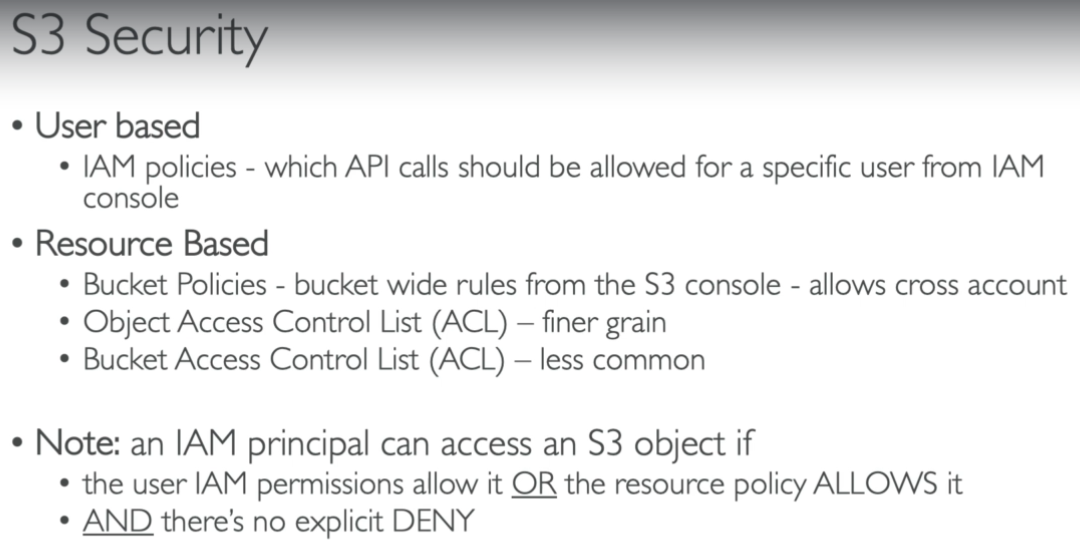
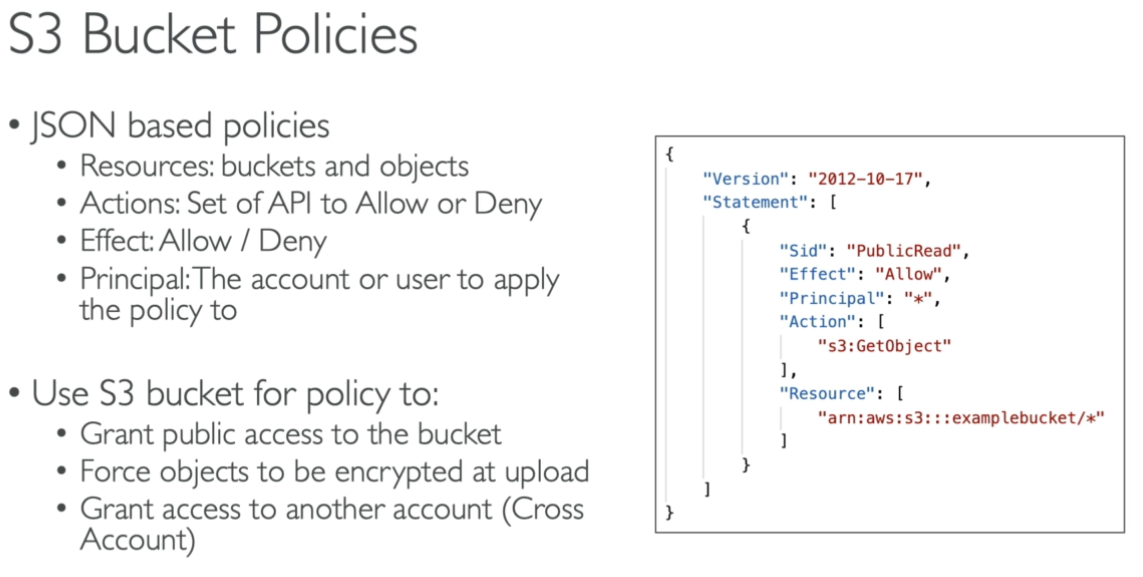
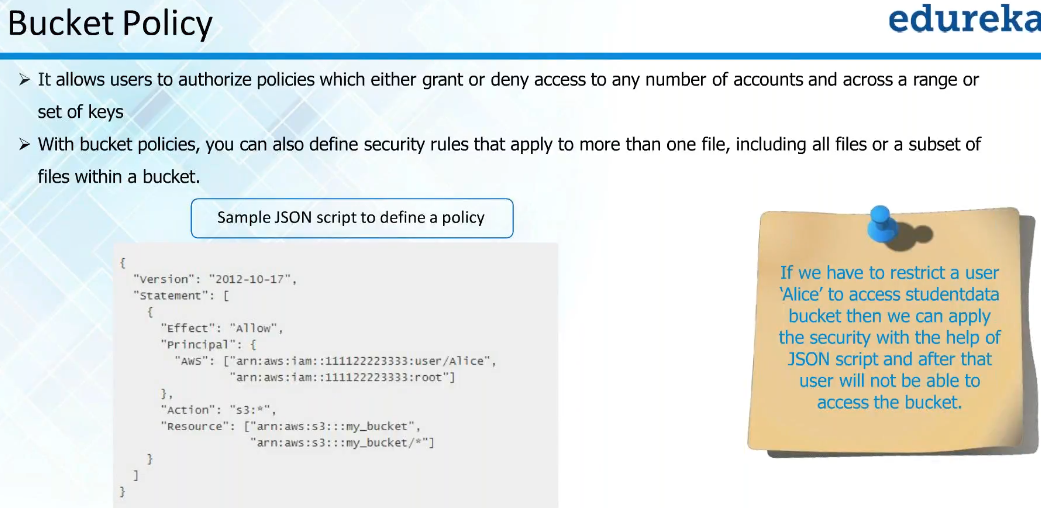
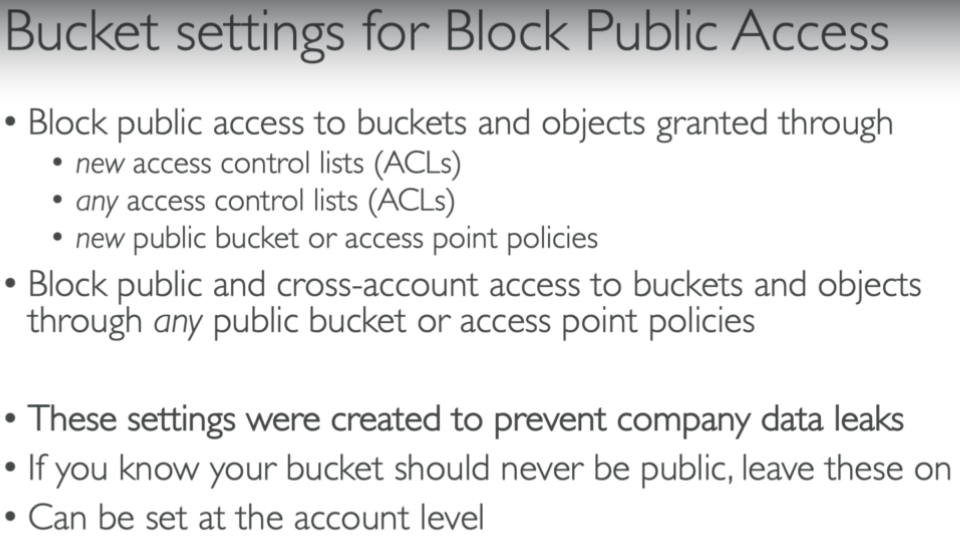
**S3 security:**

