S3 Object Components-Advance

Initial Information About The lesson

In this lesson, we will take a look at all components of all parts of the S3 Object.

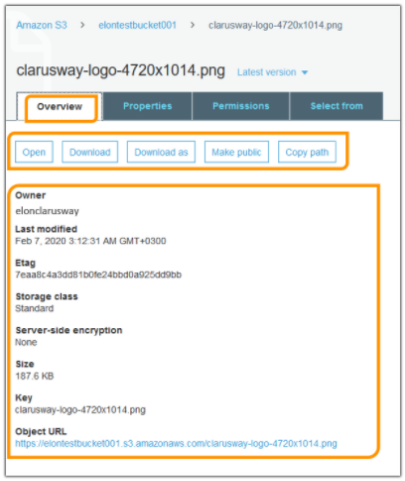
Since each of the AWS services is integrated with many other services, sometimes it is not possible to learn all aspects of a service or a feature of that service without knowing the other services.

Therefore, as mentioned above, in this lesson the entire component of the S3 bucket will be explained. However, some, especially those used with other AWS services, will be explained at a high level, and some other components will be shown in more detail and with examples.

- Please apply the detailed described components yourself also.
- It will be sufficient to have a general knowledge about the components described at a high level.
- By completing this AWS course, you will have sufficient knowledge about the components described in this lesson.

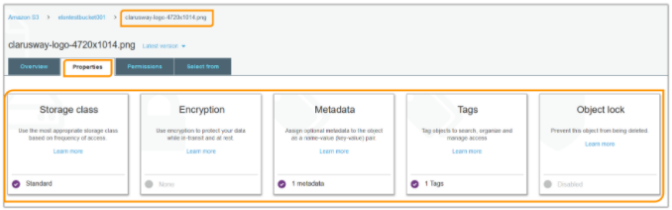
Object - Overview

- To display the **Object overview panel** using the Amazon S3 console, select the **Overview** tab.
- Select the **checkbox** next to the name of the object for which you want an overview.
- A panel that provides an overview of all of an object's essential information at one location will appear.



- The object can be opened, downloaded, made public or the path of the object can be copied by using relevant buttons on the object overview panel.
- On this panel, there is also some information such as **owner, last modified, etag, storage class,** etc.
- If the object is not blocked to public, it can also be opened on a web browser by clicking **Object URL** link.

Object - Properties

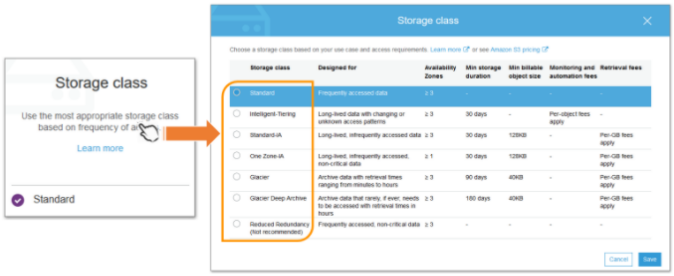


After selecting the **Properties** tab, some settings and information panels appear on the page.

- Storage Class
- Encryption
- Metadata
- Tags
- Object lock

Now we will examine what we need to know about these panels one by one.

Properties - Storage Classes



Each object in Amazon S3 has a storage class associated with it. Amazon S3 offers a range of storage classes for the objects that you store. You choose a class depending on your use case scenario and performance access requirements. All of these storage classes offer high durability.

AWS offers those different storage classes to suit different usage scenarios with a high level of reliability and support SSL data encryption during transmission but they differ by their cost.

Storage Class Options:

- **Standard**
- **Intelligent-Tiering**
- **Standart-IA**
- **One Zone-IA**
- **Glacier**
- **Glacier Deep Archive**
- **Reduced Redundancy** (Not recommended by AWS)

All of the storage classes **except for One Zone-IA** are designed to be resilient to simultaneous complete data loss in a single Availability Zone and partial loss in another Availability Zone. Storage class types will be discussed in more detail in the following lessons.

Properties - Encryption

Data encryption is used to provide added security for data objects stored in S3 buckets. Data protection refers to protecting data while in transit and at rest.

- **Transit** means it travels to and from Amazon S3. The data can be protected by using **Secure Sockets Layer (SSL)** or **Client-side encryption** while the data is in transit.
- **Rest** means it is stored on disks in Amazon S3 data centers. The data can be protected by using **Server-Side Encryption** or **Client-side encryption** when the data is at rest.

Client-side encryption is the act of encrypting data before sending it to Amazon S3. AWS costomers can use either a customer master key (CMK) stored in AWS Key Management Service (AWS KMS) or a master key they store within their application.

