Introduction to S3

How AWS define Amazon S3?

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

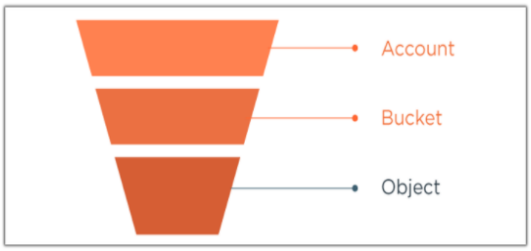
- This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics.
- Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements.
- Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

One of AWS's oldest services, Amazon S3 could be defined as AWS object-based file storage service.

- Amazon S3 stores data in buckets as objects.
- An object consists of a file or metadata that optionally identifies this file.

S3 - Bucket

What is Bucket?

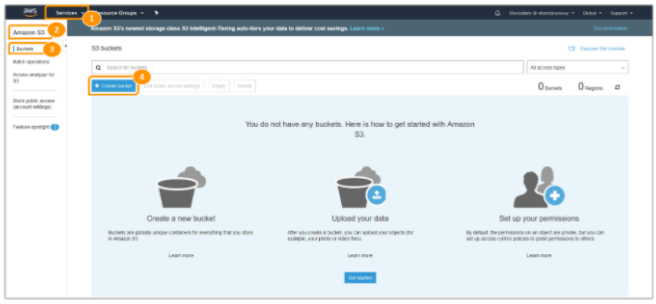


- A bucket is a logical storage unit used to store objects in AWS.
- A bucket can also be considered as a container and also the first thing we create in S3.
- Stored objects in a bucket may be in the form of any files such as text, image, movie, video, etc.
- Objects are consist of keys and values. The key is the name of the object, and the value is the data that the object stores.
- An S3 bucket should be first created in one of the AWS Regions to upload data to Amazon S3. Then any number of objects can be added into that bucket.
- Folders like objects can also be created in a bucket.
- The number of objects that can be stored in a bucket is not limited, but each AWS account can only have 100 buckets at once.
- Since S3 is a global service, a region must be selected when creating a bucket. When you store anything in S3, it's replicated across AZs in that region.
- S3 also saves HTML files in buckets and lets us host static web pages without having to maintain a server.
- S3 is an object-based storage system, not a blocked-based. So buckets are not available for mounting into a server as a drive or a disk.

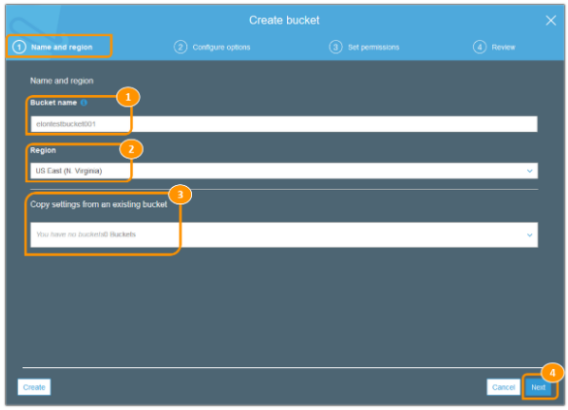
Creating a Bucket - Name and Region

Let's open the S3 service by connecting to the AWS Management Console and create our first bucket.

- Sign in to the AWS Management Console.
- Open the **S3** page using the **Services** tab from the menu bar.
- Click the **Buckets** link from the menu on the left.
- If you have not created a bucket before, the page will return empty as below.



- Click **Create bucket** tab.



Bucket name:

First, we should define the **bucket name**.

- This name must be **unique**.
- If you type a bucket name created by someone else before, you will receive a warning that this name exists.
- For example, if you want to create a bucket named test, you cannot create it since it has been used before.
- Let's call it special with our names like **elontestbucket001**.

Region:

Secondly, the Region where the bucket will be created must be determined.

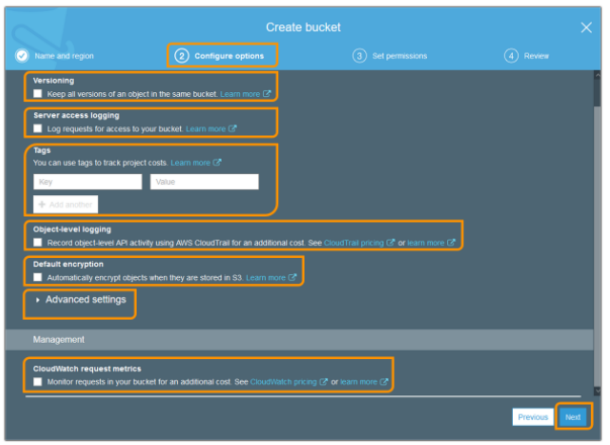
- Because S3 is a region-based service, a bucket can be created only in a specific region.
- Multiple buckets can be created in different regions and synchronized with each other, but a bucket can only be held in one region.
- So we cannot distribute a bucket to all regions.
- The region you want to work on should be selected for holding buckets according to your needs.
- In this example, let's select **US East (N. Virginia)**.

