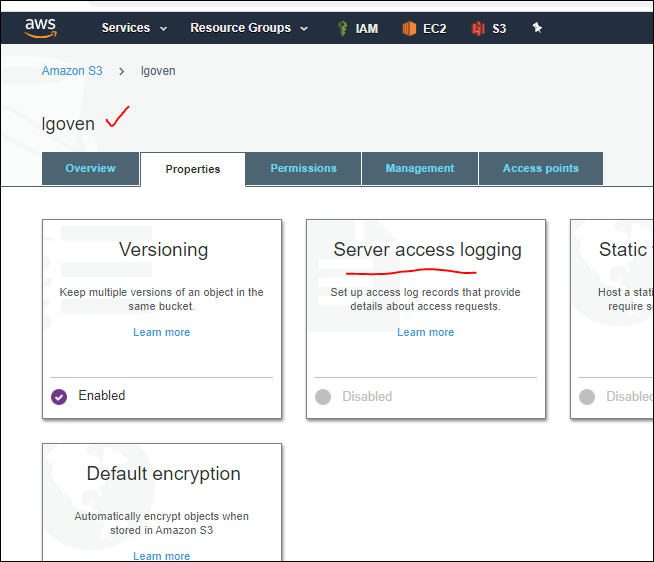
|  |
| --- |
| D: 16/06/2020 |
|  |  |
|  | Object lock : |
|  | --> Should be enabled when we create bucket. |
|  | --> Versioning must be enabled. |
|  |  |
|  | Governance mode can be disabled by AWS accounts that have specific IAM permissions. |
|  | Compliance mode cannot be disabled by any user, including the root account. |
|  |  |
|  |  |
|  | Transfer acceleration : If we want to upload / download data via edge locations. |
|  |  |
|  | Events : |
|  | --> SQS : Simple Queue service .. |
|  | --> Lambda : Serverless architecture.. |
|  | --> SNS : Simple Notification Service : |
|  | ==> Navigate to "SNS" Create a "TOPIC" and add subscribers. |
|  |  |
|  |  |
|  | Requester pays : Instead of bucket owner, who is requesting the data, he'll get charged for the request / data transfer. |
|  |  |
|  |  |
|  |  |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |
|  | https://join.slack.com/t/awswithavinash/shared\_invite/zt-f4xzhxmb-c22h9F4TMz3UQH9nLK~8Vw |
|  |  |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

We are dealing with some of the properties of S3 Bucket.

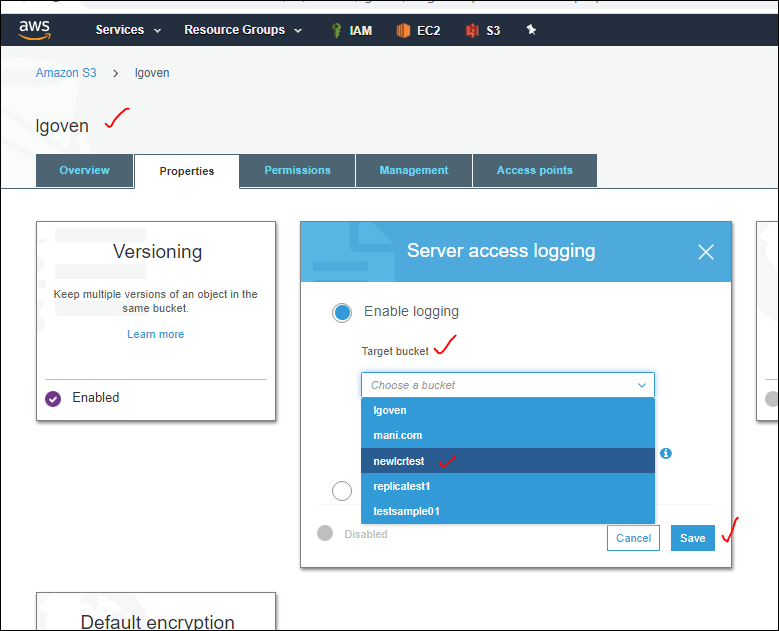
So in the Properties we have the “Server Access logging”, which is not much more we are using coz for each and every bucket, we can’t go and do the verify or understand the logs. So we have any option called [**“Cloud Trail”**] in Cloud trail we have an option called data events. Once we enable this , then what ever the buckets existing and which are created in future are also log will be enabled.

This feature we will give extensively in organization level.

If we need to know who is accessing and using the bucket ,we can use this feature.



By using this [Server access Logging] we can save the logs of that bucket to other bucket. Even we can save in same bucket i.e., source and target are same, but there will be lot of mess aswe are going to have lot of logs like arepitative cycle.



**“When your source bucket and target bucket are the same, additional logs are created for the logs that are written to the bucket. These extra logs can increase your storage billing and make it harder to find the logs that you're looking for.”** This is what happens when we select the same bucket as Target bucket.

We get log in plain text format.

-----------------------------------------------------------------------------

Advance Settings 🡪 Object locks.

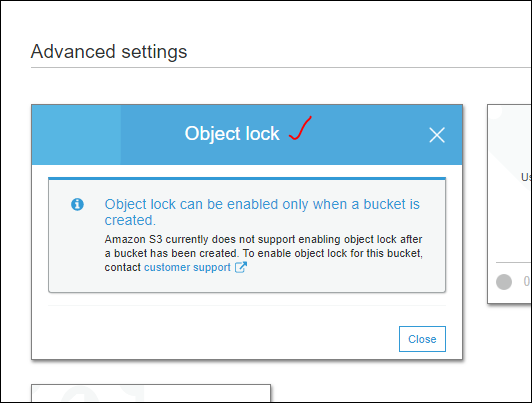
**Object locks:**

* **Object lock can be enabled only when a bucket is created.**

**Amazon S3 currently does not support enabling object lock after a bucket has been created. To enable object lock for this bucket, contact**[**customer support**](https://aws.amazon.com/contact-us) **.**

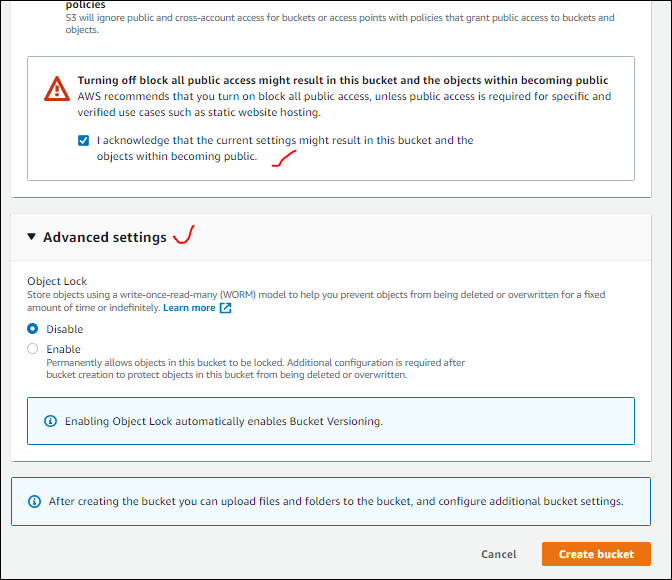
|  |
| --- |
| --> Should be enabled when we create bucket. |
| --> Versioning must be enabled. |
|  |
| Governance mode can be disabled by AWS accounts that have specific IAM permissions. |
| Compliance mode cannot be disabled by any user, including the root account. |

We have some data and that to we need to secure that data,thenw e can choos this Object lock. That data should be deleted by any user including IAM user also, sometimes even Root user also. So when we don’t any one to delete the data of the object then we have an Object Lock.

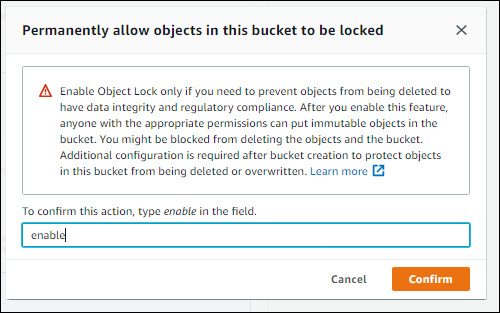


We can raise a ticket to enable the object lock if it is already created one.