Server-side encryption is the encryption of data at its destination by the application or service that receives it. Amazon S3 encrypts your data at the object level as it writes it to disks in its data centers and decrypts it for you when you access it. The objects are encrypted using Server-side encryption with either **Amazon S3-managed keys (SSE-S3)** or **AWS Key Management Service (AWS KMS)** customer master keys (CMKs).

Amazon S3-Managed Keys (SSE-S3):

When you use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3), each object is encrypted with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

AWS Key Management Service (SSE-KMS):

Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service. There are separate permissions for the use of a CMK that provides added protection against unauthorized access of your objects in Amazon S3. SSE-KMS also provides you with an audit trail that shows when your CMK was used and by whom. Additionally, you can create and manage customer-managed CMKs or use AWS managed CMKs that are unique to you, your service, and your Region.

AWS customers can select either AES-256 or AWS-KMS type encryption from this panel on S3 management console.

Properties - Metadata

Users can define object metadata either when uploading an object or after the object created. Following are the two kinds of object metadata in AWS:

- System metadata
- User-defined metadata.

System-Defined Object Metadata:

For each object stored in a bucket, Amazon S3 maintains and processes a set of system metadata. For example, Amazon S3 maintains the object creation date and size metadata and uses this information as part of object management. When you create objects, you can configure values of these system metadata items or update the values when you need to. There are two categories of system metadata:

- Metadata such as object creation date is a **system controlled metadata** where only Amazon S3 can modify the value.
- Other system metadata, such as the storage class configured for the object and whether the object has server-side encryption enabled, are examples of customer controlled system metadata. If your bucket is configured as a website, sometimes you might want to redirect a page request to another page or an external URL. In this case, a webpage is an object in your bucket. Amazon S3 stores the page redirect value as the system metadata whose value you control.

User-Defined Object Metadata:

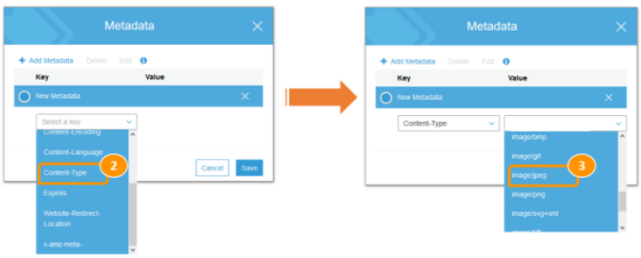
When uploading an object, you can also assign metadata to the object. You provide this optional information as a name-value (key-value) pair when you send a PUT or POST request to create the object.

- User-defined metadata is a set of key-value pairs.
- Amazon S3 stores user-defined metadata keys in lowercase.

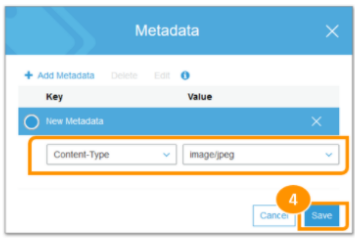
Adding System Metadata

- Click **Add metadata** link.

- Select a key from the **Select a key** menu.
- Depending on which key you select, select a value from the **Select a value** menu or type a value.



- Click the **Save** button.



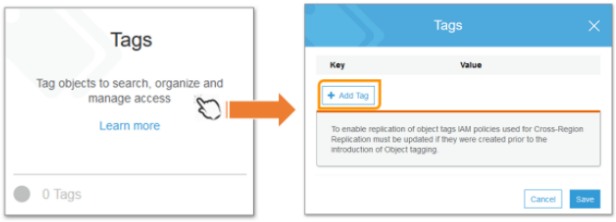
Adding User-Defined Metadata

- Click **Add metadata** link.

- Select the **x-amz-meta-** key from the **Select a key** menu.
- Any metadata starting with the prefix **x-amz-meta-** is user-defined metadata.
- Depending on which key you select, select a value from the **Select a value** menu or type a value.

- Type a custom name following the **x-amz-meta-** key.
- For example, for the custom name **info**, the metadata key would be **x-amz-meta-info.**
- Type a value for the custom key for example test-metadata.
- Click the **Save** button.

Properties - Tags

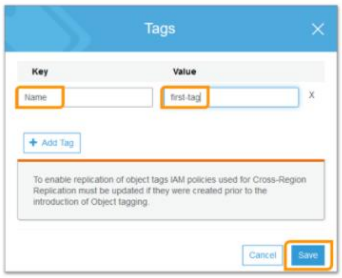


Object tagging is used to categorize storage. For example, assume that you store project files in your S3 bucket. You might tag these objects with a key named project and value, like project name. Following are some features of tagging:

- Multiple tags can be added to an object.
- Tags can be added either to existing objects or to new objects when you upload them.
- The key and values are case sensitive.
- Tags that are associated with an object must have unique tag keys.
- Up to 10 tags can be associated with an object.

