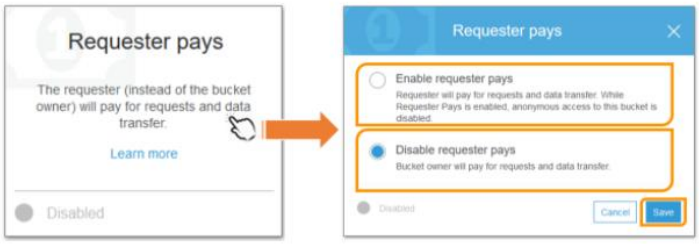
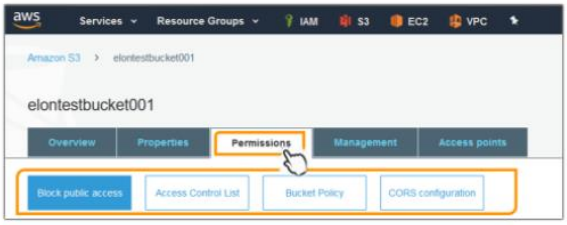
Properties - Requester Pays



You can enable Requester Pays so that the requester (instead of the bucket owner) pays for requests and data transfers.
Enable requester pays: Requester will pay for requests and data transfer. While Requester Pays is enabled, anonymous access to this bucket is disabled.
Disable requester pays: Bucket owner will pay for requests and data transfer.

Bucket - Permissions



Bucket access **permissions** specify which users are allowed access to the objects in a bucket and which types of access they have. For example, one user might have only read permission, while another might have read and write permissions.

The followings are the options for bucket permissions:

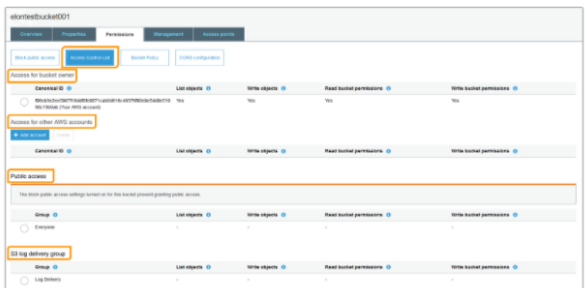
- Block public access (bucket settings)
- Access Control List
- Bucket Policy
- CORS Configuration

Permissions - Block Public Access

Amazon S3 block public access prevents the application of any settings that allow public access to data within S3 buckets.

- **Block public access** can be set when the bucket is created or after it is created.
- The **block public access** setting can be configured for an individual S3 bucket or for all the buckets in your account.

Permissions - Access Control List



Access Control Lists (ACLs) are resource-based access policies that grant access permissions to buckets and objects.

- You can grant permissions to other AWS account users or to predefined groups.
- The user or the group that you are granting permissions to is called the *grantee*.
- Each permission you grant for a user or group adds an entry in the ACL that is associated with the bucket.
- The ACL lists grants, which identify the grantee and the permission granted.
- By default, the owner, which is the AWS account that created the bucket, has full permissions.

You can manage bucket access permissions for the following:

- **Access for your AWS accounted root user**

  The *owner* refers to the AWS account root user, and not an AWS Identity and Access Management (IAM) user.

- **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.

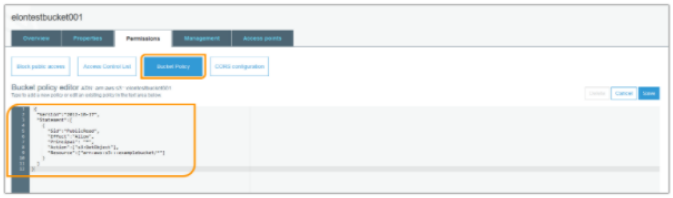
⚠ **Caution ! :**

- There is no extra charge for enabling server access logging on an Amazon S3 bucket.

- **S3 log delivery group**

  S3 log delivery group grant access to Amazon S3 to write server access logs to the bucket. If a bucket is set up as the target bucket to receive access logs, the bucket permissions must allow the **Log Delivery** group write access to the bucket. When you enable server access logging on a bucket, the Amazon S3 console grants write access to the **Log Delivery** group for the target bucket that you choose to receive the logs.