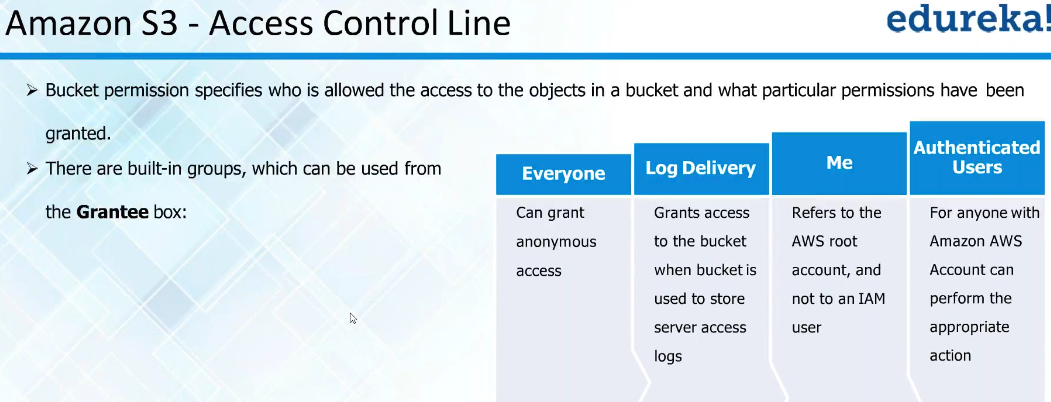


* If a user has IAM permissions to access the bucket and there is explicit deny on the bucket to not allow. Then user can’t access it.