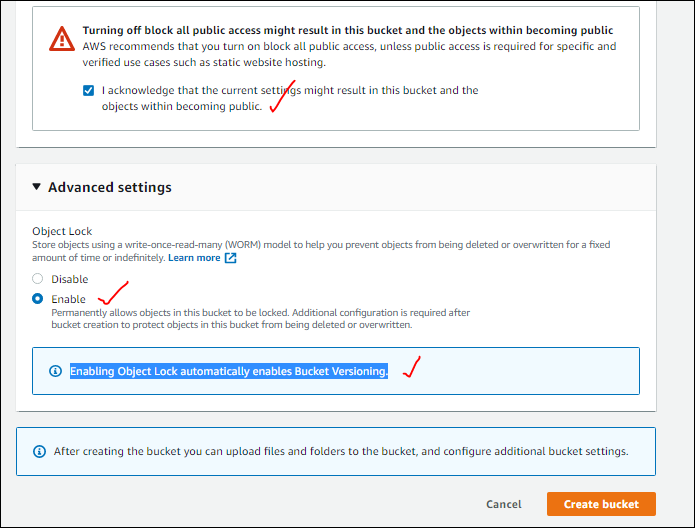
Now we are creating a new bucket. With naming as “[ moto123”].and provide the necessary options to it. We can unblock the public access.



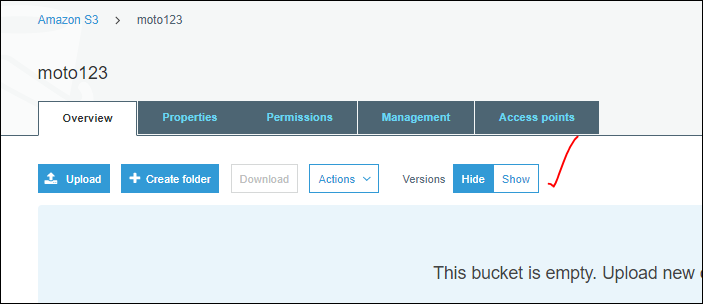
Select eh [ Enable ], and write **enable** to confirm it, then only confirm button will be enabled.



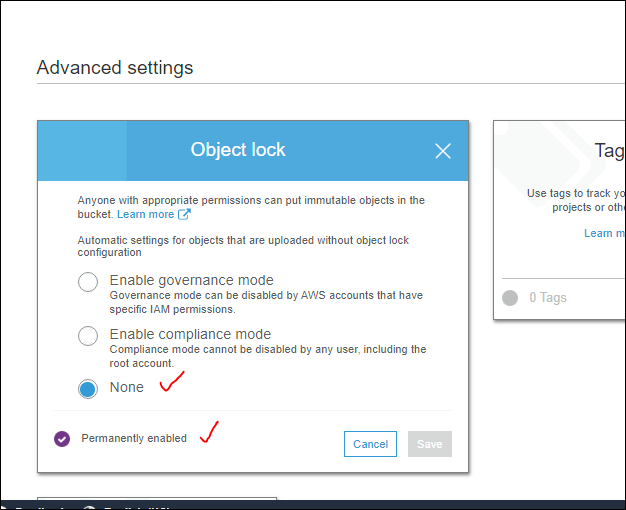
After we confirm we can see that automatically Versioning is enabled and now we can create bucket.



Now get into that bucket [moto123] which is created, we can see that versioning is enabled automatically, and bucket is empty.



We have enabled Objet lock while creating the bucket, but by default it is set to None.



Actually we have two types of mode :

1. Enable governance mode: **Governance mode can be disabled by AWS accounts that have specific IAM permissions.**
2. Enable compliance mode: **Compliance mode cannot be disabled by any user, including the root account.**

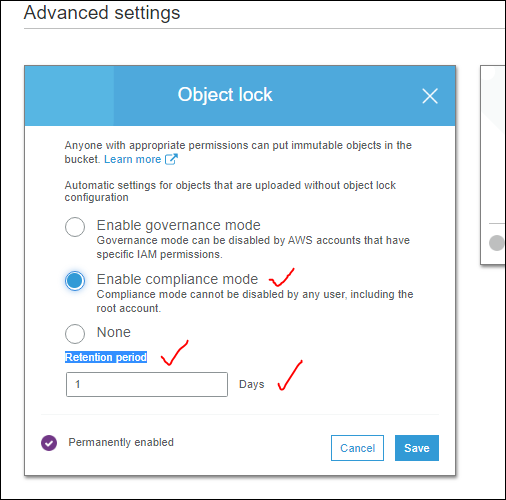
So for the defined days [**Retention period**] we can’t delete it.

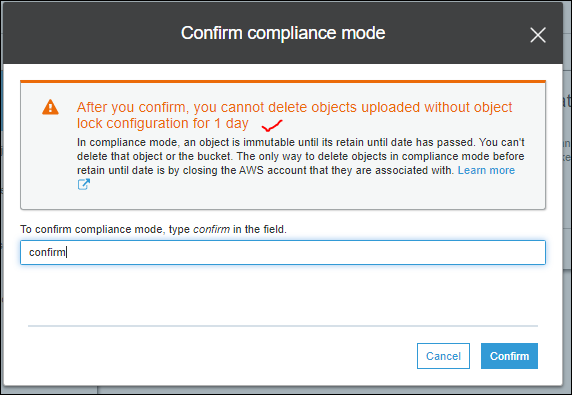
**Governance mode**, the object will be ImMutant.

While defining the [Retention period] we need to be cautious coz, if we give 9999 days until that days we cant delete it or we need to contact AWS Support team.

If we need to disable object lock we need to wait until the applied Retention period once it is finished,

Now for practice purpose we are setting to 1 day and click on save, it will open the Confirm compliance mode. Make it confirm.



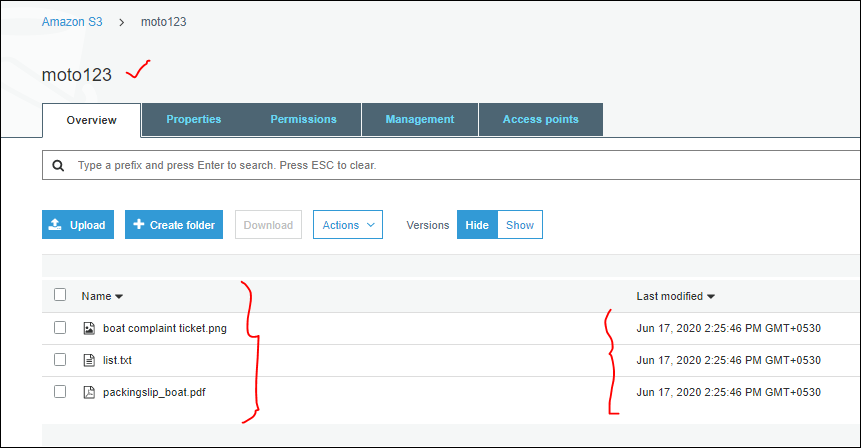


After you confirm, you cannot delete objects uploaded without object lock configuration for 1 day

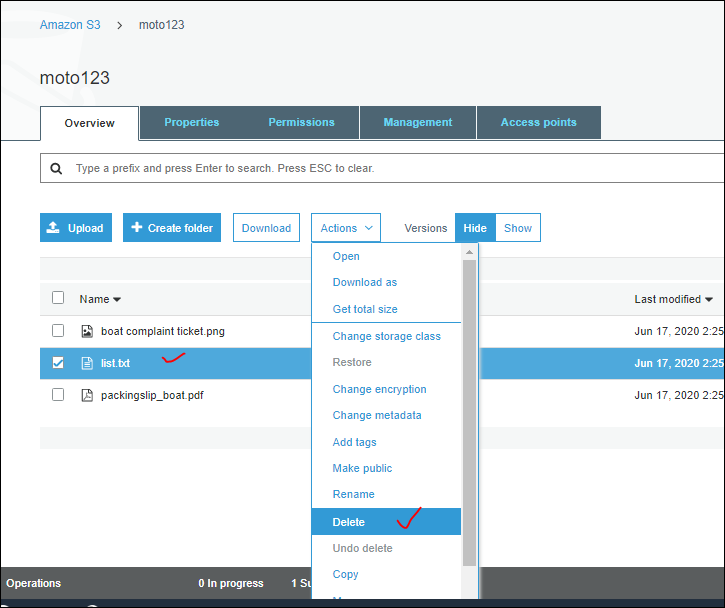
In compliance mode, an object is immutable until its retain until date has passed. You can't delete that object or the bucket. The only way to delete objects in compliance mode before retain until date is by closing the AWS account that they are associated with. [Learn more](https://docs.aws.amazon.com/console/s3/object-lock)

Object lock was successfully updated for this bucket.