Permissions - Bucket Policy



A bucket policy is a **resource-based** AWS Identity and Access Management (IAM) policy.

- You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it.
- In the **Bucket Policy editor** text box, type or copy and paste a new bucket policy, or edit an existing policy.
- The bucket policy is a JSON file. The text you type in the editor must be valid JSON.

S3 Bucket Components-Advance

Initial Information About The lesson

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

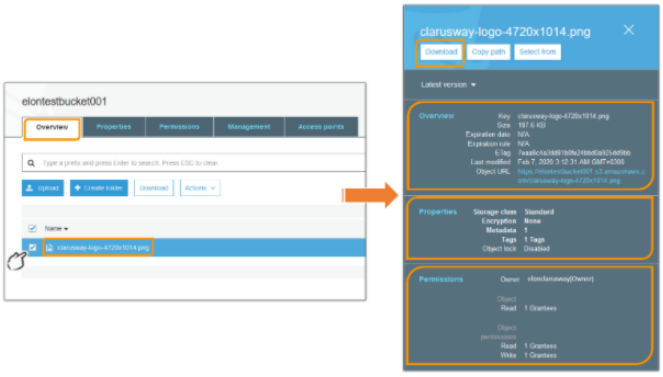
Since each of the AWS services is integrated with many other services, sometimes it is not possible to learn all aspects of a service or a feature of that service without knowing the other services.

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.

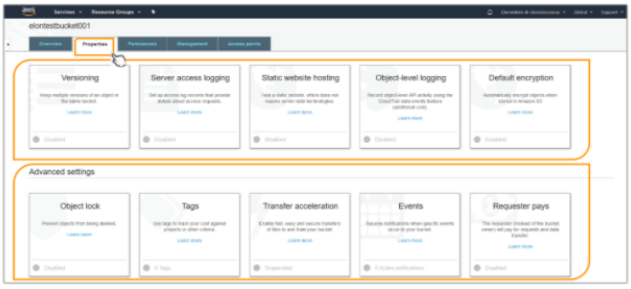
Bucket - Overview

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



- To download the object, choose **Download** in the object overview panel.
- To copy the path of the object to the clipboard, choose **Copy Path**.
- You can also overview some information about the object such as properties end permissions.

Bucket - Properties



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

- Versioning
- Server access
- Static website hosting
- Object level logging
- Default encryption
- Advanced settings (Object lock, Tags, Transfer acceleration, Events, Requester pays.

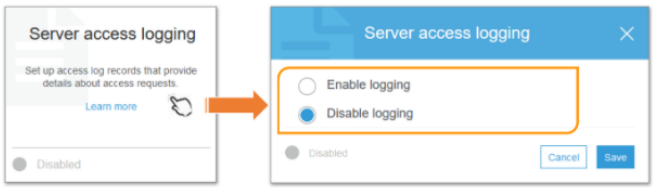
Now we will examine what we need to know about these panels one by one.

Properties - Versioning

This panel is used for setting Object Versioning. Versioning protects you from the consequences of unintended overwrites and deletions. You can also use versioning to archive objects so you have access to previous versions. If a bucket is versioning-enabled, Amazon S3 creates another version of an object under the following conditions:

- If you upload an object that has the same name as an object that already exists in the bucket, Amazon S3 creates another version of the object instead of replacing the existing object.
- If you update any object properties after you upload the object to the bucket, such as changing the storage details or other metadata , Amazon S3 creates a new object version in the bucket.

Properties - Server Access Logging



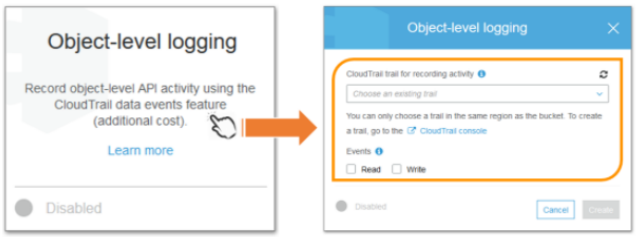
Server Access Logging provides detailed records for the requests that are made to an S3 bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits. By default, Amazon Simple Storage Service (Amazon S3) doesn't collect server access logs.