Copy settings from an existing bucket:

Thirdly, **Copy settings from an existing bucket** option can be used if there is a bucket that created before.

- Settings in that bucket can be taken for creating a new bucket.
- So when creating more than one bucket, we are free from adjusting each bucket each time.
- In this example, there is no bucket that was created before in the account and also no need to use this option. So, leave it as default.
- Click the **Next** button to go on the second step.

Creating a Bucket - Configure Options



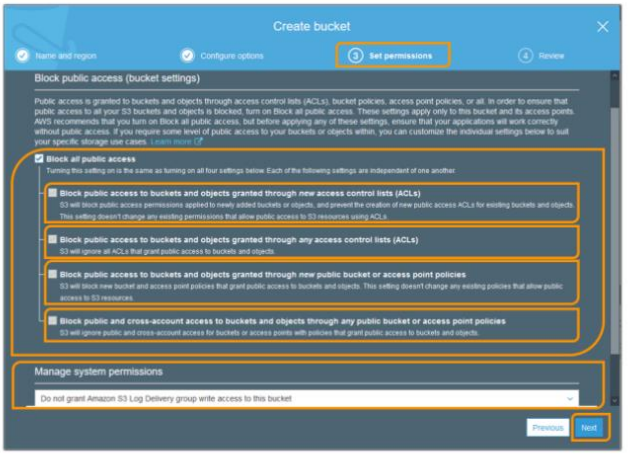
AWS offers the following options for creating a bucket in this step.

- Versioning
- Server access logging
- Tags
- Object-level-logging
- Default encryption
- Advanced settings
- CloudWatch request metrics

The options on this page will be discussed in more detail in the next lessons.

- So, leave it as default.
- Click the **Next** button to go on the third step.

Creating a Bucket - Set Permissions & Review



This is the part where we define the permissions regarding access to the bucket we will create in S3. Under **Block all public access** option, there are 4 different sub-options for accessing the bucket as below.

Block all public access:

- **Block public access to buckets and objects granted through new access control lists (ACLs)**
- **Block public access to buckets and objects granted through any access control lists (ACLs)**
- **Block public access to buckets and objects granted through new public bucket or access point policies**
- **Block public and cross-account access to buckets and objects through any public bucket or access point policies**

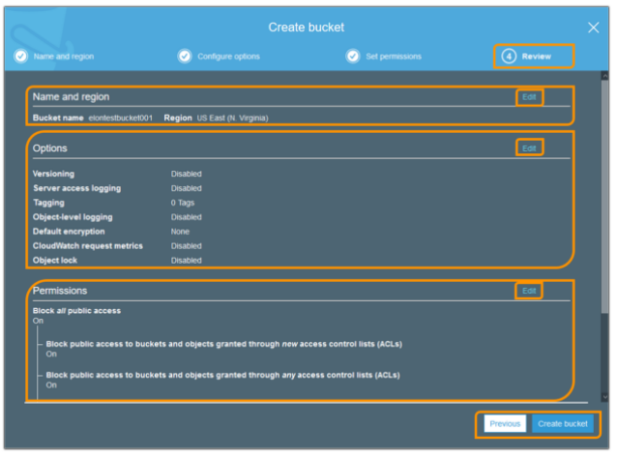
Previously, AWS created all buckets as public means open to the outside world.

- Because some people didn't know exactly or missed that, they might put a lot of important files in those buckets.
- So, this can be an important issue that causing a major security weakness.
- AWS has changed this in recent years and Public access to buckets is no longer open by default.

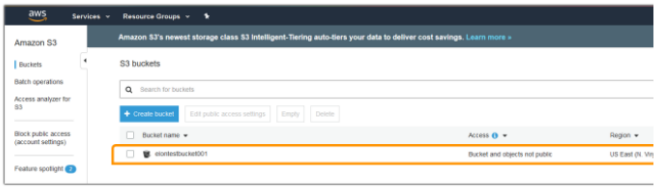
Now, when creating buckets, it is displayed by AWS as blocked to public access by default. As AWS mentioned on the page;

- 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 to suit your specific storage use cases.

Click the **Next** button to go on the final step.

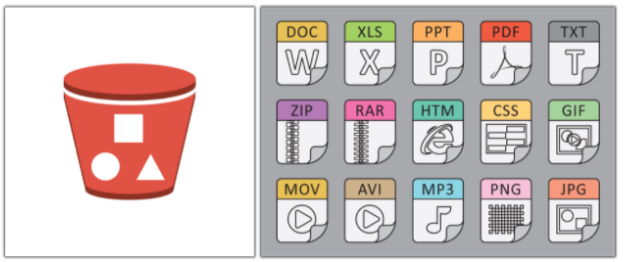


- At this stage, all previous transactions can be reviewed and edited if needed, and the previous step can be returned by clicking the Previous tab.
- After the review process, the bucket can be created by clicking the **Create bucket** tab.