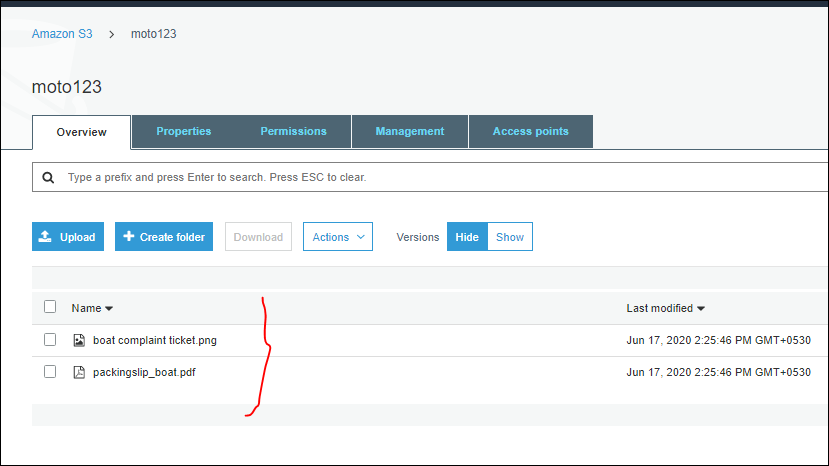
Now we are going to add some data [objects] to the created bucket [moto123] with Object lock property.



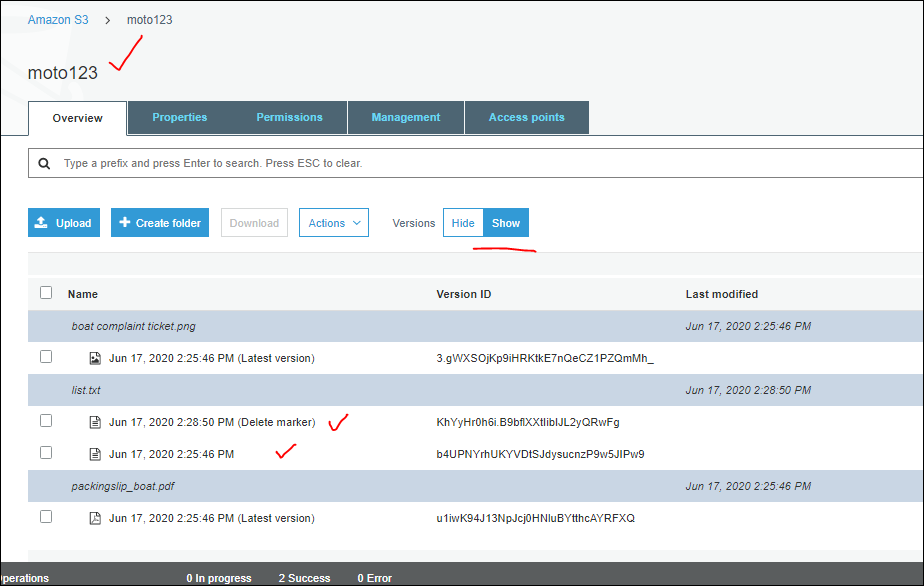
Now try to delete the added objects in the moto123 bucket, it will delete in “version –Hide” and same can be created as delete marker in version show.



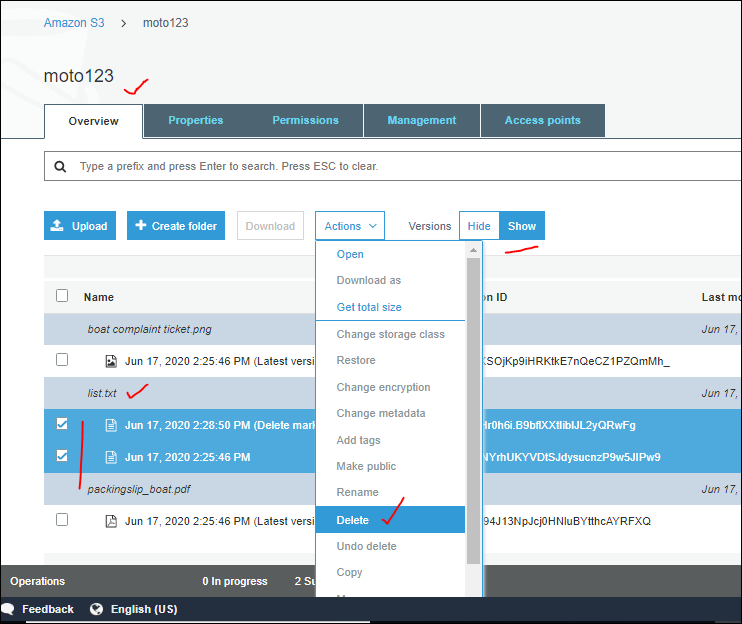
It got deleted in Hide



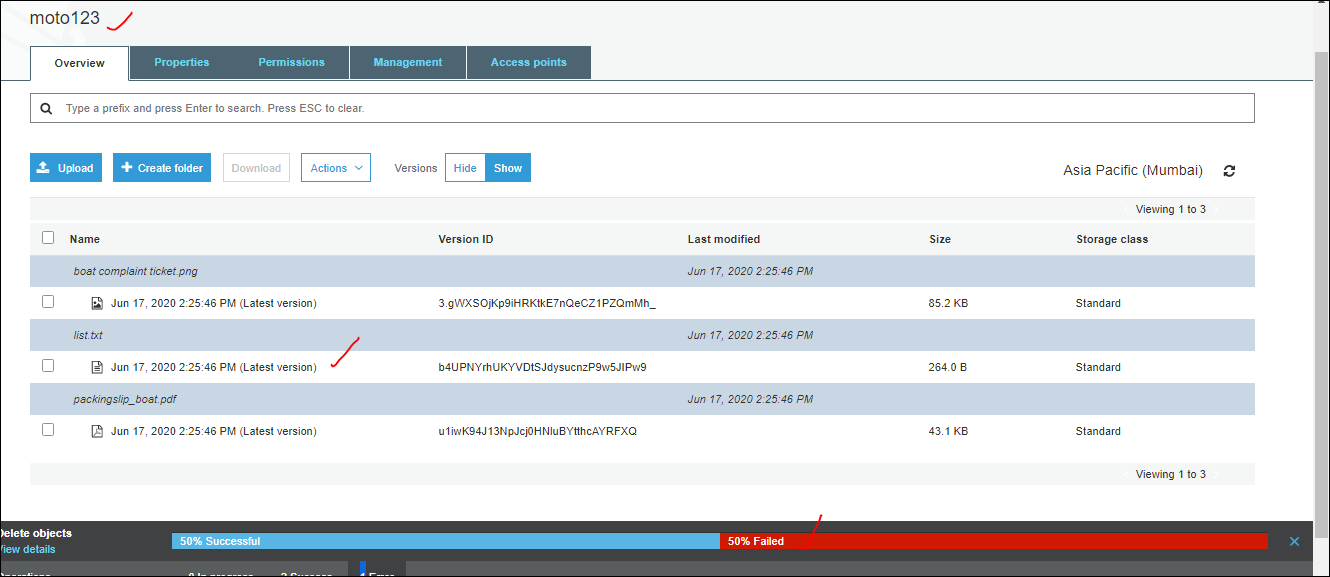
We can find the delete marker for the deleted object in show as shown below



Now we wil try to delete the both files including the delete marker file also,



But it wont delete the latest file as shown below for period of Retention which we have given initially at enabling the object lock feature for the bucket.



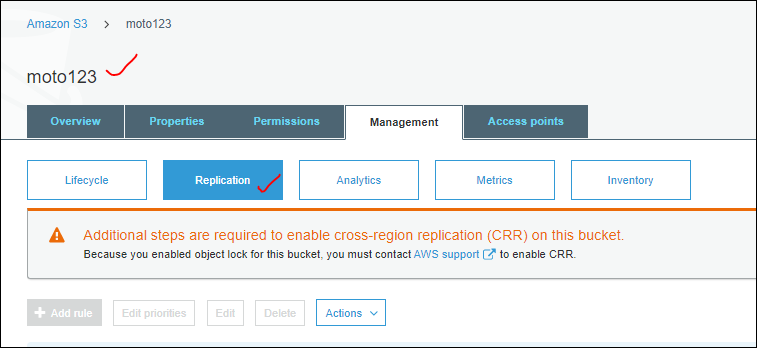
Even if we try for the latest version file also we cant delete it until the Retention period should complete.