- When you enable logging, Amazon S3 delivers access logs for a source bucket to a target bucket that you choose.
- The target bucket must be in the same AWS Region as the source bucket and must not have a default retention period configuration.

⚠Caution ! :

- There is no extra charge for enabling server access logging on an Amazon S3 bucket.
- However, any log files that the system delivers to you will accrue the usual charges for storage. (You can delete the log files at any time.)
- AWS does not assess data transfer charges for log file delivery, but does charge the normal data transfer rate for accessing the log files.

Properties - Object Level Logging



To configure a trail to log data events for an S3 bucket, you can use either the AWS CloudTrail console or the Amazon S3 console. If you are configuring a trail to log data events for all the Amazon S3 buckets in your AWS account, it's easier to use the CloudTrail console.

CloudTrail supports logging Amazon S3 object-level API operations such as `GetObject`, `DeleteObject` and `PutObject`. These events are called data events. By default, CloudTrail trails don't log data events, but you can configure trails to log data events for S3 buckets that you specify, or to log data events for all the Amazon S3 buckets in your AWS account.

Cloudtrail topic will be discussed in more detail in the following lessons.

> ⚠ **Caution ! :**
> - Additional charges apply for data events. For more information, see AWS CloudTrail Pricing on AWS official site.

Properties - Default Encryption

Amazon S3 default encryption provides a way to set the default encryption behavior for an Amazon S3 bucket.

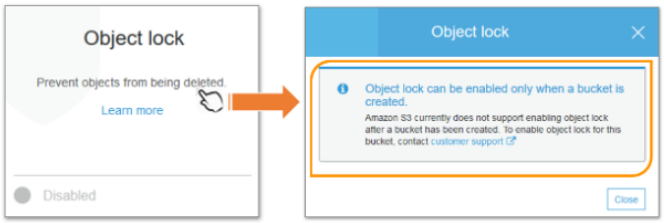
- You can set default encryption on a bucket so that all objects are encrypted when they are stored in the bucket.
- The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or AWS Key Management Service (AWS KMS) customer master keys (CMKs).
- When you use server-side encryption, Amazon S3 encrypts an object before saving it to disk in its data centers and decrypts it when you download the objects.
- Default encryption works with all existing and new Amazon S3 buckets.
- Without default encryption, to encrypt all objects stored in a bucket, you must include encryption information with every object storage request. You must also set up an Amazon S3 bucket policy to reject storage requests that don't include encryption information.
- There are no new charges for using default encryption for S3 buckets.

Properties - Object Lock

Advanced settings topic includes the following sub-topics.

- Object Lock
- Tags
- Transfer Acceleration
- Events
- Requester pays

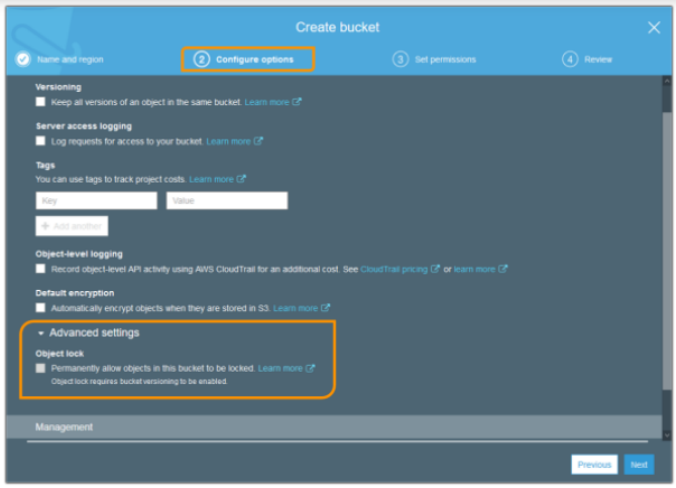
Let's start with the **Object lock** topic first.



