Question: I am a java/aws developer wanted to know what part of this is relevant for me.

Ans: we need a storeage, for any application,jave/.net, in that case we use S3, and we are going to access data from S3, for ex; Youtube, where we are going to generate the thumbnails, videos, so for that we need storage we are using S3.

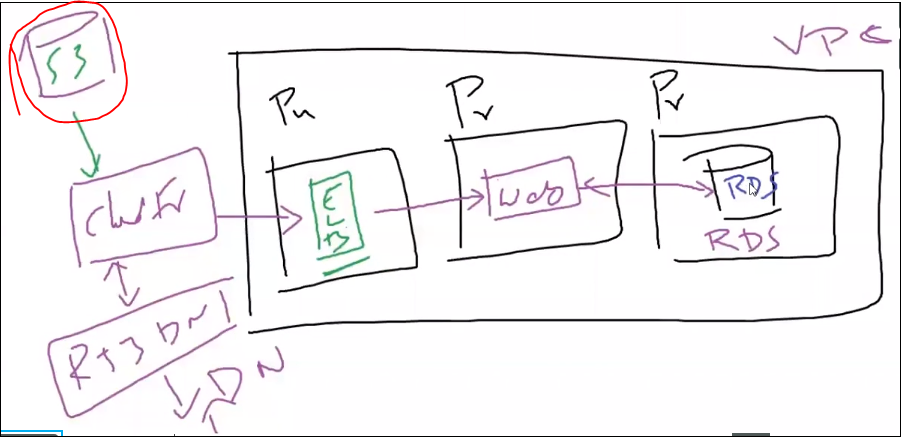
Deployment is hapned in EC2 instance,it hapns in servers.on top of OS by using run time environment, like middle ware applications, apche tom cat, enginex,

We can use S3 in another manner also, developer will write all the code and put it in S3 instead of git, and push it to a server.or we can prepare a build and its output like jar, war file we can put in bucket and push it into EC2 instance.

In all these cases we are no were installing or running an application in S3 platform. That why it is specifically mentioned as object based storage.

Question: lot of programs like dynamo DB’s, making like managing the applications, so which just talk to AWS nothing else what kind of components are required to development ?

We have separate session on Data base.



Now we are just started with S3, we need to go thru all the modules, how we are intergrating all will be covered in coming sessions.

Basically the services are same, focus area are different for developer/ architect, yes, what all services are covered are same for all certifications.

how we are going to cover the services , how we are using services in real time, how we are going to provision and how we are going to use.

Developer: how we are accessing the services.

Solution Architect : what is the solution, how we are going to opt what solution we are going to suggest for the client requirement.

Sys ops Administrator: when ever any issue happened, operational things will come under it. But S3, IAM, EC2 are all common.

17-06-20:

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

ACL : Access COntrol List..

List Object :

Write Object :

BP : JSON format.. We can use policy generator..

IAMUser 1 : S3FullAccess ==> Bucket (User2, Readonly on objects/ restrict put operation)

IAM User 2 : S3 Full Access

Policy Generator:

Effect : DENY

--> Allow

--> Deny

Principle : IAM USer ARN Name / IAM group ARN Name.. arn:aws:iam::518084852393:user/user2

Action : What do you want to allow/deny.. : PUT OBJECT

Resources : On what bucket : arn:aws:s3:::user1.bucket.asd

Object Level : arn:aws:s3:::user1.bucket.asd/\*

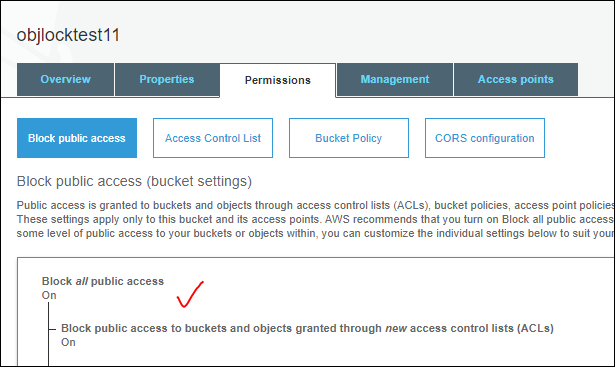
Bucket Level : arn:aws:s3:::user1.bucket.asd

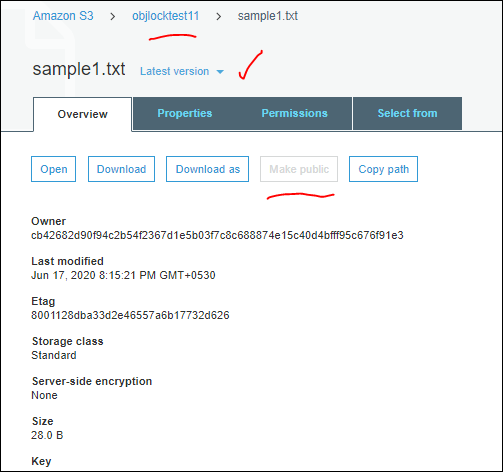
-----------------------------------------------------------------------------------------------------------------

Who can manage the object lock after the Retention period, is decided by the “Governance mode” / “Compliance Mode”.

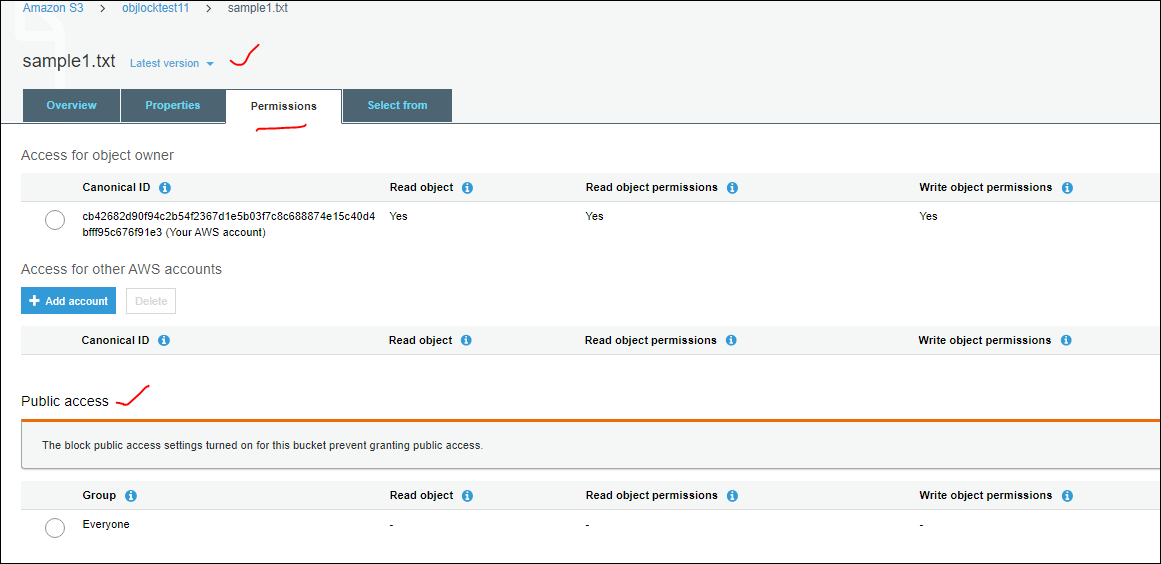
**S3 Bucket – Permissions – Block public access:**

**In “Block public access”**  if we “block all public access” is ON. That means all the permissions are blocked for objects if we check in that object properties.





