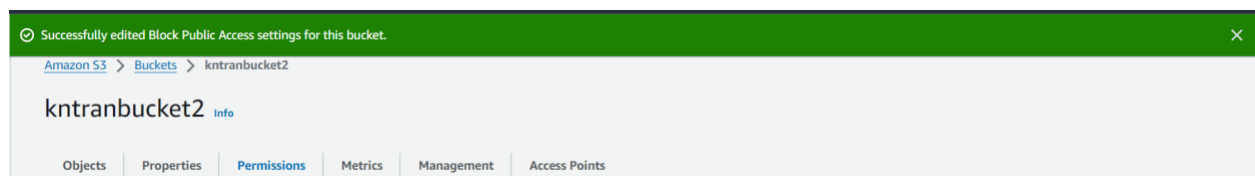


Figure 4.c. Successfully edited the public access

The be able to allow access to the website, we have to make the website go public.

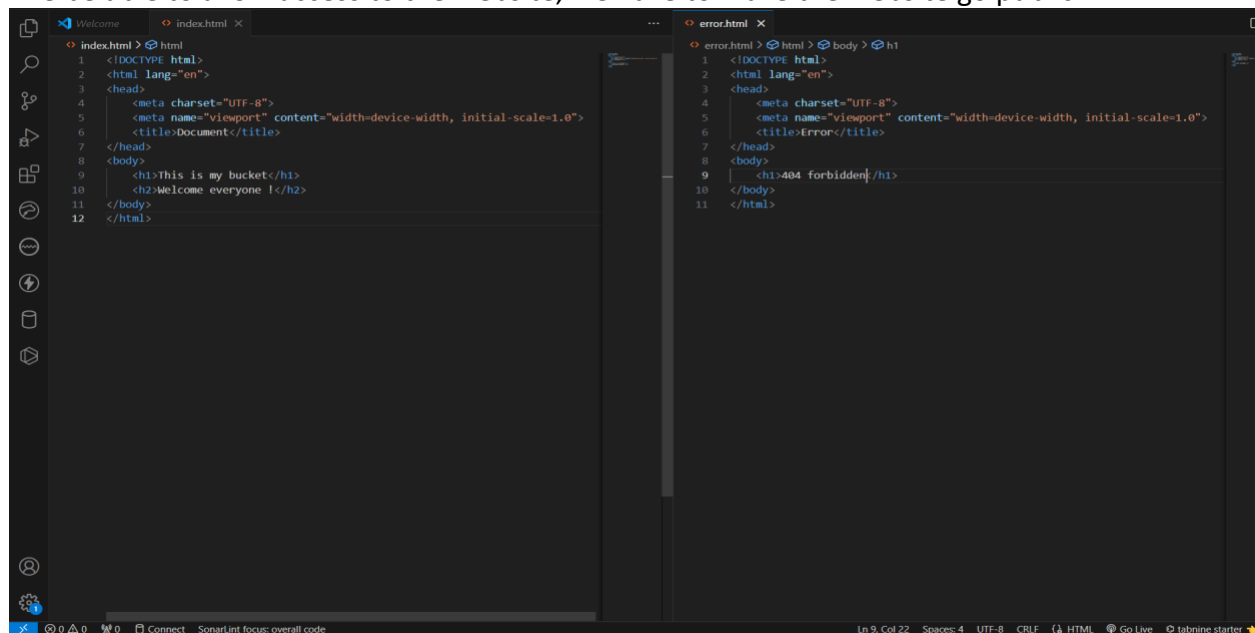


Figure 5.a. Create documents for the static website



Files and folders (2 Total, 475.0 B)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	error.html	-	text/html
<input type="checkbox"/>	index.html	-	text/html