- Congratulations! The first bucket was successfully created.

What is Object in S3 ?

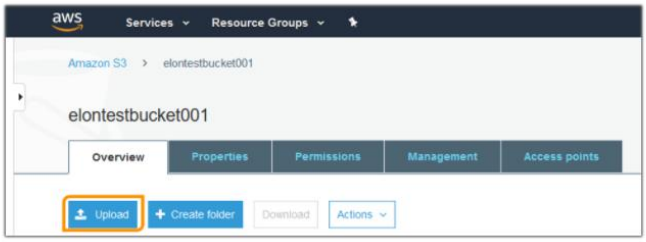


- An object can be any kind of file; a text file, a photo, a video, etc.
- Objects are consist of keys and values.
- The key is the name of the object, and the value is the data that the object stores.
- Objects have metadata that means information about data. For example, the creation date of the object, size, content length variables are metadata that are kept with that object.
- An unlimited number of data objects can be added to a bucket.
- Objects exist in buckets that are created in a specific AWS Region. Objects never leave that region unless you explicitly transfer them to a different region.
- The object size of the data can be up to 5 TB. Max 5 TB size is a limit for a single file. It is unlimited in terms of the number of files you can put in S3. You can put as many files as you want.
- The max. size of an object you can upload via AWS Management Console is 160 GB. For uploading a file greater than 160 GB, the AWS CLI, AWS SDK, or Amazon S3 REST API is needed to be used.
- Objects can also be moved to a created folder in S3.
- If the object uploaded in a bucket no longer needs to be stored, it should be deleted to prevent further charges. Because while the bucket is free to create, objects uploaded into buckets are charged as long as they are stored in the bucket.

Uploading an Object - Select Files

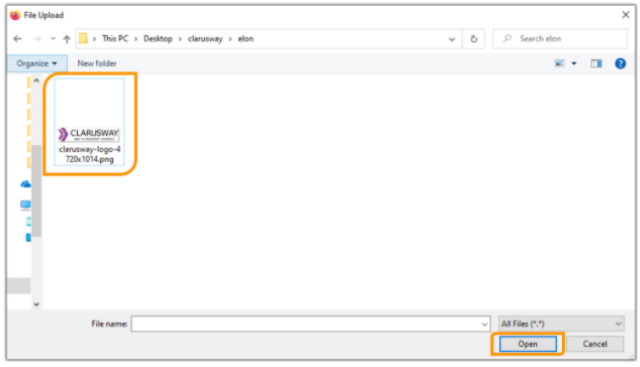
Let's open the S3 service by connecting to the AWS Management Console and upload an object to the bucket we created before.

- Sign in to the AWS Management Console.
- Open the **S3** page using the **Services** tab from the menu bar.
- Click the **Buckets** link from the menu on the left.
- Then open the bucket we created before by clicking on it.

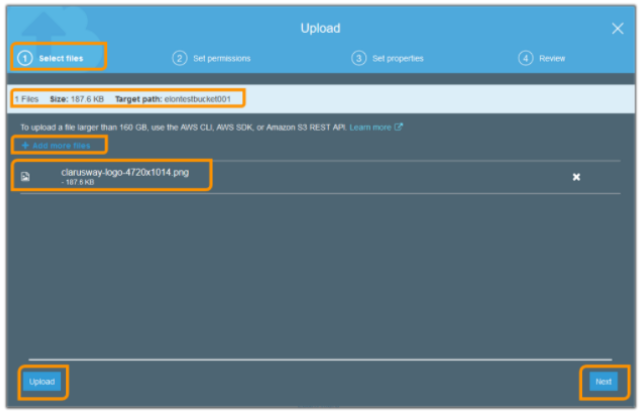


- Click the **Upload** button.

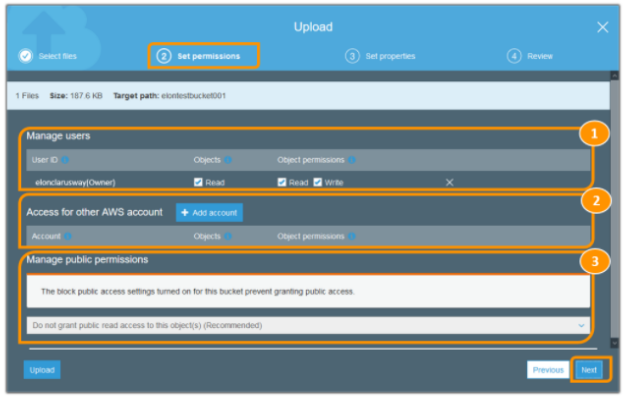
- Files are can be uploaded by either drag-and-drop or by pointing and clicking. Only the Chrome and Firefox browsers support drag-and-drop functionality.
- Click the **Add files** button to point and click the file.