Even if we go to the permissions of the object, if we scroll down we can see the **Public access,**

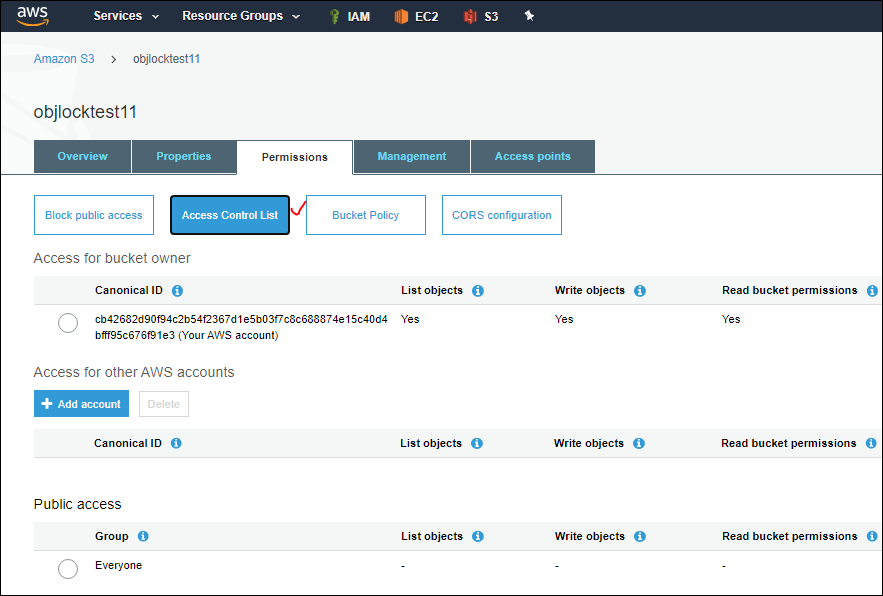


Even if we try to enable the Public access at object level by using the “Public access” it will denied, coz it is blocked at bucket level only , so we can make it public at cost.

So if we need to share data to public we can make at Bucket level by turn off the **Block all public access,** after here we done at access point but for each object which we need to make it public for that we need to provide “Make public” then only we can share it to public.

**S3 Bucket – Permissions –Access Control List:**

**🡪 IN block public access is related to couple of Access Control List and some are with Public Policy.**

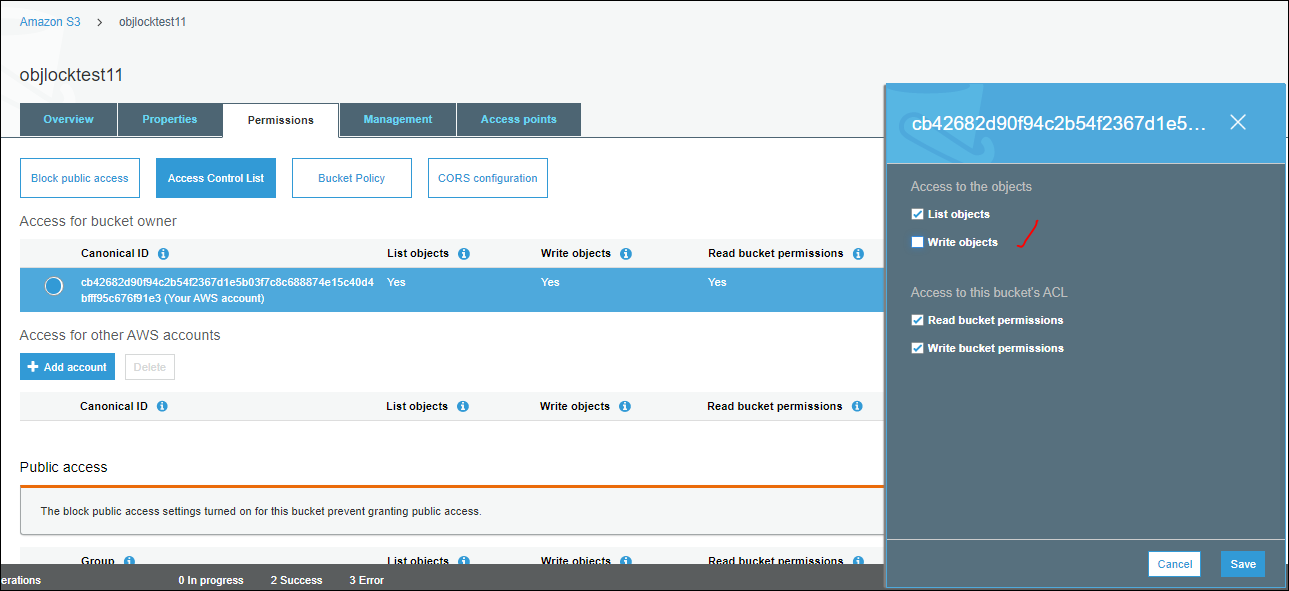


If we observe in the above image, we can see the Canonical ID, List object write objectsm Read bucket permissions..

It is not recommended to modify our own settings, suppose if we uncheck the write objects to try to save it will shown a warning message that “ [This action will remove your AWS account root user's access to this bucket

After you confirm this setting, the root user for this account will no longer have access to the following:

* Write objects ] “ so who ever have the permissions IAM, root user can’t write upload any object into this bucket.if we change the permissions.

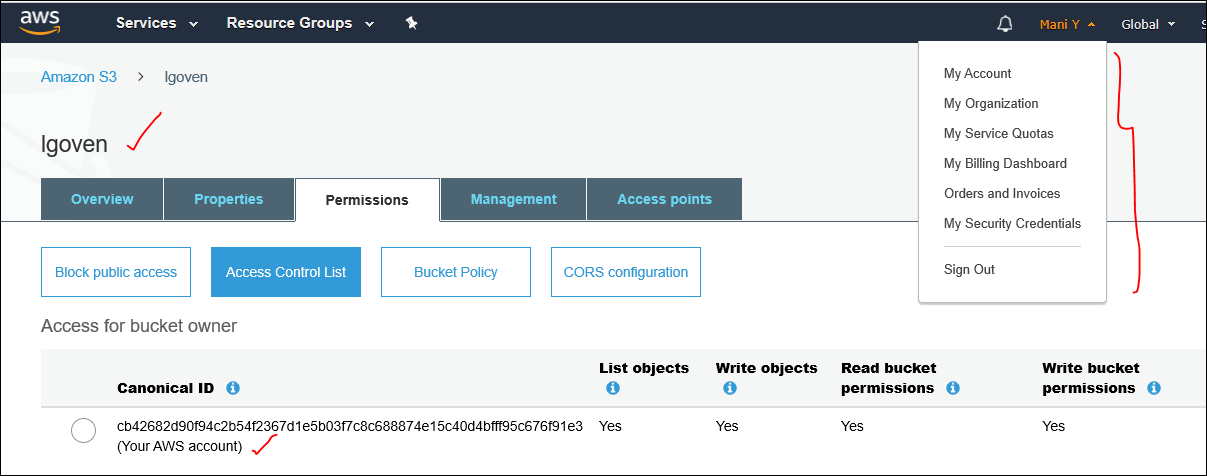


We have four kind of access permissions in Access :