Main reason to enable the object lock is we can delete the object even at version Show instantly, until that retention period has to complete then only we can delete it, This is like a log.

* For Object Lock enabled Bucket -- we cant set the Replication, but we can set it but using addition steps.this is the statement we get when wee try to do it.

Additional steps are required to enable cross-region replication (CRR) on this bucket.

Because you enabled object lock for this bucket, you must contact [AWS support](https://aws.amazon.com/contact-us) to enable CRR.

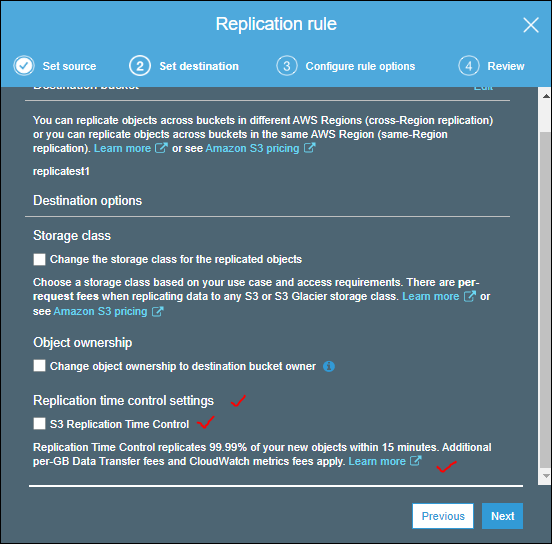


* Is there any lag when wee try to perform SRR or CRR ?

There is a lag , that first we need to see the size of the object which we are going to replicate.

That to only 15 minutes [“Replication Time Control replicates 99.99% of your new objects within 15 minutes. Additional per-GB Data Transfer fees and CloudWatch metrics fees apply. [Learn more](https://docs.aws.amazon.com/AmazonS3/latest/dev/replication-time-control.html) “]

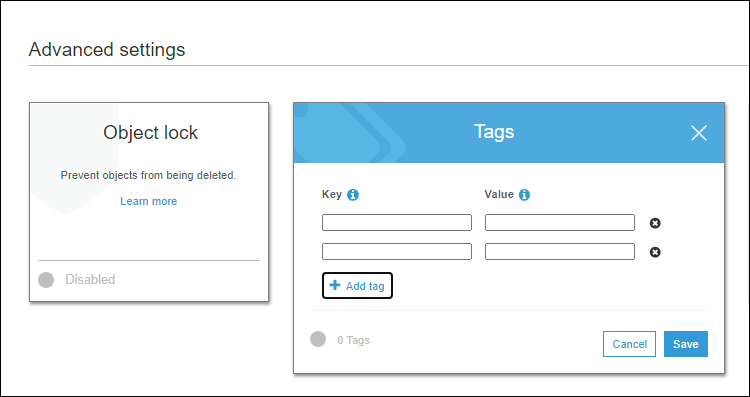
So there might ne charges apply as mentioned as shown below.

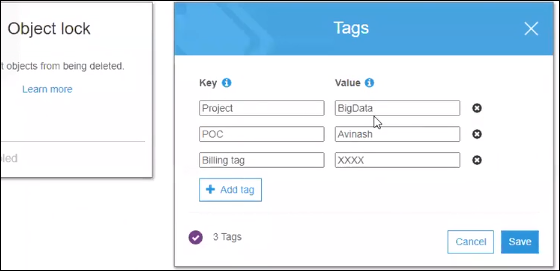


-----------------------------------------------------------------------------------------------------------------------------

**S3 Bucket – Properties – Tags:**

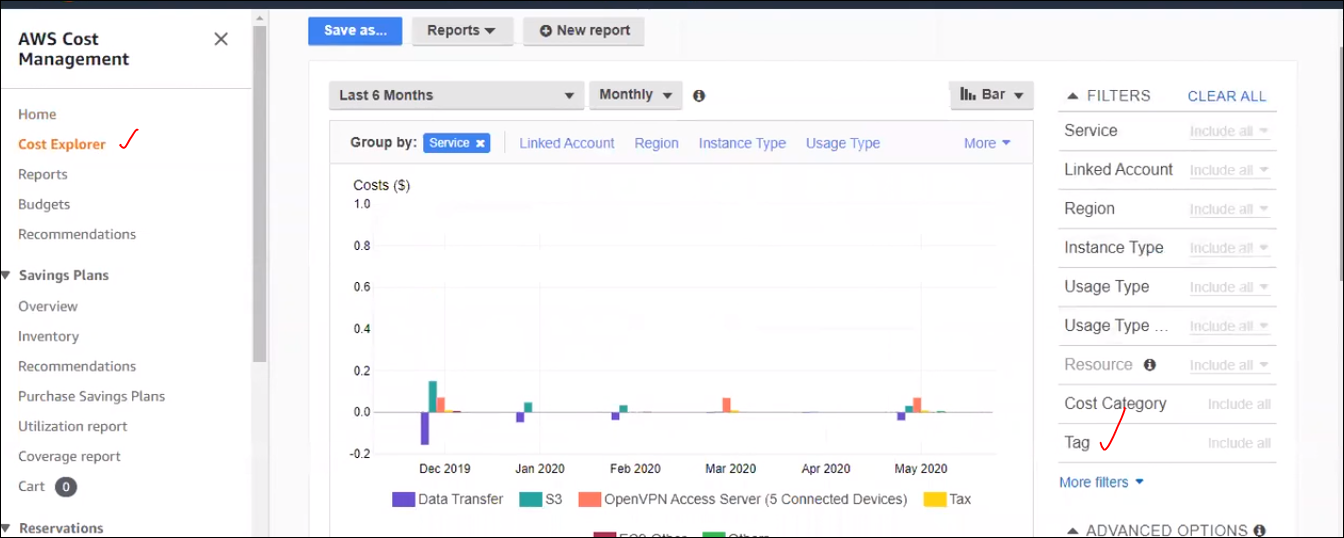
* Tags are very small option but very effective feature. We don’t really create any resources without Tags in Enterprise level.
* For ex:- we have 100 of buckets, out this 100 we need to know which bucket is created for which project,who is point of contact (POC), owner, requested, and how much that bucket is costing.
* BY adding the tags we have an option and all like cost center we can filter based on this tags, how much money we are spending with detailed info.

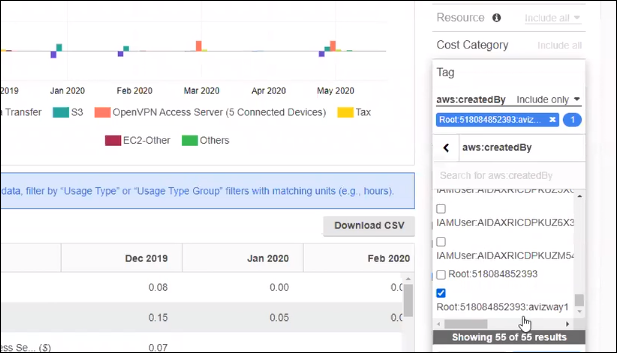






Here we can see the tags act as a filters, for the billing.





* What is the time it required to reflect the tag in Cost management?

If we need to see what all the resources will have this tags, for that we have [“ Resources Groups”].by creating a resource group we can filter all the rsources by using this Tag mechanism.