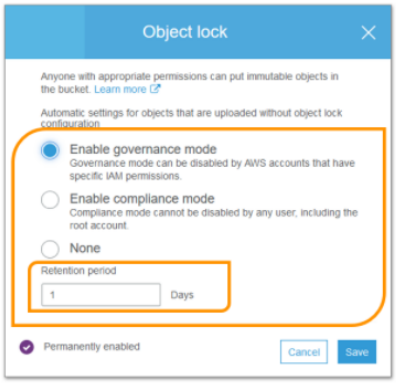
Amazon S3 object lock lets user store objects in Amazon S3 using a **write-once-read-many (WORM)** model. Amazon S3 object lock prevents an object from being deleted or overwritten for a fixed amount of time or indefinitely.

Before you lock any objects, you have to enable a bucket to use the Amazon S3 object lock.

- You enable object lock when you create a bucket.



- After you enable Amazon S3 object lock on a bucket, you can lock objects in that bucket.
- When you create a bucket with object lock enabled, you can't disable object lock or suspend versioning for that bucket.
- If Object lock is enabled when creating the bucket, it can be set by the following panel.



- Choose a **retention mode**.

  In **governance mode**, users can't overwrite or delete an object version or alter its lock settings unless they have special permissions. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary. You can also use governance mode to test retention-period settings before creating a compliance-mode retention period.

  In **compliance mode**, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode ensures that an object version can't be overwritten or deleted for the duration of the retention period.

- Define the **Retention period.**

  A **retention period** protects an object version for a fixed amount of time. When you place a retention period on an object version, Amazon S3 stores a timestamp in the object version's metadata to indicate when the retention period expires. After the retention period expires, the object version can be overwritten or deleted unless you also placed a legal hold on the object version.

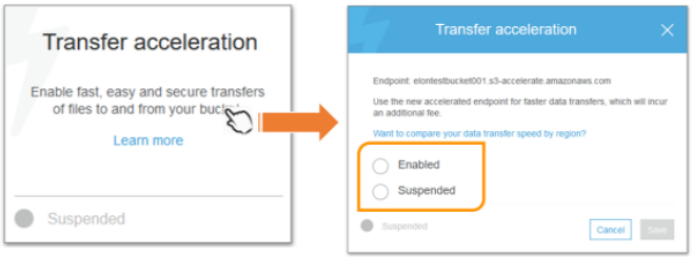
- Finally, click **the Save** button.

Properties - Tags

With AWS cost allocation, you can use bucket tags to annotate billing for your use of a bucket.

- A tag is a key-value pair that represents a label that you assign to a bucket.
- To add tags, choose **Tags**, and then choose to **Add tag**.

Properties - Transfer Acceleration



Transfer Acceleration is an advanced topic and it is useful to have a general knowledge about it.

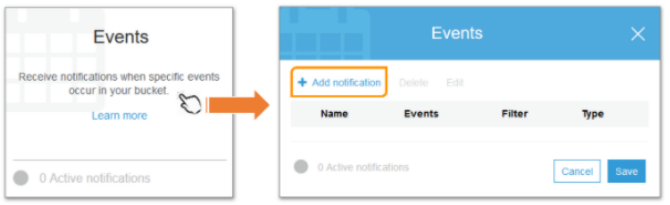
Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket.

- Transfer Acceleration takes advantage of Amazon CloudFront's globally distributed edge locations.
- As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

You might want to use Transfer Acceleration on a bucket for various reasons, including the following:

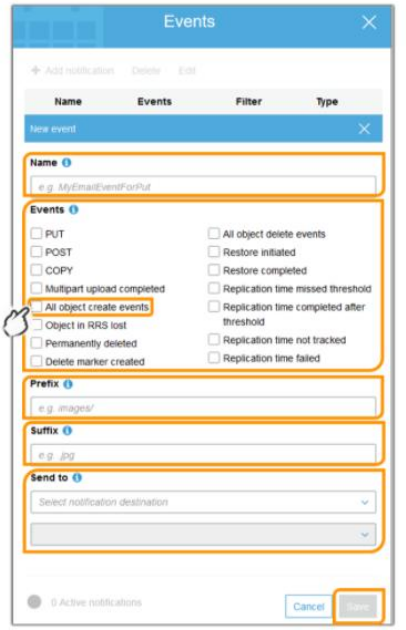
- You have customers that upload to a centralized bucket from all over the world.
- You transfer gigabytes to terabytes of data on a regular basis across continents.
- You are unable to utilize all of your available bandwidth over the Internet when uploading to Amazon S3.