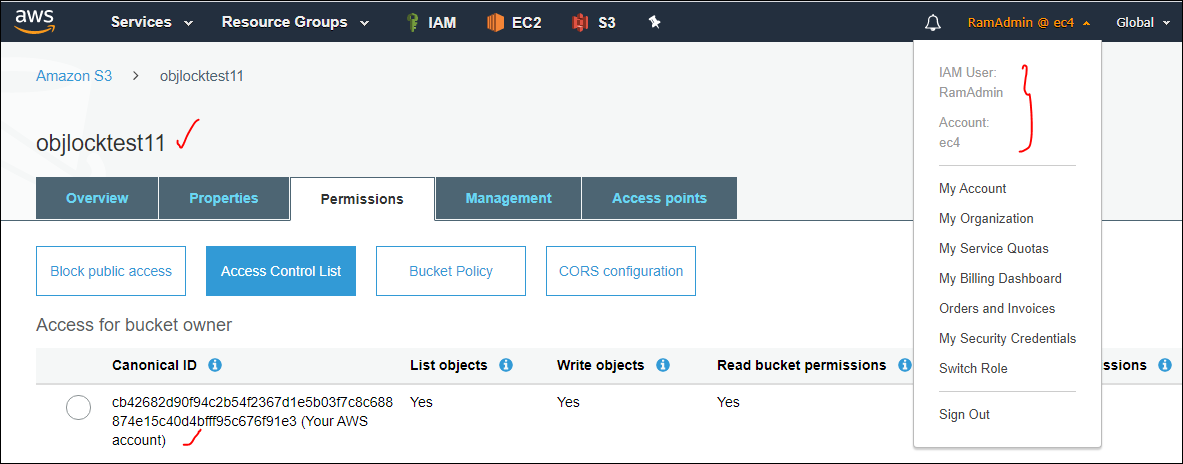
1. List object : will list all the objects present in the S3 bucket. What ever bucket if we access in tha bucket it will list all the objects in “Overview” tab.
2. Write object: who can upload/ overwrite/ delete /modify data of the objects into the buckets.
3. Read bucket permissions: if one user can modify his permissions or other permission at bucket level if the user is able to see.
4. Write bucket permissions: if the user can do any changes he has write bucket permissions.

For every account there we are going to have a Canonical id for the particular AWS Account. Suppose if we have a root user – we have 2-3 IAM users all will have the same Canonical id for all buckets. As shown below.

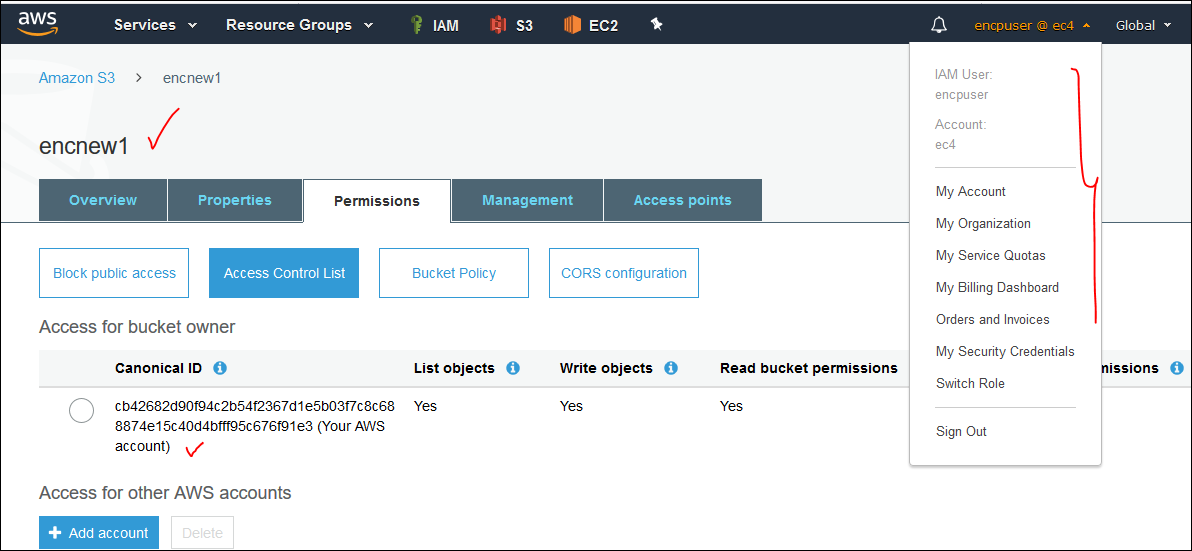
Root user:



IAM user 1 [ ramadmin] from same root user [maniy]:



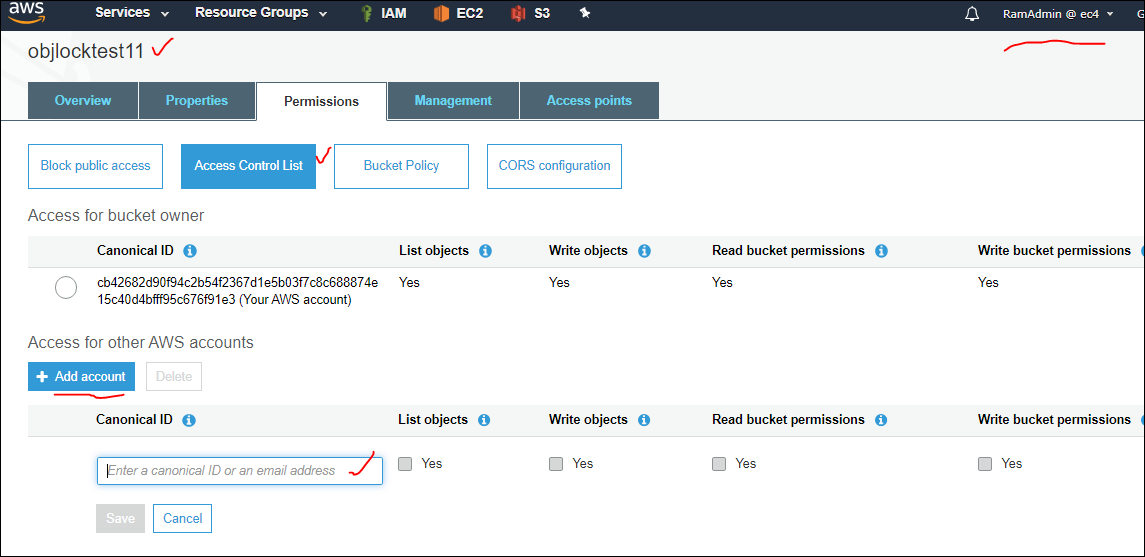
IAM user 2 [ encpuser ] from same root user [maniy]:



Canonical id is mainly designed for S3 platform only. For example another AWS account user has to share some data with us, in that case where is that uniqueness is coming to account, so that uniqueness is coming to S3 platform is from canonical ID.