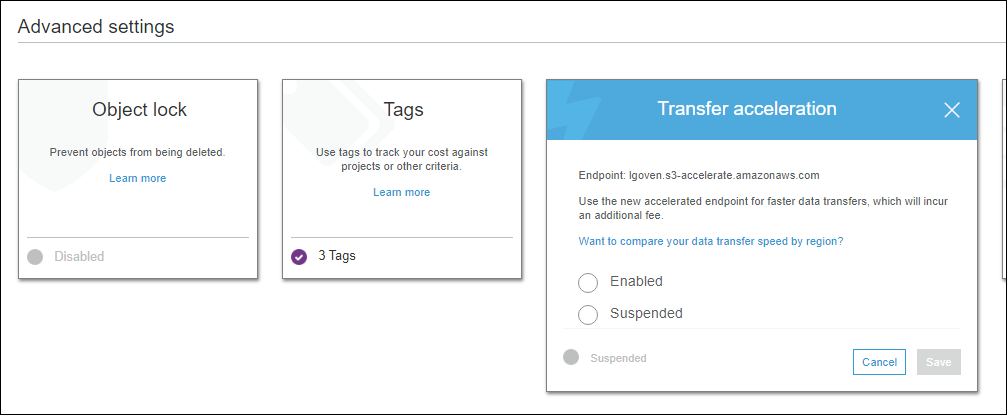
* Suppose a resource is created with tag, we can get the info by using third party tools tht can be discussed in systems manager..
* We will go bucket level tagging, coz each bucket may have 100 of files, it is difficult to navigate to each and every file property to assign this tags.
* Does the created tag reflects immediately in the Cost management.?
* How can we track who has edited , created.. all such functionalities in S3?

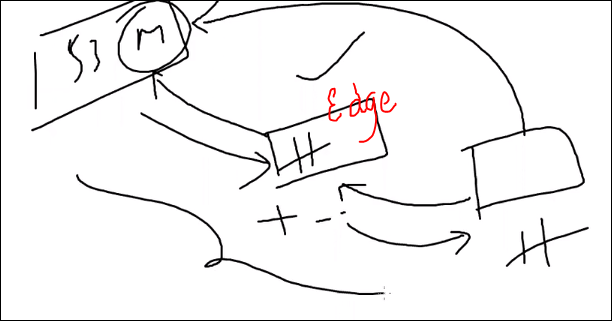
------------------------------------------------------------------------------------------------------------------------------

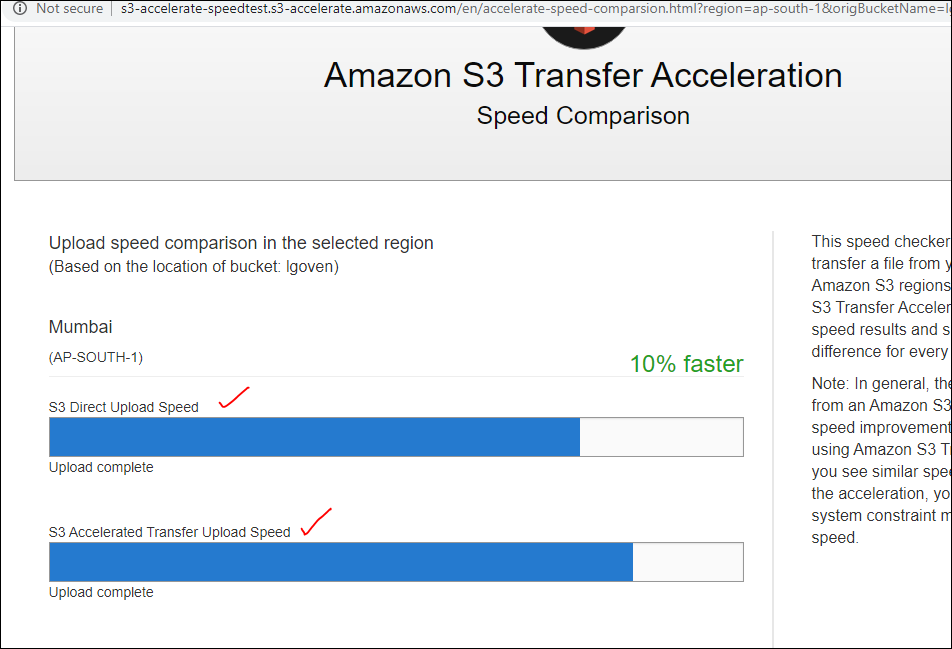
**S3 bucket – properties-- Transfer acceleration :**

If we want to upload / download data via edge locations.

If we directly uploading the data without enabling this feature,for ex: we are uploading data fro Hyd to Mumbai reagion, if it has the Edge location then data transfer will happen between these region with a connector edge. Again we cant garrenty for positive results . this is required as the geographicall distance increased between data upload and download we need this Edge service, so we will test this before enabling this feature in Bucket properties , Amazon will maintain dedicated bandwith between the edge locations and the Source regions, Amazon has 216 edge locations, 210 + H locations, for this basically it cost us,if we enable this feature also nothing more will cost wit will be , even if we enable also it will upload and download data wherever near edge location is available. But we can test the speed via direct upload what is the speed, and via edge what is the speed. By using this link we can monitor this [ “[Want to compare your data transfer speed by region?](https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html?region=ap-south-1&origBucketName=lgoven" \t "_blank) “ ] as shown in fig.







Same can be seen for all regions based on the positive results we can upload or download the data.S

If we enable the Transfer Accelaration we get 10% faster in upload and download the data from the regions.

* So edge is also a data center but not as big as avaiablity source.

-----------------------------------------------------------------------------------------------------------------------------

|  |
| --- |
| Events : |
| --> SQS : Simple Queue service .. |
| --> Lambda : Serverless architecture.. |
| --> SNS : Simple Notification Service : |
| ==> Navigate to "SNS" Create a "TOPIC" and add subscribers. |

**S3 bucket – Properties – Events:**

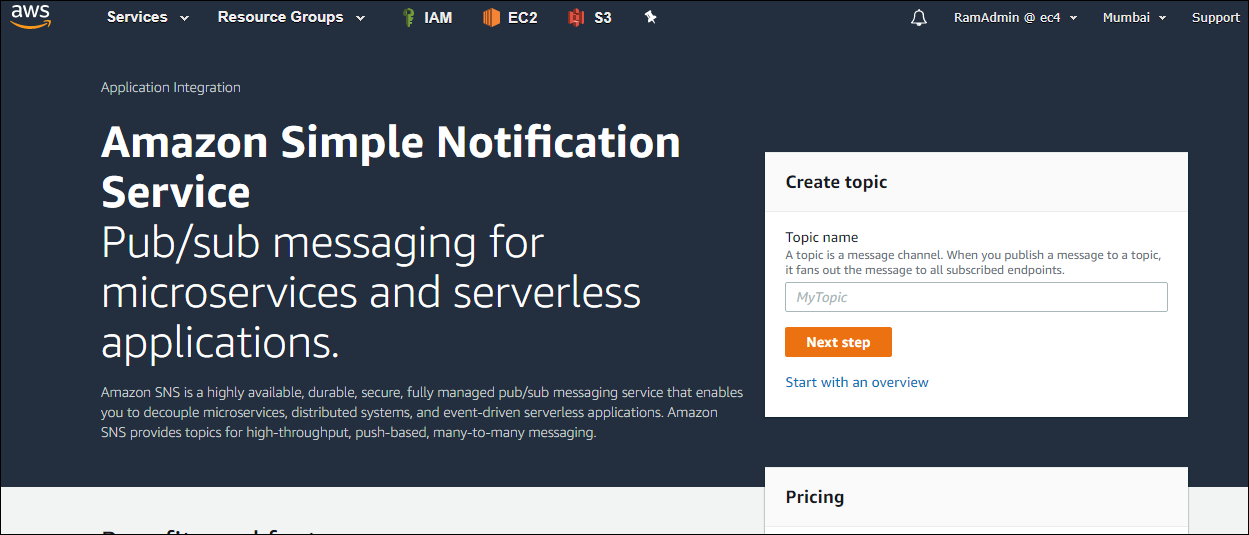
Event supports has three options

1. SQS : Simple Queue Service [ when something is happing on S3 bucket, we can trigger a Queue, and we can run a job which is configured in EC2 instance.]
2. Lambda : Serverless architecture, we can automatically tigger some jobs that are configured in lambda] , these featured are discussed later
3. SNS : Simple Notification Service.

Now we are going to discuss events based on the SNS. [ we can create a topic in SNS, we can add subscribers, to the topic, then when something happens , when any event occurred on this bucket, we can get an email to all subscribers users. Let us see how it works.

Who ever are subscribed to this service with email , those users ahs to confirm once they get th mail.