Properties - Events



Amazon S3 bucket events can be enabled to send a notification message to a destination whenever the events occur. When configuring event notifications for a bucket, you must specify the type of events that you want to be notified of and the destination where you want the notifications sent.

- First, click **Add notification** link on the events panel.



- Type a **name** for your event.

- Select the type of event from the **Events** section. For example, if **All object create events** is selected, a notification will be sent anytime an object is created in your bucket. More than one event can also be selected at once.

- Type an object name **Prefix** or a **Suffix** to filter the event notifications by the prefix or suffix. For example, you can set up a filter so that you are sent a notification only when files are added to an image folder (for example, objects with the name prefix **images/** and with the name suffix **.jpg**).

- Choose the type of destination to have the event notifications **sent to**. Event notification messages can be sent to the following types of destinations:

  An Amazon Simple Notification Service (Amazon SNS) topic – A web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients.

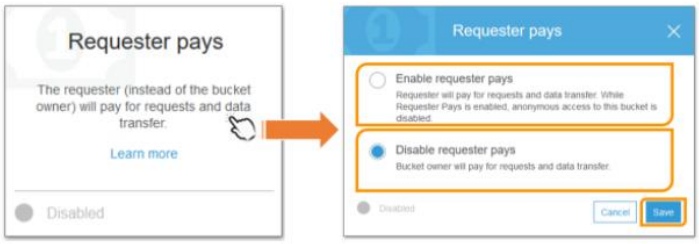
  An Amazon Simple Queue Service (Amazon SQS) queue – Offers reliable and scalable hosted queues for storing messages as they travel between computers.

  Lambda function – AWS Lambda is a compute service where you can upload your code and the service can run the code on your behalf using the AWS infrastructure. You package up and upload your custom code to AWS Lambda when you create a Lambda function.

- Click the **Save** button.
- Amazon S3 sends a **test message** to the event notification destination.

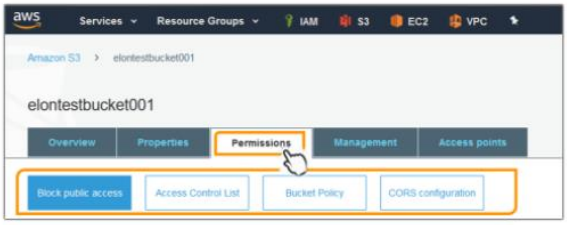
Events topic may seem a bit complicated at this stage. However, it will be much easier to understand as you learn about other services during the course.

Properties - Requester Pays



You can enable Requester Pays so that the requester (instead of the bucket owner) pays for requests and data transfers.
Enable requester pays: Requester will pay for requests and data transfer. While Requester Pays is enabled, anonymous access to this bucket is disabled.
Disable requester pays: Bucket owner will pay for requests and data transfer.

Bucket - Permissions



Bucket access **permissions** specify which users are allowed access to the objects in a bucket and which types of access they have. For example, one user might have only read permission, while another might have read and write permissions.

The followings are the options for bucket permissions:

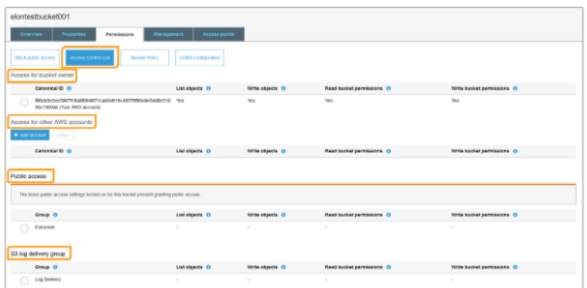
- Block public access (bucket settings)
- Access Control List
- Bucket Policy
- CORS Configuration

Permissions - Block Public Access

Amazon S3 block public access prevents the application of any settings that allow public access to data within S3 buckets.