🡪 So if we share the canonical id to access for other AWS accounts

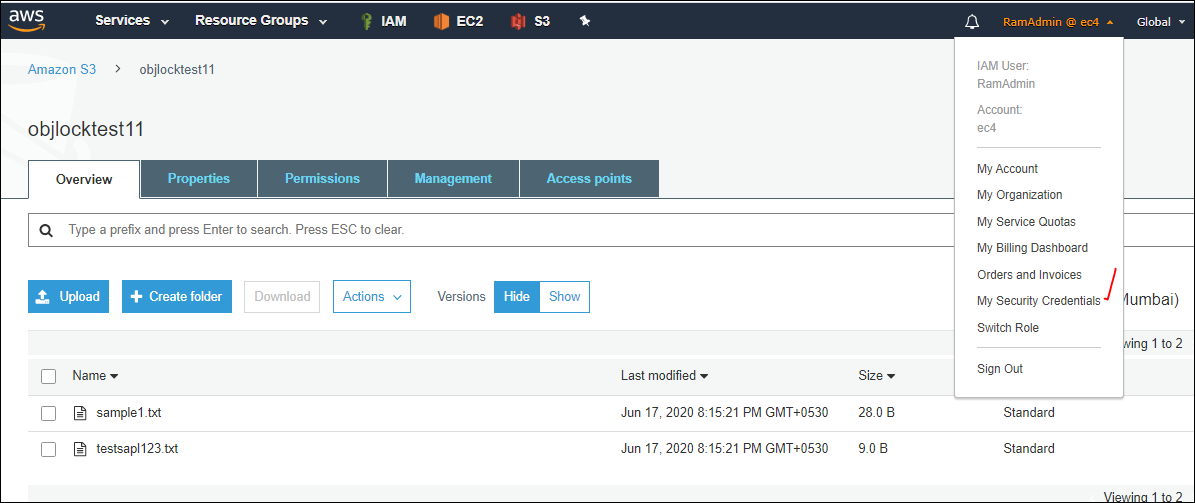
* Even if we need to provide access OF THE BUCKET to another AWS Account.jusr click on the Add account under the access control list tab.

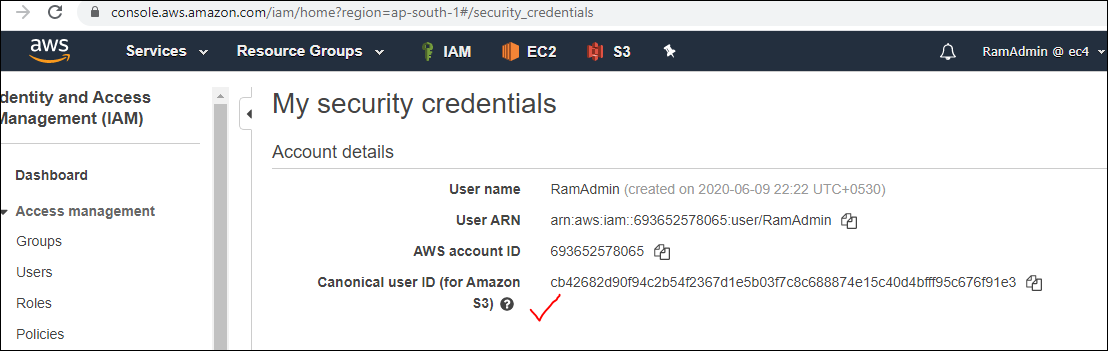


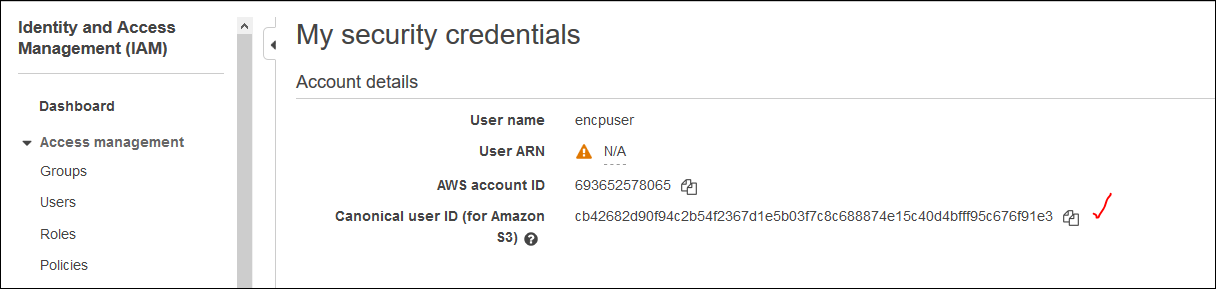
Here we can enter the canonical id or root email id.but email address is not going to work.so we need to use canonical id. We are not sure what issues email address , email will not work.

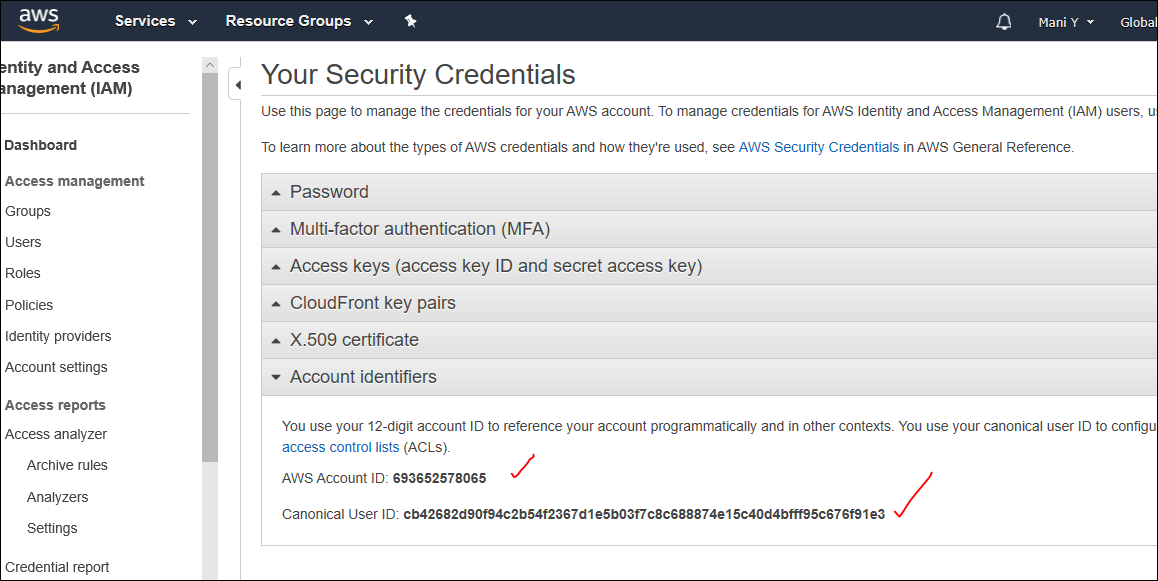
* Where can we find the canonical id for an account?

Click on the user name on top right corner – MY Security Credentials.