- Click the **Open** button.



Uploading an Object - Set Permissions

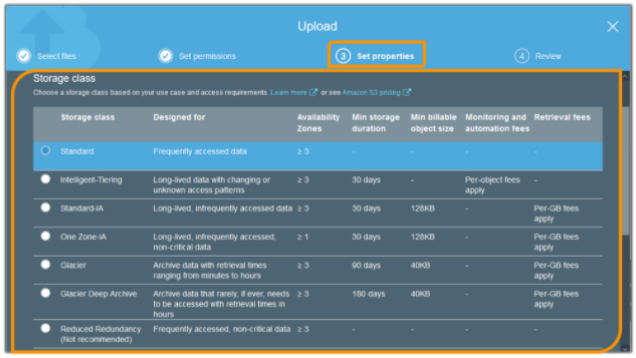


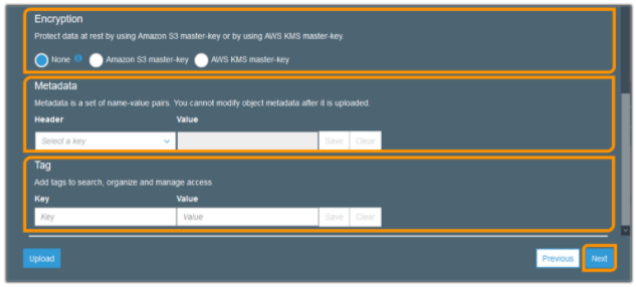
- On the **Set Permissions** Step;
  1. **The permissions for the AWS account owner** can be changed by **Manage users** options. The owner does not refers to an IAM user, it refers to the AWS account root user.
  2. **Add account** option can be used to grant access to another AWS account.
  3. **Manage public permissions** option lets users grant read access to objects to the general public (everyone in the world). AWS defines **Granting public read access** as applicable to a small subset of use cases such as when buckets are used for websites and recommends not to change the default setting of **Do not grant public read access to this object(s)**. Object permissions can be changed any time after you upload the object.
- Click the **Next** button to go on the next step.

Uploading an Object - Set Properties

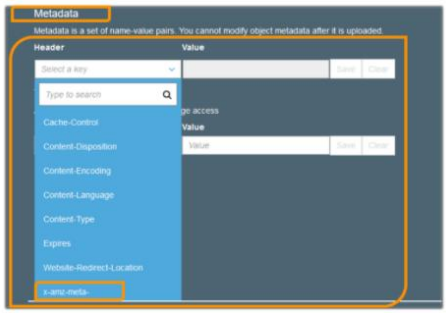
On the **Set Properties** Step; the storage class, encryption method, metadata, and tags information can be defined as below.

- A **storage class** should be selected for the files uploading according to user needs such as AZ's, storage duration, and fees, etc. We'll see the **storage class** in more detail on the following lessons.





- Choose which form of **encryption** you are uploading for the files. If you wouldn't want to encrypt them, pick **None**.
- To encrypt the uploaded files using keys that are managed by Amazon S3, choose **Amazon S3 master-key**.
- To encrypt the uploaded files using the AWS Key Management Service (AWS KMS), choose **AWS KMS master-key**. Then choose a customer master key (CMK) from the list of AWS KMS CMKs.

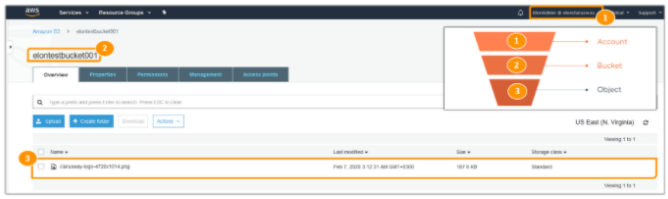


- **Metadata** for S3 objects is represented by a name-value (key-value) pair and can not be modified after the object is uploaded.
- Two types of metadata exist in S3: **AWS S3 system-defined metadata**, and **user-defined metadata**.
- A header can be select to add **Amazon S3 system-defined metadata** to all of the objects uploading.
- Any metadata that begins with the **x-amz-meta- prefix** will be regarded as **user-defined metadata**. User-defined metadata is stored with the object, and retrieved when the object is downloaded.

- **Tagging** an object gives users the ability to categorize data.
- Each tag is a key-value pair and both are case sensitive.
- Max. 10 tags can be defined per object.
- Click the **Next** button to go on the final step.

Uploading an Object - Review

- **Review** and then click the **Upload** button.



- Congratulations! The first object was successfully added to the bucket.