- **Block public access** can be set when the bucket is created or after it is created.
- The **block public access** setting can be configured for an individual S3 bucket or for all the buckets in your account.

Permissions - Access Control List



Access Control Lists (ACLs) are resource-based access policies that grant access permissions to buckets and objects.

- You can grant permissions to other AWS account users or to predefined groups.
- The user or the group that you are granting permissions to is called the *grantee*.
- Each permission you grant for a user or group adds an entry in the ACL that is associated with the bucket.
- The ACL lists grants, which identify the grantee and the permission granted.
- By default, the owner, which is the AWS account that created the bucket, has full permissions.

You can manage bucket access permissions for the following:

- **Access for your AWS accounted root user**

  The *owner* refers to the AWS account root user, and not an AWS Identity and Access Management (IAM) user.

- **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.

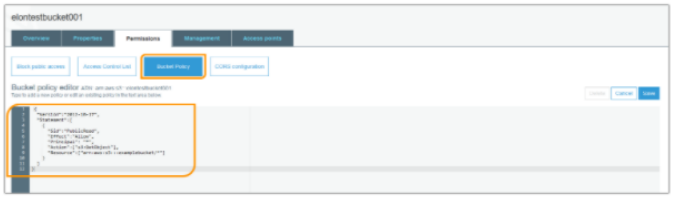
⚠ **Caution ! :**

- There is no extra charge for enabling server access logging on an Amazon S3 bucket.

- **S3 log delivery group**

  S3 log delivery group grant access to Amazon S3 to write server access logs to the bucket. If a bucket is set up as the target bucket to receive access logs, the bucket permissions must allow the **Log Delivery** group write access to the bucket. When you enable server access logging on a bucket, the Amazon S3 console grants write access to the **Log Delivery** group for the target bucket that you choose to receive the logs.

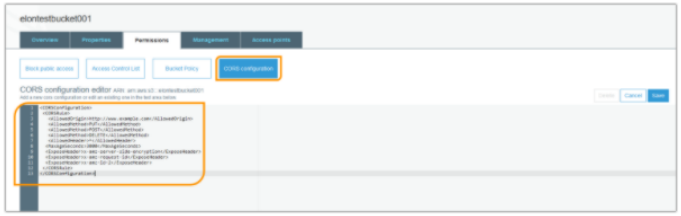
Permissions - Bucket Policy



A bucket policy is a **resource-based** AWS Identity and Access Management (IAM) policy.

- You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it.
- In the **Bucket Policy editor** text box, type or copy and paste a new bucket policy, or edit an existing policy.
- The bucket policy is a JSON file. The text you type in the editor must be valid JSON.

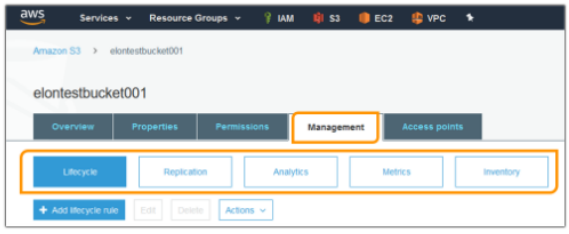
Permissions - CORS Configuration



Cross-Origin Resource Sharing (CORS) allows client web applications that are loaded in one domain to interact with resources in another domain.

- To configure your bucket to allow cross-origin requests, you add CORS configuration to the bucket.
- A CORS configuration is an XML document that defines rules that identify the origins that you will allow accessing your bucket, the operations (HTTP methods) supported for each origin, and other operation-specific information.
- The text that you type in the editor must be valid XML.