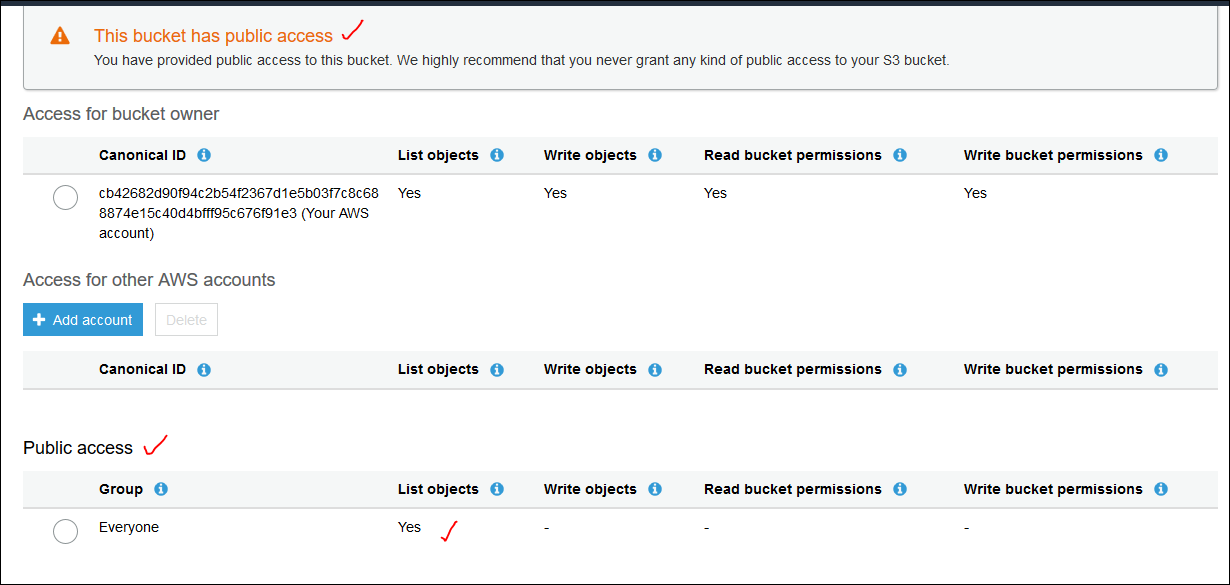


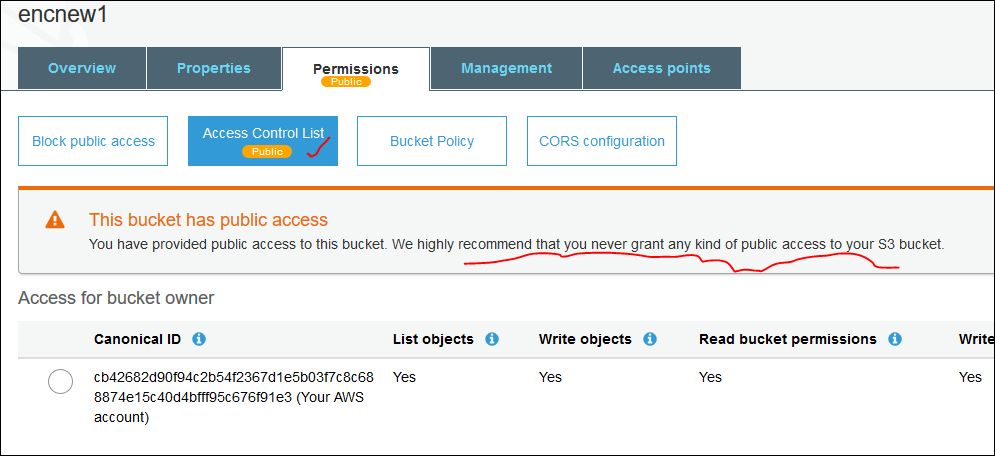


So by adding the other AWS account canonical id we can provide access to the list objects / write objects / read / wirte bucket permissions.

* But other AWS account user will not get the shared bucket like list now how we are looking.then how can he access it, by using CLI [Command line interface ], other third party application.
* By using CLI, we will discuss in EC2 module.
* So by using those two options another AWS account user can access the shared bucket.
* So finally a bucket has to be shared between two different AWS account users can be achieved by sharing the Canonical id, so that one AWS account user 1 can provide access to another AWS account user 2.

Public access: if we enable the options under it , we can share the details to every one.





* So who ever know the buckets urls then can access that entire bucket data.
* This is not at all recommended to grant any public accessto s3 bucket.

**S3 log delivery group:**

These buckets actually we can use to store the logs also, for ex; suppose one application is running and it will sent all logs to another service called cloud watch, and that cloud watch want to store all the logs into this S3 bucket.in that case whether valid permissions are there to store the logs or not. So if we enable the list/write objectsclcik on save. Now that bucket is eligible to store all the logs from any third party applications or using any Amazon tools also.for any of the log delivery group.

Load balancer, VPC all store the logs in S3.so whenever we get any issue while storing the log in S3, we need to check the whether S3 log delivery is enabled or not.

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

**S3 bucket – permission --Bucket Policy:**

**Before getting into this option we need to chk the block public access settings should be turned off.**

By using the ACL, we cant achieve some scenarios:

Suppose we have IAM user 1 and IAM user 2 for same root user. Both IAM users has S3 full Access.

IAM user 1 has special bucket where IAM user 2 is restricted to it that special bucket. But IAM suesr should have read only access on objects of IAM user1 special bucket or user2 should be restricted to upload that objects in that particular buckets. Such kind of scenario can be achieved by using Bucket Policy.

Basically bucket policy is written in json format. We have policy generator and we can apply that generated policy on the our S3 bucket.

Scenario:- create an IAM user 1, IAM user2 both should have S3 full access.

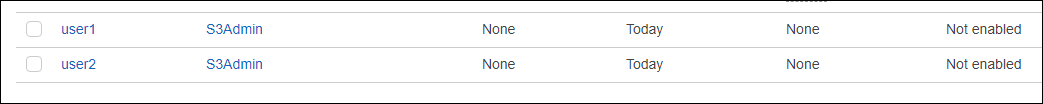
IAM user 1 🡪 Bucket to this User2 should have Read only on objects/ restrict put (upload) operation.

By using ACL we cant design the above scenario, either we can modify all the permission for all IAM users, or we can share with another IAM user another AWS account user or we can make it public.