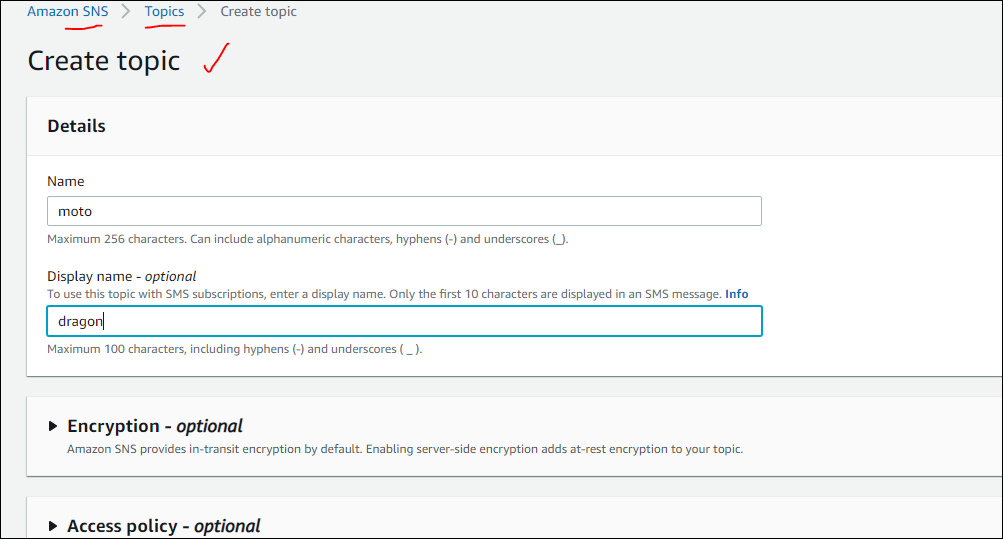
Now naviage to **AWS management Console – Application Integration – simple Notification Service.**



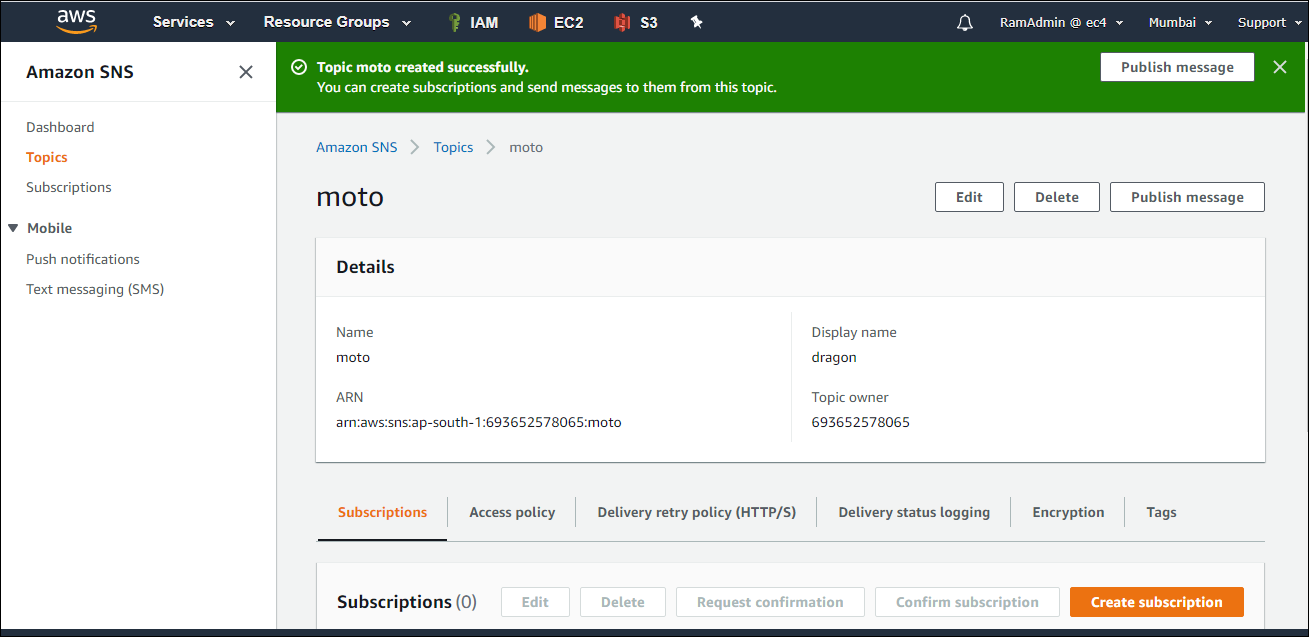
If S3 doesn’t have valid permissions on the SNS , then we are going to get an error when we tried to apply the event as sown below.

Scenario 1: without permission for S3 to SNS ,

Create a topic and try to use that topic in S3 bucket event.

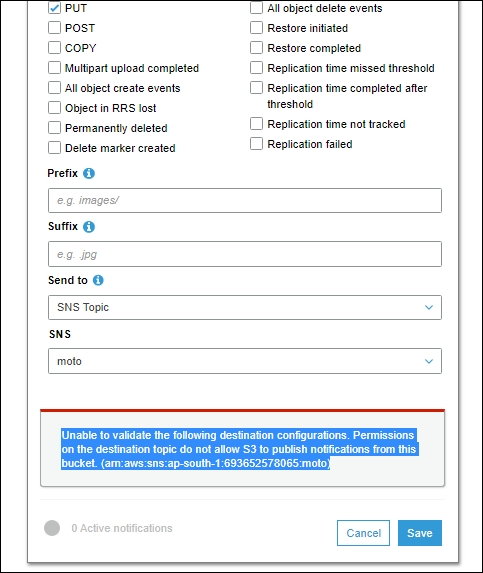


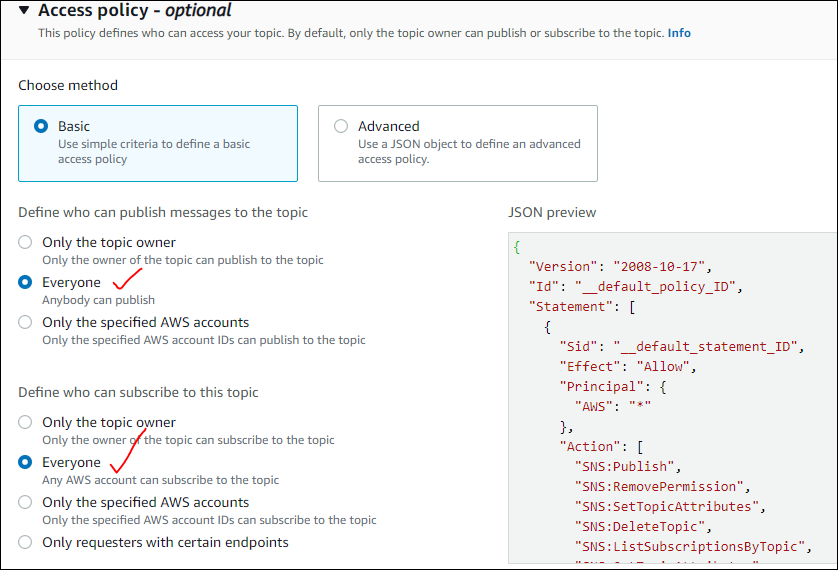
Wehave separate seesion on the SNS, but time being we are just crating a topic and tries to use that in S3 bucket event .



This is the error we face if we wont have valid permissions on SNS service by S3 bucket.