To add a tag to an object:

- Click **Add Tag** button.

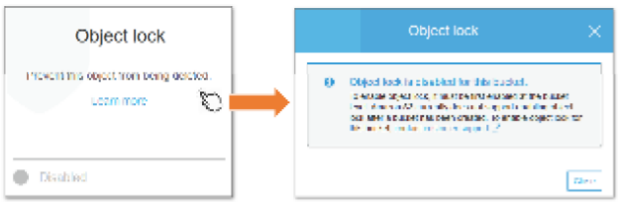


- Type **key** and **value** of the tag.
- Click the **Save** button.

Properties - Object Lock

You can use Amazon S3 object lock to store objects using a *write-once-read-many* (WORM) model.

- It can help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely.
- You can use Amazon S3 object lock to meet regulatory requirements that require WORM storage, or add an extra layer of protection against object changes and deletion.

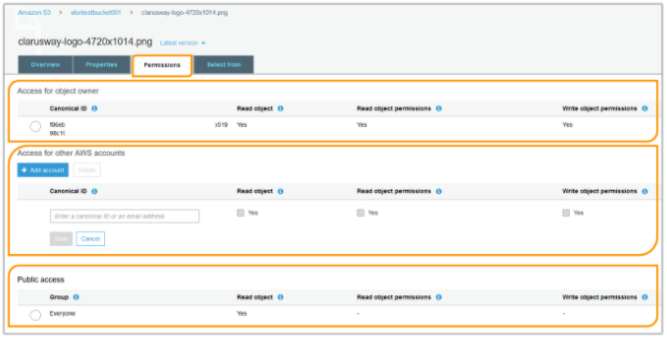


To enable object lock, it must be first enabled at the bucket level.

- Amazon S3 currently does not support enabling object lock after a bucket has been created.
- To enable object lock for this bucket, you should contact customer support only.

To enable object lock in an enabled bucket, you can follow the same instructions in the Properties - Object Lock page in the **S3 Bucket Components** lesson.

Object - Permissions



You can manage bucket access permissions for the following:

- **Access for object owner**

  The *owner* refers to your AWS account.

- **Access for other AWS accounts**

  To grant permissions to an AWS user from a different AWS account.

⚠ **Caution ! :**

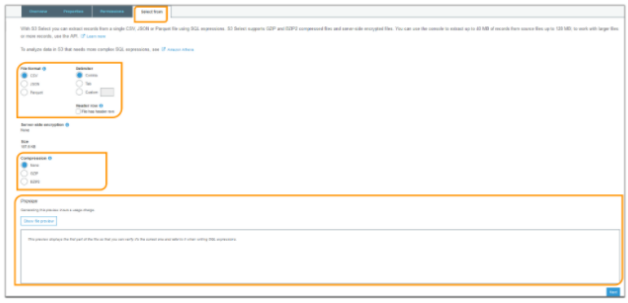
- When you grant other AWS accounts access to your resources, be aware that the AWS accounts can delegate their permissions to users under their accounts. This is known as *cross-account access*.

- **Public access**

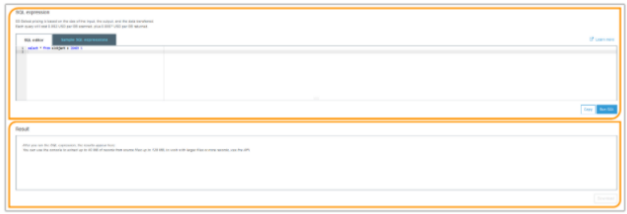
  Granting public access permissions means that anyone in the world can access the bucket.

Object - Select From

With Amazon S3 Select, you can use simple structured query language (SQL) statements to filter the contents of Amazon S3 objects and retrieve just the subset of data that you need. By using Amazon S3 Select to filter this data, you can reduce the amount of data that Amazon S3 transfers, which reduces the cost and latency to retrieve this data.



Amazon S3 Select works on objects stored in CSV, JSON, or Apache Parquet format. It also works with objects that are compressed with GZIP or BZIP2 (for CSV and JSON objects only), and server-side encrypted objects. You can specify the format of the results as either CSV or JSON, and you can determine how the records in the result are delimited.



You pass SQL expressions to Amazon S3 in the request. Amazon S3 Select supports a a subset of SQL. For more information about the SQL elements that are supported by Amazon S3 Select, see SQL Reference for Amazon S3 Select and S3 Glacier Select.