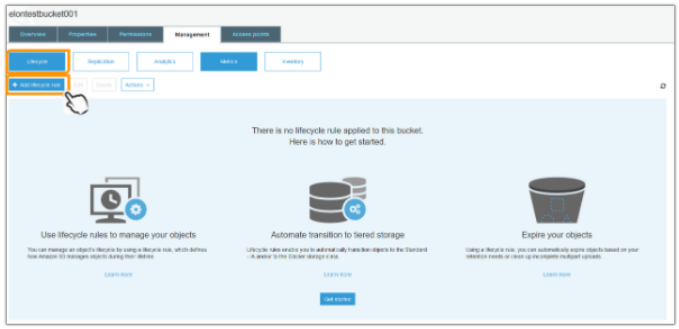
Bucket - Management



The followings are the options for bucket storage management tools:

- Lifecycle
- Replication
- Analytics
- Metrics
- Inventory

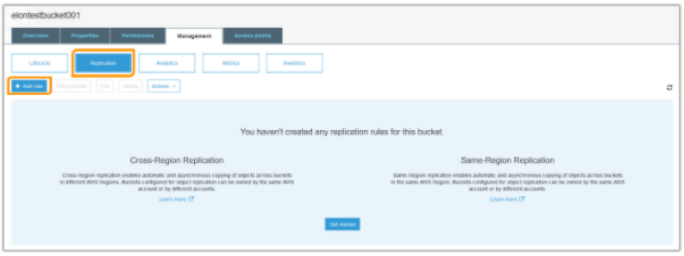
Management - Lifecycle



Creating a Lifecycle Policy defines actions you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time).

You can define a lifecycle policy for all objects or a subset of objects in the bucket by using a shared prefix (that is, objects that have names that begin with a common string).

Management - Replication



Replication is the automatic, asynchronous copying of objects across buckets in the same or different AWS Regions. Replication copies newly created objects and object updates from a source bucket to a destination bucket.

Replication requires versioning to be enabled on both the source and destination buckets.

The object replicas in the destination bucket are exact replicas of the objects in the source bucket.

- They have the same key names and the same metadata—for example, creation time, owner, user-defined metadata, version ID, access control list (ACL), and storage class.
- Optionally, you can explicitly specify a different storage class for object replicas.
- And regardless of who owns the source bucket or the source object, you can choose to change replica ownership to the AWS account that owns the destination bucket.

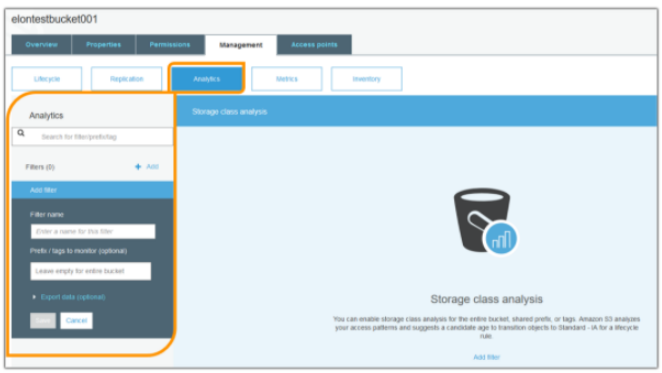
You use the Amazon S3 console to add replication rules to the source bucket.

- Replication rules define which source bucket objects to replicate and the destination bucket where the replicated objects are stored.
- You can create a rule to replicate all the objects in a bucket or a subset of objects with a specific key name prefix, one or more object tags, or both.
- A destination bucket can be in the same AWS account as the source bucket, or it can be in a different account.
- If the destination bucket is in a different account from the source bucket, you must add a bucket policy to the destination bucket to grant the owner of the source bucket account permission to replicate objects in the destination bucket.
- The Amazon S3 console builds this required bucket policy for you to copy and add to the destination bucket in the other account.

When you add a replication rule to a bucket, the rule is enabled by default, so it starts working as soon as you save it. Here are 2 example for adding replication rule on AWS.

- Adding a Replication Rule When the Destination Bucket Is in the Same AWS Account
- Adding a Replication Rule When the Destination Bucket Is in a Different AWS Account

Management - Analytics



By using the Amazon S3 analytics storage class analysis tool, you can analyze storage access patterns to help you decide when to transition the right data to the right storage class.

- Storage class analysis observes data access patterns to help you determine when to transition less frequently accessed STANDARD storage to the STANDARD_IA (IA, for infrequent access) storage class.
- Storage class analysis does not give recommendations for transitions to the ONEZONE_IA or GLACIER storage classes.