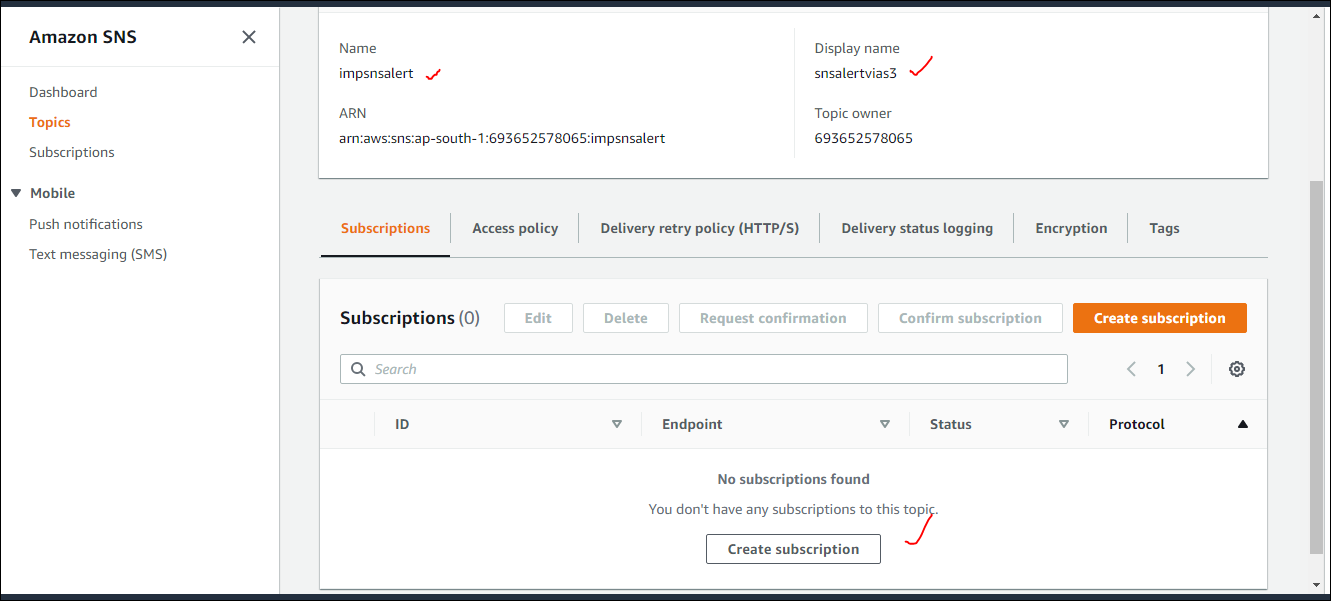
Unable to validate the following destination configurations. Permissions on the destination topic do not allow S3 to publish notifications from this bucket. (arn:aws:sns:ap-south-1:693652578065:moto)



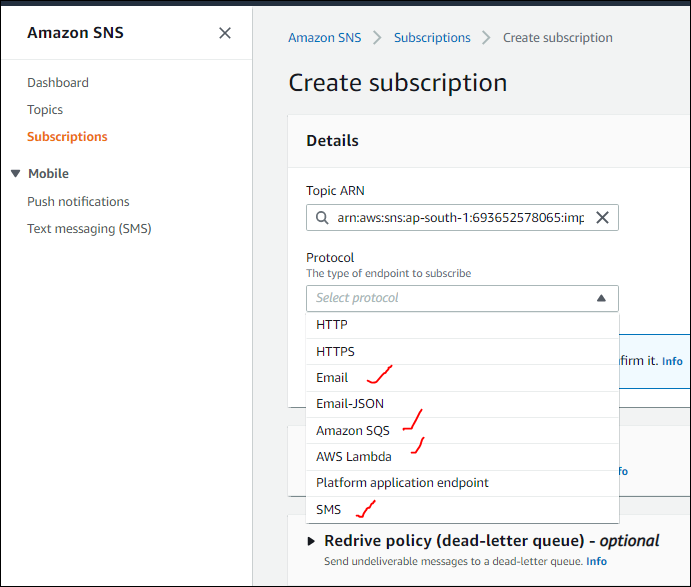
While creating the SNS Topic, we need to provide the Access Policy at movement weare giving to every one as shown I below image.S  


Now wehave given permiisons to S3 on SNS to sent the mails via using this SNS service.

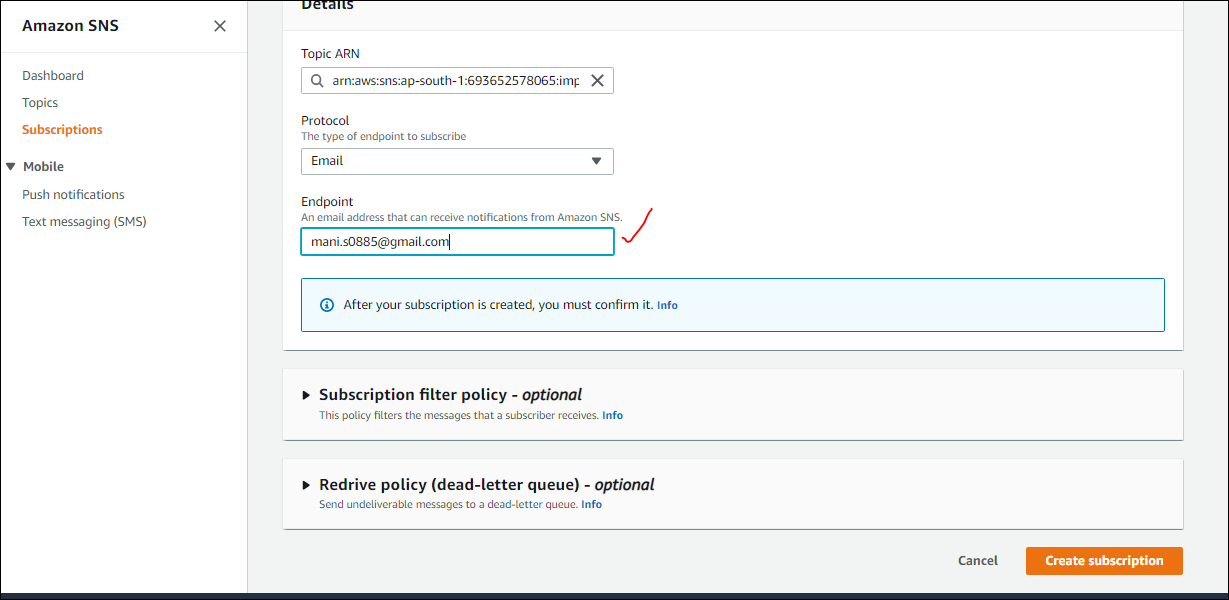
Now add some subscribers to the created topic.



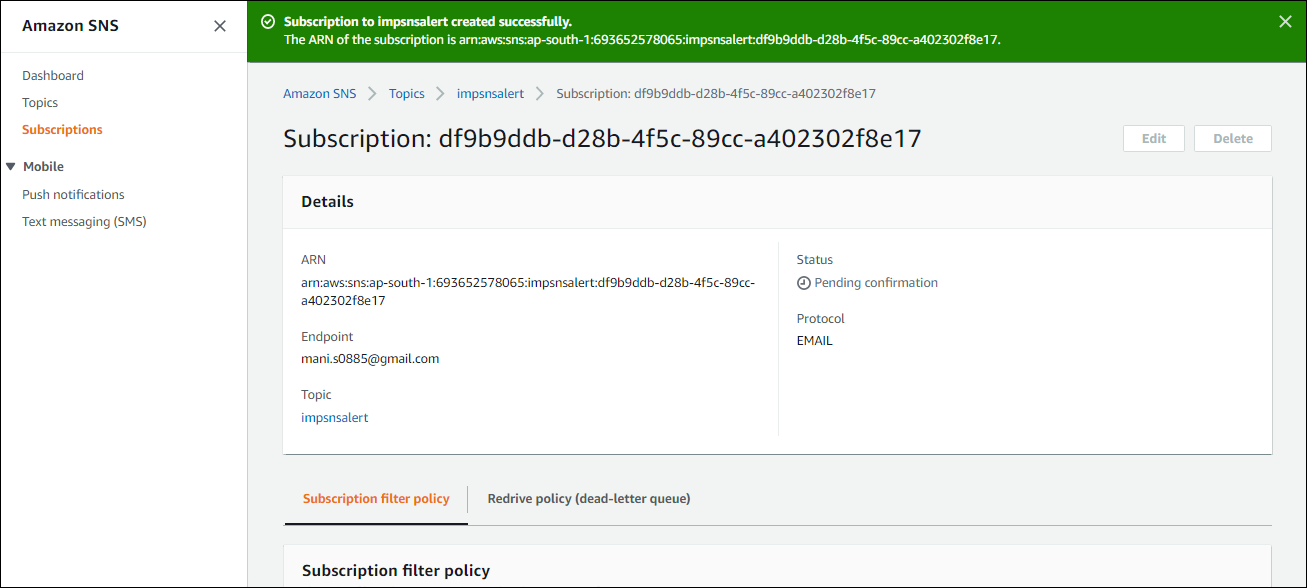
We can select the protocol through which w can give the alert



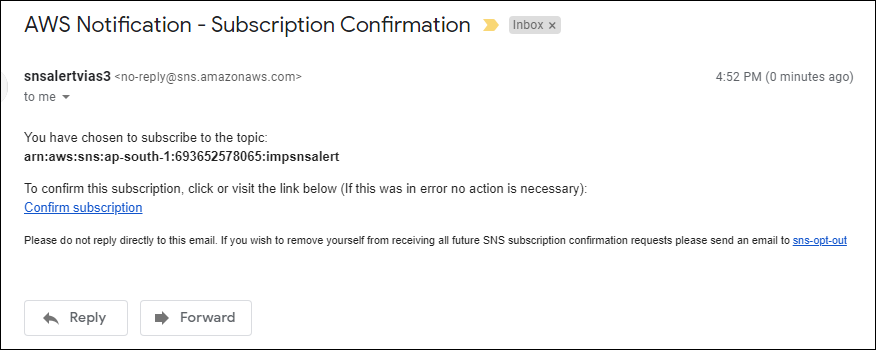
We can give SMS also but that is going to cost us.