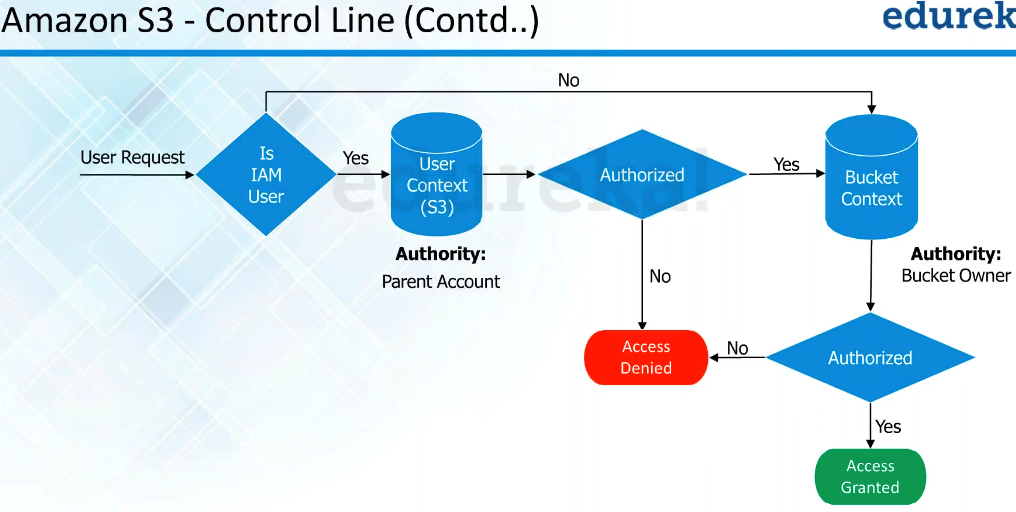


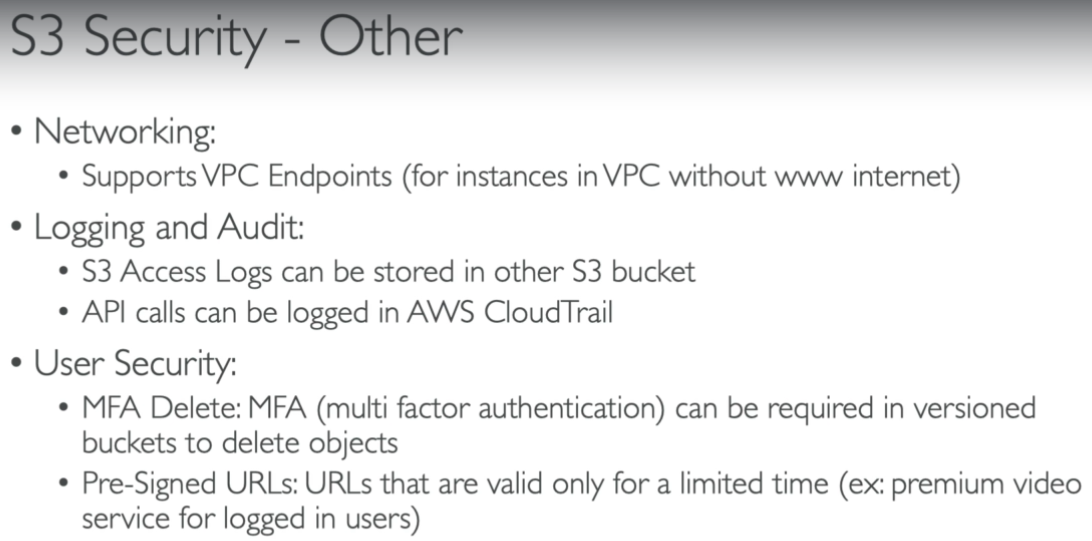




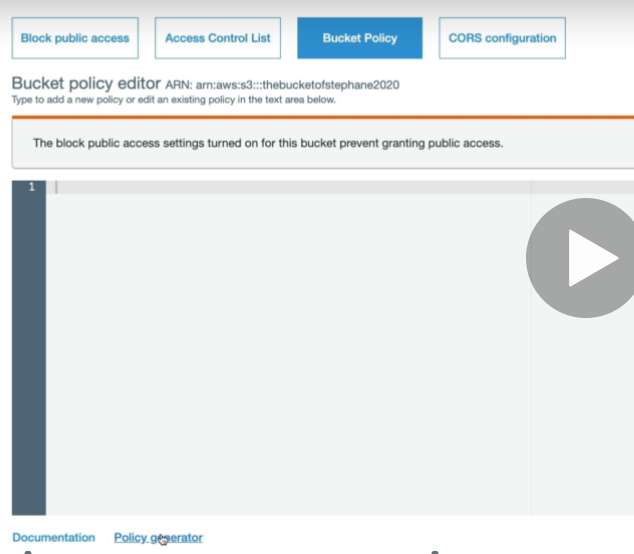


* We can have our application logs stored here





**Hands on:**

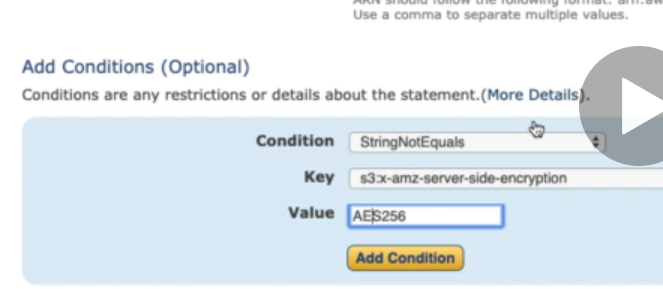


* We need to go to bucket policy inside the bucket and need to place the JSON file in empty space or we can use the policy generator to generate the JSON. We can also get the ARN in above image.

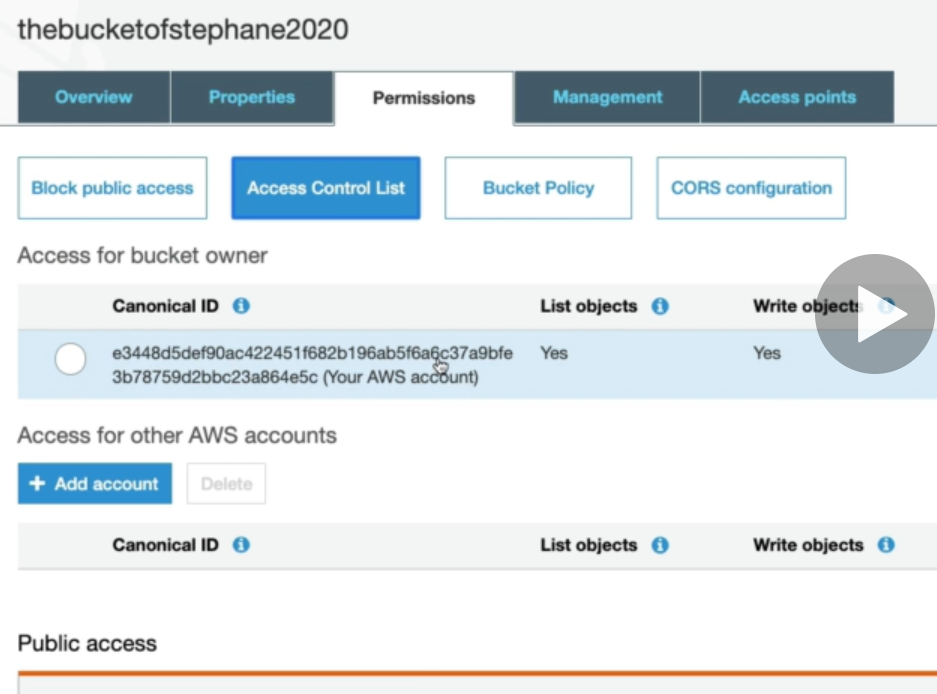