Management - Metrics

Amazon CloudWatch metrics for Amazon S3 can help you understand and improve the performance of applications that use Amazon S3. There are several ways that you can use CloudWatch with Amazon S3.

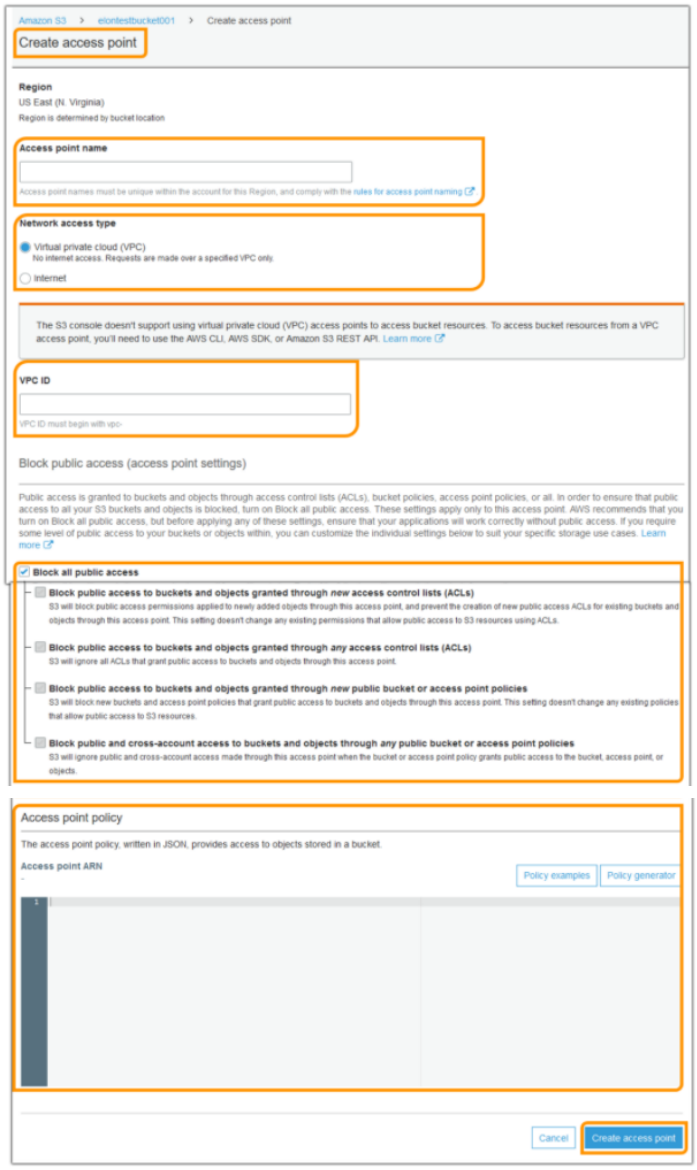
There are three types of **Amazon CloudWatch metrics** for Amazon S3:

- *Storage metrics* are reported once per day and are provided to all customers at no additional cost.
- *Replication metrics* are available 15 minutes after enabling a replication rule with S3 Replication Time Control (S3 RTC).
- *Request metrics* are available at 1-minute intervals after some latency to process, and the metrics are billed at the standard CloudWatch rate.

Management - Inventory

Amazon S3 inventory provides a flat-file list of your objects and metadata, which is a scheduled alternative to the Amazon S3 synchronous `List` API operation. Amazon S3 inventory provides comma-separated values (CSV) or Apache optimized row columnar (ORC) or Apache Parquet (Parquet) output files that list your objects and their corresponding metadata on a daily or weekly basis for an S3 bucket or for objects that share a prefix (objects that have names that begin with the same string).

Bucket - Access Points



You can use Amazon S3 access points to manage access to your S3 objects.

- Amazon S3 access points are named network endpoints that are attached to buckets that you can use to perform S3 object operations, such as uploading and retrieving objects.
- A bucket can have up to 1,000 access points attached, and each access point enforces distinct permissions and network controls to give you fine-grained control over access to your S3 objects.