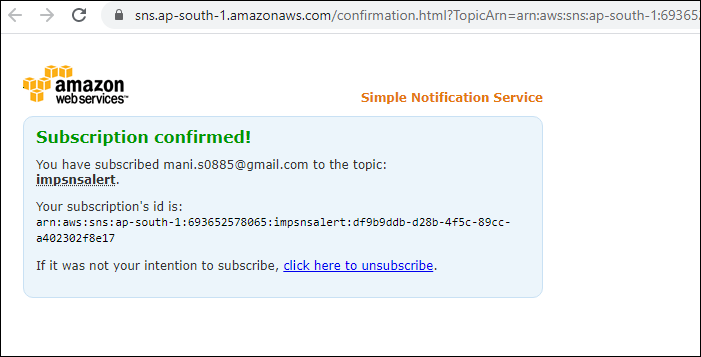
Now we have provided the subscribers to the topic in SNS.

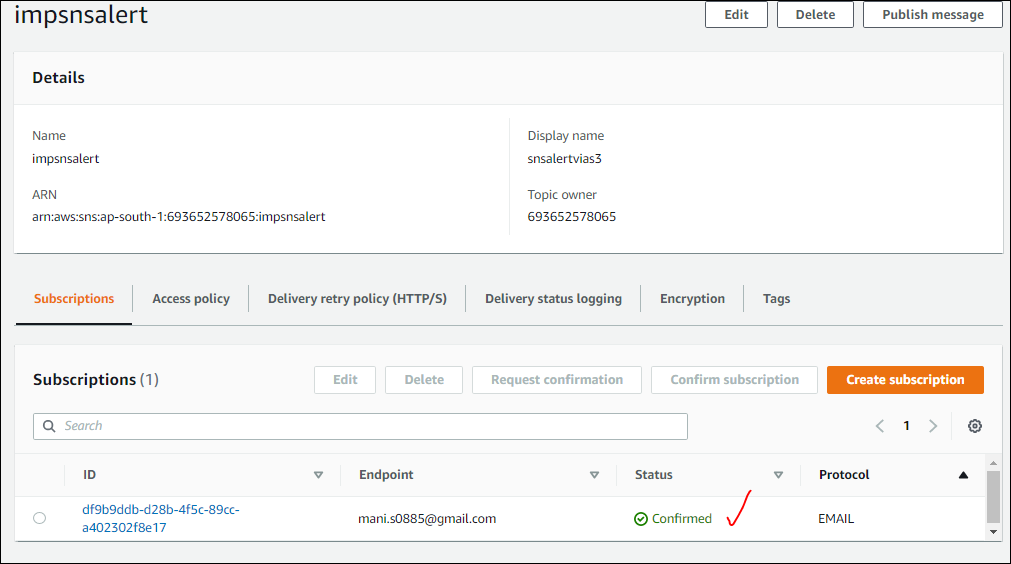


After creation we will get an email , which we need to confirm the subscription. Until that time status of the subscription will be in pending , once we confirm then only we can see the Confirmed status in topic

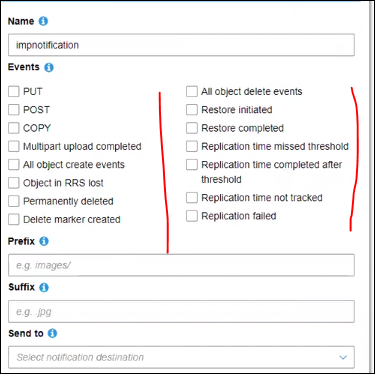


Once confirmed

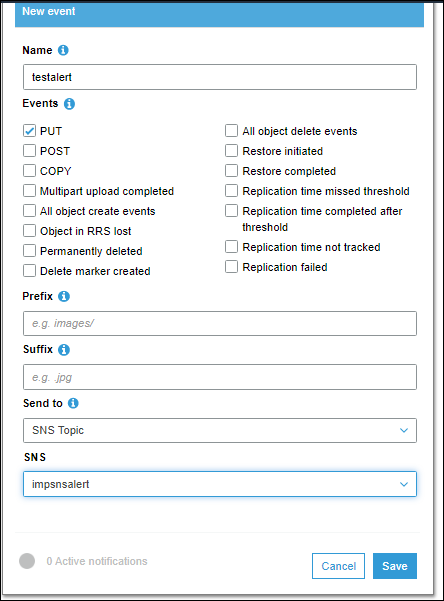




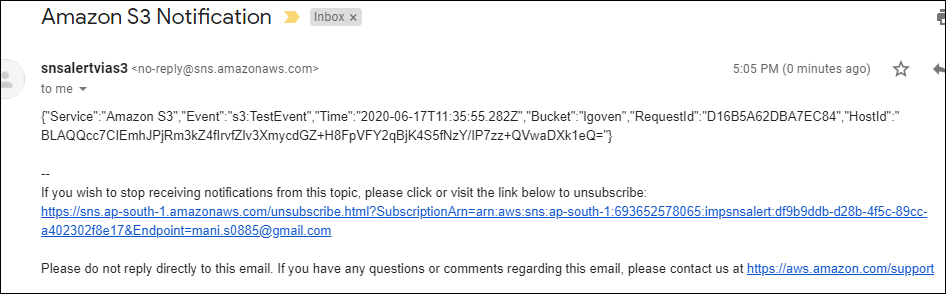
Now do the same process to add an even to the S3 bucket as we created the SNS , while adding the Events we cant customize them, we need to select the Events which are available in the list .to do cuatomize we need to use third party tools .



Prefix and suffix will actually add this event to the them if we have folder as test then this even will apply , even if we have folder test1 also this will apply. As if we add prefix as “test”.



So afer adding the event we can get an email as a testing mail.



Basically the notifications are in Json format, if we need to customize it is not possible in S3, but we have **Cloud watch** there we can customize it.

Here we opted for PUT event, so when we upload any fiel to S3 bucket, we will get a notification.

With details.



* If we create multiple SNS events we can get overlap error.but it is possible tocreate multiple , but make sure to maintain valid SNS topics.

-----------------------------------------------------------------------------------------------------------------------------

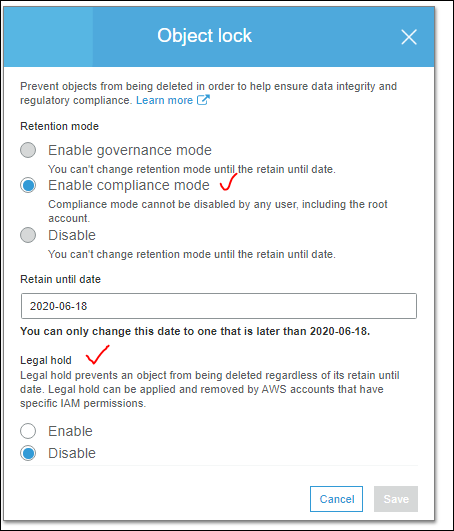
**S3 Bucket – properties -- Requester pays :**

Instead of bucket owner, who is requesting the data, he'll get charged for the request / data transfer.

For eg; we are trying to access the data from the the bucket, by endof the month,we are going to get the bill, for all those request.

🡪 if we apply object lock for a bucket, and try to delete it cant be deleted until its Retention period.

And if we enable Legal hold it prevents to delete an object of its retain until date.



Let us try to enable the Legal hold. This is enabled in Object level .

Legal hold was successfully enabled for this object.

We have created new bucket objlocktest11” and applied “legal hold” for an object “ sample1.txt”.

We will wait for 1 day even hard delete will happen or not.