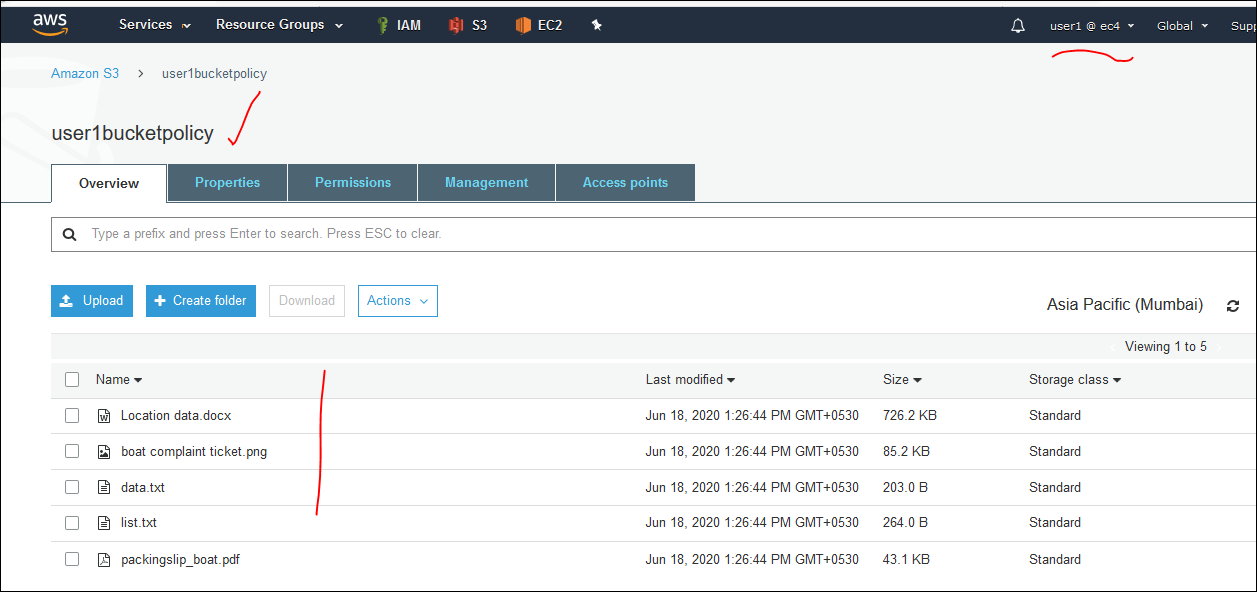
But here both users are in same AWS account, this is basically user 1 bucket, for this bucket user 2 should have the permissions to upload any object for user1 bucket.

Such type of scenarios we can achieve by using **bucket policies.**

Now created users [user1, user2].

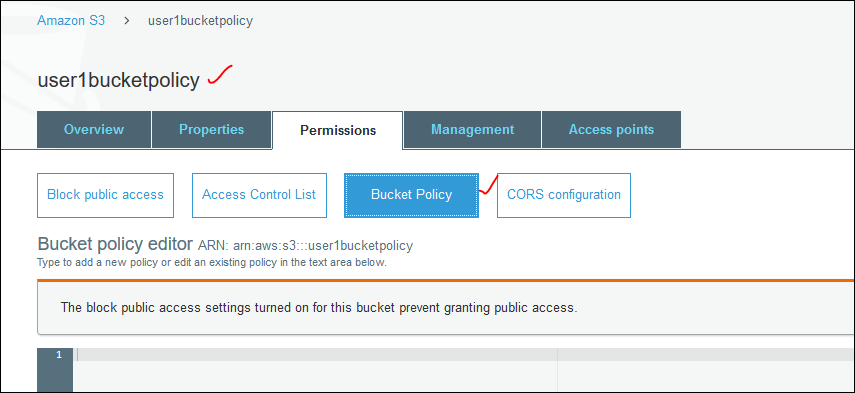


Now create a bucket [ user1bucketpolicy ] for user1.



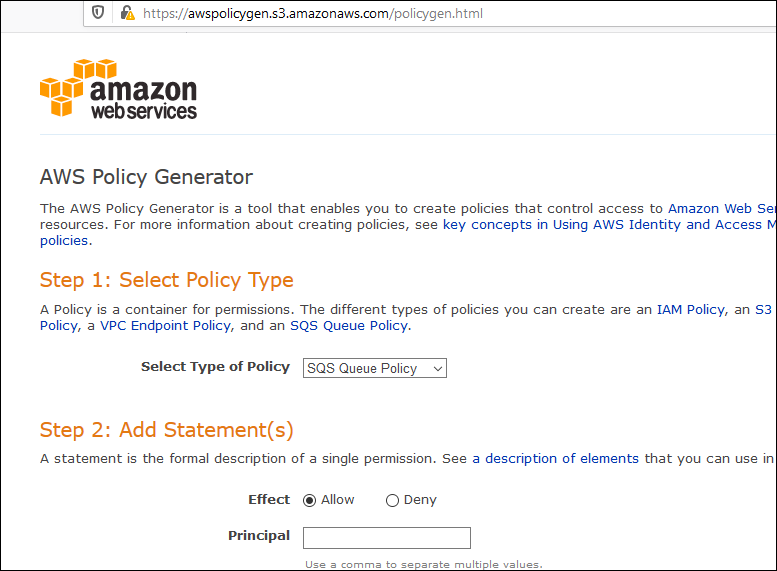
Now we aregoing to give all permissions to user 2 except to upload any data into this [user1bucketpolicy ] bucket.

In this case we have any option called bucket policy.in this we have policy generator, where wcan generate the olicy and apply to the bucket.

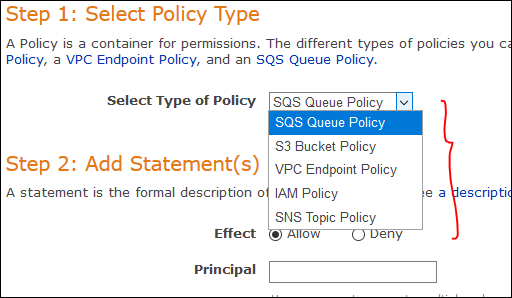




Click on the policy generator



Now we need to select the policy type. as we are applying for S3 , so select the S3 Bucket policy form the drop down list.



Before generating the policy we need to consider some of the things.

**1) Effect:** what is the effect by using this policy, whether we need to allow / Deny. Based on the actions.

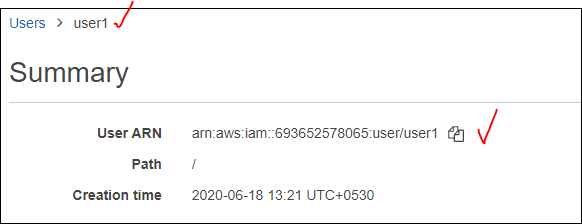
--> Allow

--> Deny

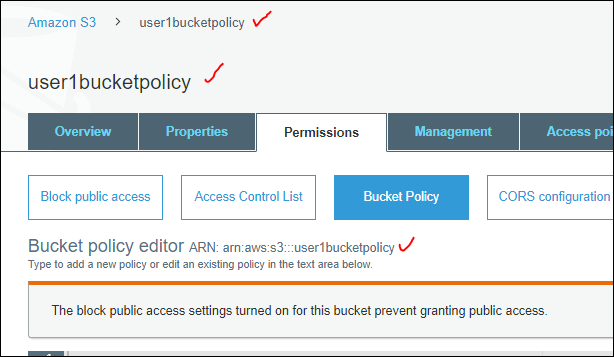
**2) Principle :** IAM USer ARN Name / IAM group ARN [ Amazon Resource name ] Name.. arn:aws:iam::518084852393:user/user2

🡪If we want to restrict for multiple people group is best thing.

🡪 ARN can be created when a user has created we will get ARN.



🡪 similarly if a bucket has created we will get ARN for it .



So in principal we can provide the ARN value to Allow/ deny the effect of that policy. Even we can provide comma to give multiple values allow.

**3) AWS Service:** it will automatically pick if we select the “Type of Policy”.

**4)Action :** What do you want to allow/deny.. : [PUT OBJECT] this is one of the action. We can have multiple actions in it. we can’t customize them , but we can select to perform the effect on that Actions.