Destination

Info

Destination

s3://kntranbucket2

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

Figure 5.b. Upload the documents to the bucket

Edit bucket policy

Info

Bucket policy

Policy examples

Policy generator

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

Bucket ARN

arn:aws:s3::kntranbucket2

Policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": "*",
8       "Action": "s3:GetObject",
9       "Resource": "arn:aws:s3:::kntranbucket2/*"
10    }
11  ]
12 }
```

Edit statement

Select a statement

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

Add new statement

Figure 6.a. Modify bucket policy to allow access to the static website

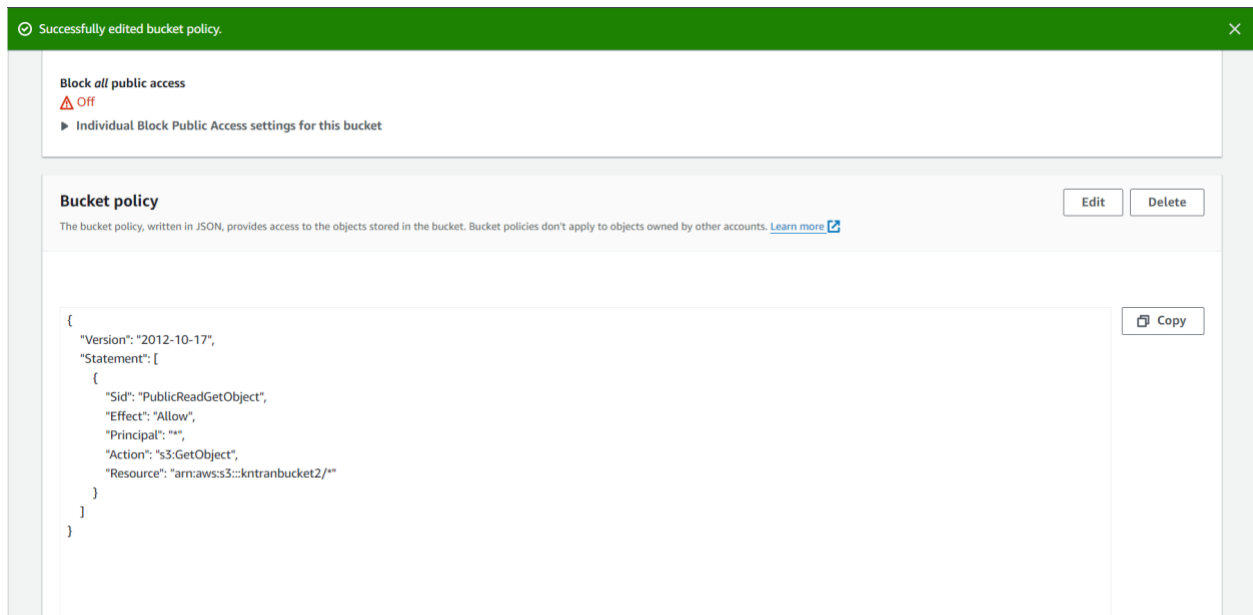


Figure 6.b. Successfully added the policies

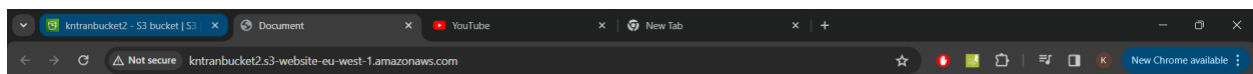


Figure 7. Website content

## Create lifecycle rule [Info](#)

### Lifecycle rule configuration

Lifecycle rule name

Up to 255 characters

Choose a rule scope

- ☐ Limit the scope of this rule using one or more filters
- ☒ Apply to all objects in the bucket



#### Apply to all objects in the bucket

If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". [Learn more](#)

- ☒ I acknowledge that this rule will apply to all objects in the bucket.

### Lifecycle rule actions

Choose the actions you want this rule to perform. Per-request fees apply. [Learn more](#) or see [Amazon S3 pricing](#)

- ☒ Move current versions of objects between storage classes
- ☒ Move noncurrent versions of objects between storage classes
- ☒ Expire current versions of objects
- ☐ Permanently delete noncurrent versions of objects
- ☐ Delete expired object delete markers or incomplete multipart uploads

These actions are not supported when filtering by object tags or object size.

Figure 8.a. Create lifecycle rule

### Transition current versions of objects between storage classes

Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. [Learn more](#)

Choose storage class transitions
Days after object creation

Standard-IA
60
Remove

Add transition

### Transition noncurrent versions of objects between storage classes

Choose transitions to move noncurrent versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects become noncurrent and are consecutively applied. [Learn more](#)

Choose storage class transitions
Days after objects become noncurrent
Number of newer versions to retain - *Optional*

Standard-IA
30
2
Remove

Add transition

### Expire current versions of objects

For version-enabled buckets, Amazon S3 adds a delete marker and the current version of an object is retained as a noncurrent version. For non-versioned buckets, Amazon S3 permanently removes the object. [Learn more](#)

Days after object creation
200

Figure 8.b. Create lifecycle rule

The lifecycle configuration was updated. Lifecycle rule "StorageClassChange" was successfully added.
It may take some time for the configuration to be updated. Press the refresh button if changes to the rule are not displayed.

Amazon S3
Buckets
kntranbucket2
Lifecycle configuration

### Lifecycle configuration

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

Lifecycle rules (1)
View details
Edit
Delete
Actions
Create lifecycle rule

Find lifecycle rules by name

Lifecycle rule name	Status	Scope	Current version a...	Noncurrent versi...	Expired object de...	Incomplete multi...
StorageClassChange	Enabled	Entire bucket	Transition to Standard-IA,	Transition to Standard-IA	-	-

Figure 8.c. Successfully created lifecycle rule

Reasons why we have to create lifecycle rule:

- Lifecycle rules can automate the retention process, ensuring that data is kept for the required duration and then deleted or archived, thereby aiding in compliance with regulatory standards.
- By transitioning data to the most appropriate storage class, you can optimize performance for frequently accessed data and reduce costs for data that doesn't require immediate access.

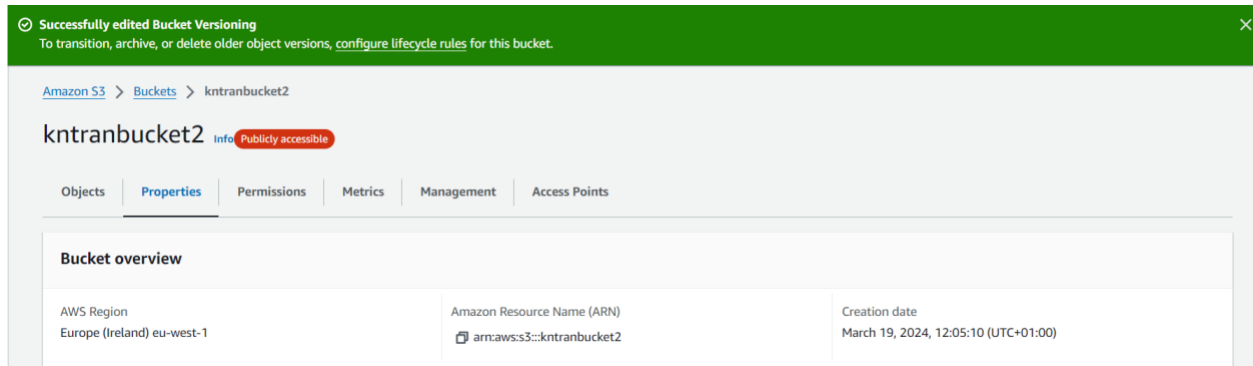


Figure 9.a. Successfully enabled bucket versioning

**Objects (9)** Info

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

☒ Show versions < 1 >

<input type="checkbox"/>	Name	Type	Version ID	Last modified	Size	Storage class
<input type="checkbox"/>	3.jpg	jpg	null	March 19, 2024, 12:07:50 (UTC+01:00)	26.9 KB	Standard
<input type="checkbox"/>	class 8 without (1).pptx	pptx	null	March 19, 2024, 12:07:49 (UTC+01:00)	2.3 MB	Standard
<input type="checkbox"/>	error.html	html	vAtiBchcFs_nzPFAjq_OsZu7niVMAMHD	March 19, 2024, 13:36:45 (UTC+01:00)	234.0 B	Standard
<input type="checkbox"/>	error.html	html	null	March 19, 2024, 12:12:10 (UTC+01:00)	234.0 B	Standard
<input type="checkbox"/>	index.html	html	yq0QypnkXuyNo6xhNA_UTEq357u8Grqd	March 19, 2024, 13:36:46 (UTC+01:00)	274.0 B	Standard
<input type="checkbox"/>	index.html	html	null	March 19, 2024, 12:12:42 (UTC+01:00)	274.0 B	Standard
<input type="checkbox"/>	LAB 01 Cloud Computing - EPITA- BOUSALEM (1).pdf	pdf	null	March 19, 2024, 12:07:48 (UTC+01:00)	2.9 MB	Standard
<input type="checkbox"/>	mysqlsampledatabase (1).zip	zip	null	March 19, 2024, 12:07:50 (UTC+01:00)	53.1 KB	Standard

Figure 9.b. Version ID of newly uploaded files

## Summary:

These tasks underscore several critical aspects of modern cloud computing practices, data management, and organizational agility, reflecting broader implications:

1. **Secure and Scalable Storage Solution:** The creation and management of AWS S3 buckets address the growing need for scalable and secure cloud storage solutions. As organizations generate and rely on vast amounts of data, having a reliable way to store, manage, and share this data securely becomes paramount. AWS S3 offers a durable infrastructure for storing data of any volume, accessible from anywhere, which is crucial for businesses operating in today's digital landscape.
2. **Enhanced Data Accessibility and Sharing:** By learning how to upload objects and configure buckets for public sharing when needed, we can ensure that the organization can efficiently distribute content. This capability is vital for sharing resources with stakeholders, distributing media files, or hosting static content for web applications, enhancing the company's ability to communicate and operate online.
3. **Cost Management and Efficiency:** The section on static website hosting and lifecycle policies introduces essential practices for managing storage costs and ensuring data is stored efficiently. Transitioning objects to less expensive storage classes and setting expiration rules help in reducing costs associated with data storage.
4. **Data Integrity and Recovery:** Implementing version control by enabling bucket versioning is critical for protecting the integrity of data. This feature allows for the recovery of previous versions of files, safeguarding against accidental deletions or modifications.

In summary, the lab's focus on AWS S3 bucket creation, object management, static website hosting, and version control transcends technical training. It embodies key principles of secure, efficient, and innovative data management in the cloud era.