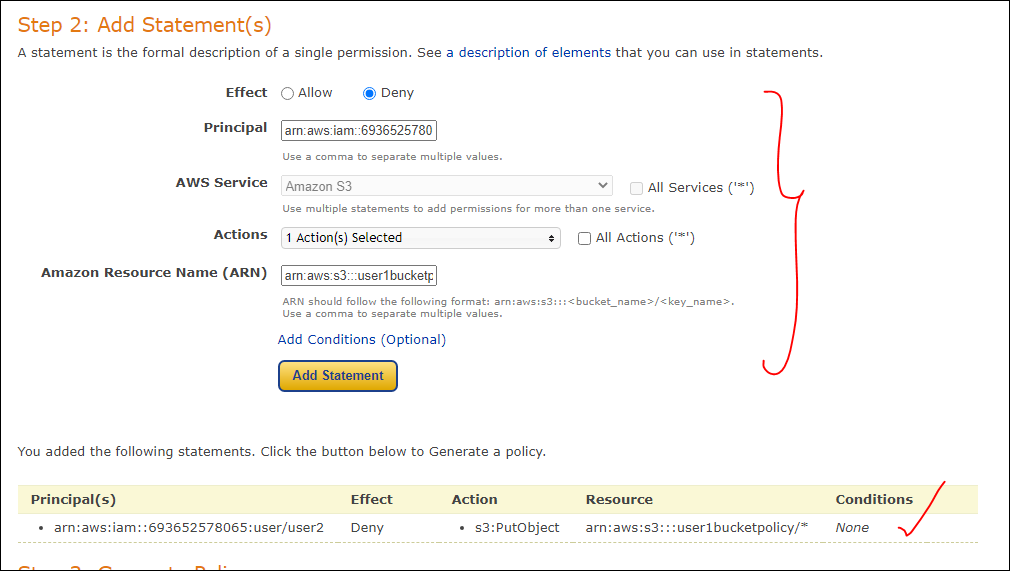
According to our scenario , we are denying the upload action [ put object] from user2 on the user 1 bucket [ user1bucketpolicy ].

**5) Amazon Resource name (ARN)** : here we need to give the Resource name on what Bucket i.e., S3 resource name which is in terms of arn [arn:aws:s3:::user1bucketpolicy ].

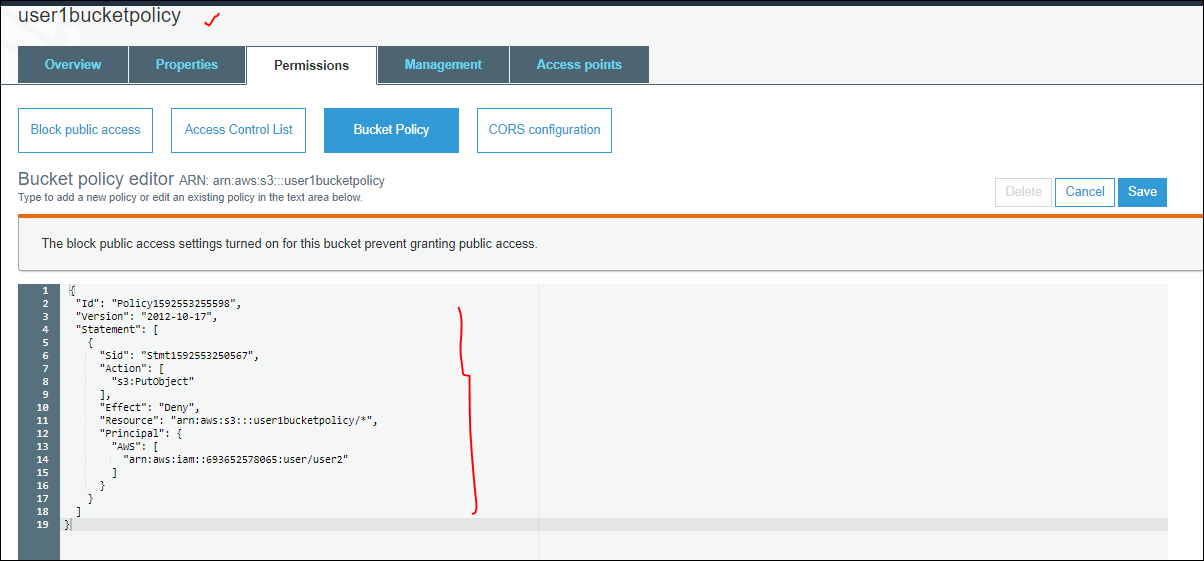
If the action is at bucket level then we need to provide the same ARN [arn:aws:s3:::user1bucketpolicy ]

If the action is at Object level then we need to provide ARN with [/\*] like [arn:aws:s3:::user1bucketpolicy/\* ]

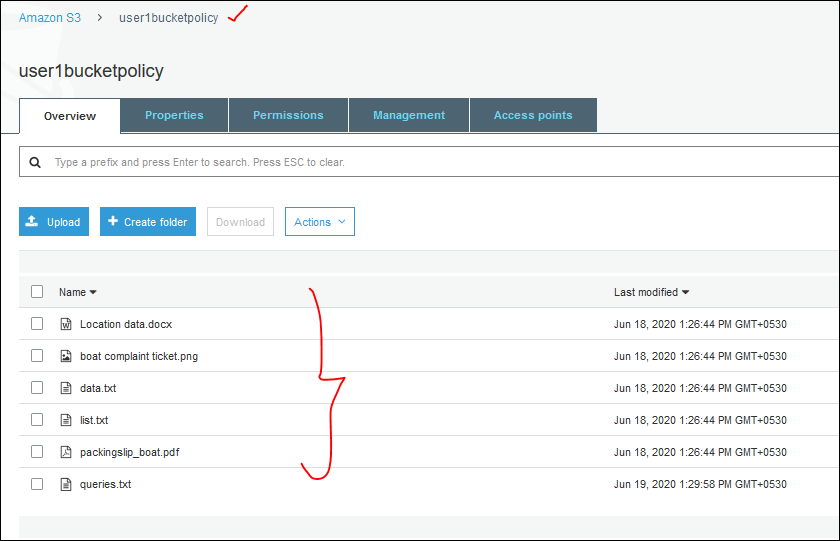
After applying all the above mentioned once , it looks like as shown below image



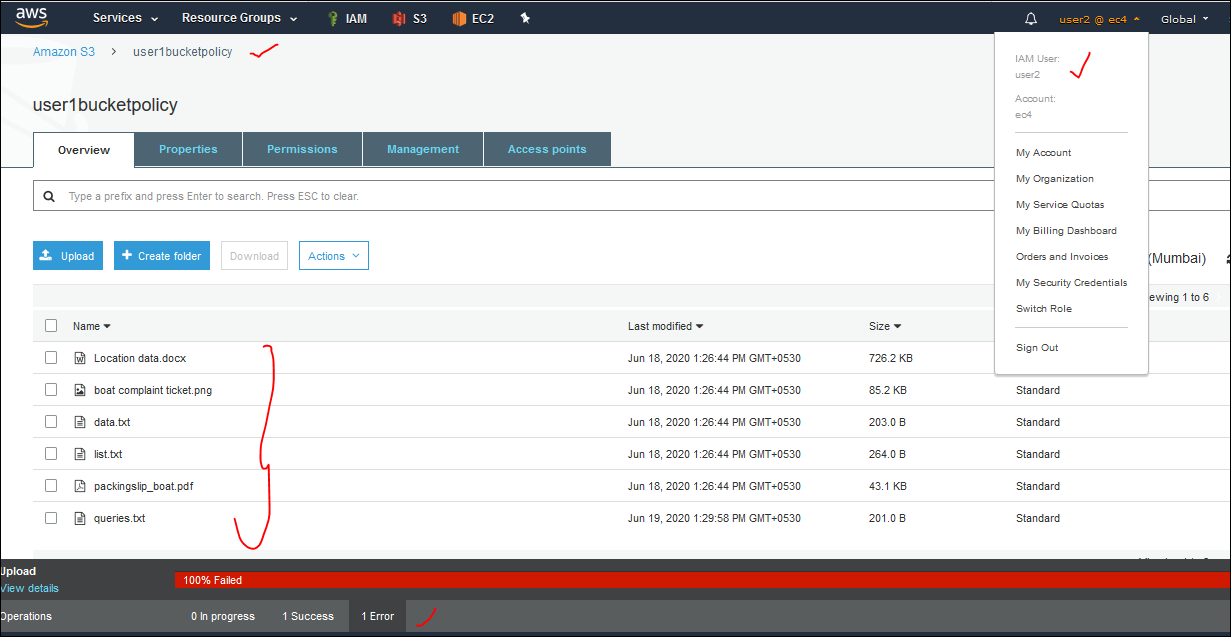
Now copy the generated policy and paste it in the Bucket Policy Editor for which bucket we are applying this policy and click on save button.



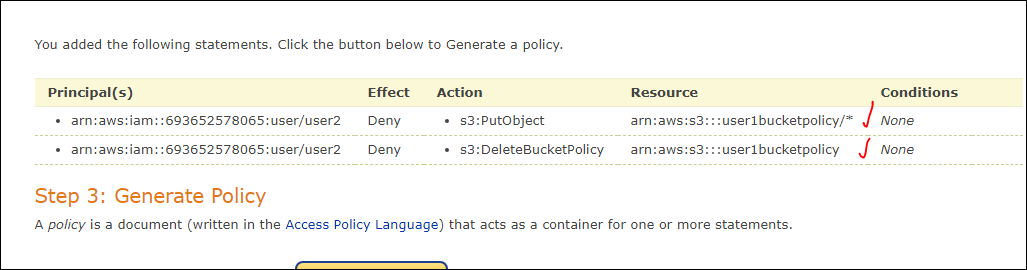
Now we can check the available data in User1bucketpolicy.as shown below.



Now login to user 2 and try to upload an object to ‘ user1bucketpolicy “ bucket.as it failed to upload an object.

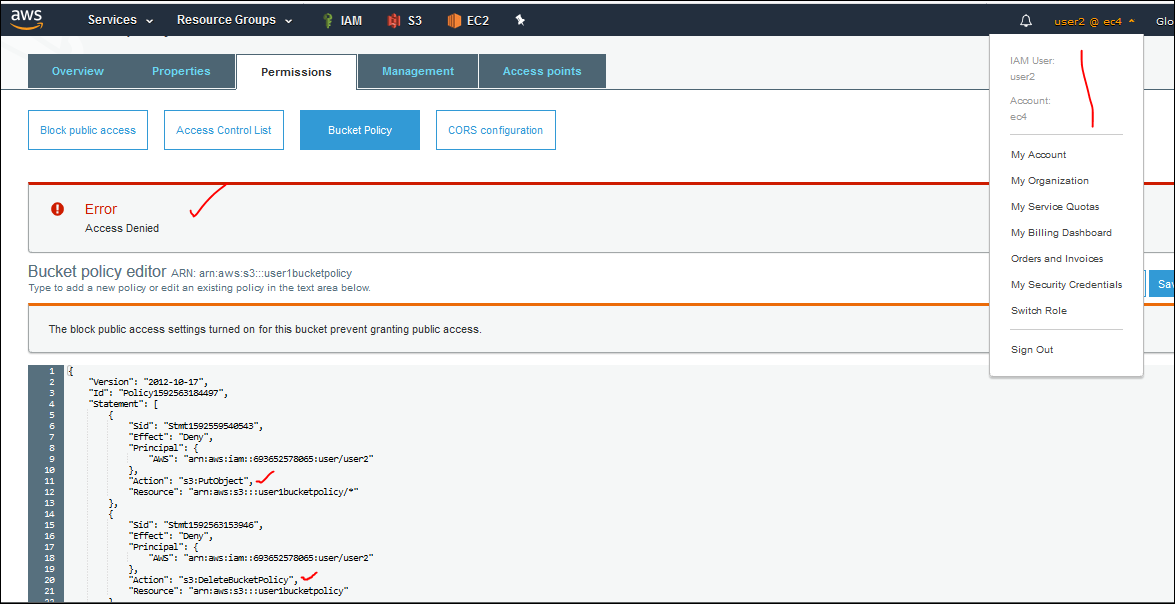


We can upload to another buckets coz we created the policy only for Bucket “user1bucketpolicy”. Here not only we restricted the user2 to upload an object but also, we need to restrict him not to delete the Bucketpolicy.





Now tried to delete with user2 , we cant coz we enabled not to delte the bucket policy.



🡪 we can add multiple users to whom we can restrict to add objects to the specified bucket. This is bucket policy.simply adding the ARN of other user.

🡪what ever the Actions we provide there are depends on different usecases as per the organization requirement.

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

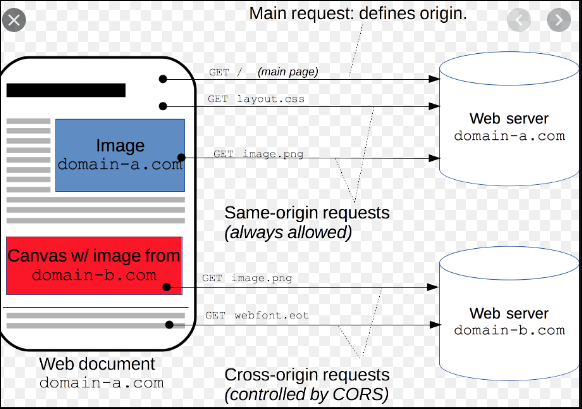
**CORS Configuration:**

It stands for cross origin sharing.

If we are using one domin and runnninf scriot from another domain. Then we can use this CORS.

It can be impletementd by using many programs , java, springs support, python, .net,

Ex:- we are trying to open an web site and the brower is restricted to run some java script, but that web site is required java script to run, so in this can it can’t load, as a developer need to deliver the web site even though the browser, domain won’t allow to run any scripts. In that case we are using the run those scripts in different domain. As shown in below image. Basically it is developer thing.



So suppose If we get any CORS configuration ticket , we can upload that CORS script.

Basic operation s are put, get, head.. basically they will provide to us.to allow from another domain and allthen we can give it.

So coming to AWS, S3 part no need to worry about this CORS Configuration feature.

Website is nothing but called Domain. Domain represents an application or website.

Basically CORS is for web application layer.

Simple thing is , suppose our browser restricts to run any java script which is required by the website and it is not running in our browser. So developer will run the application in different domain and pushes the output to our browser then we can see that web page.