* We need to select the type of policy as “s3 bucket policy”, then allow or deny permission
* Principal is \* means everyone, actions we can select “put objects” to deny the access of uploading any object into the bucket.
* Then finally, we need to give the ARN of an object. We can use \* option in actions and AWS services also.

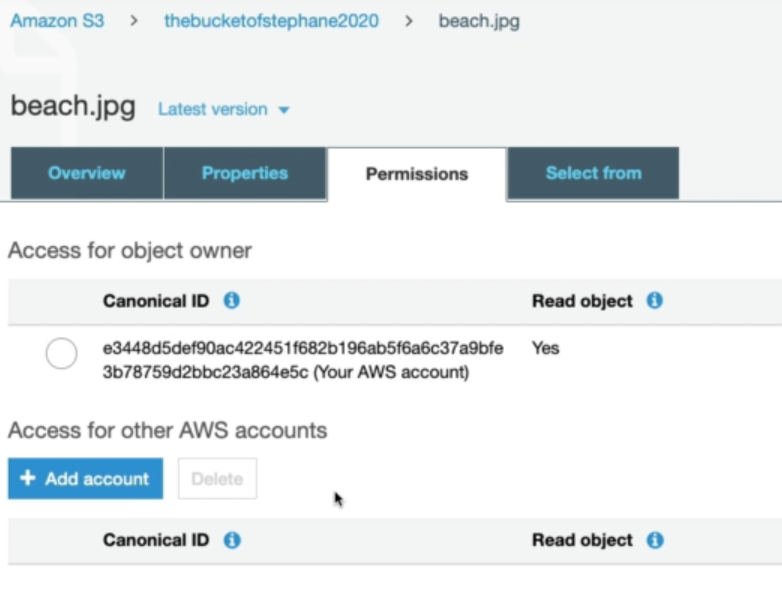
**We need give “ARN/\*” inside ARN box above, so the policy will be added to all the objects inside that ARN**



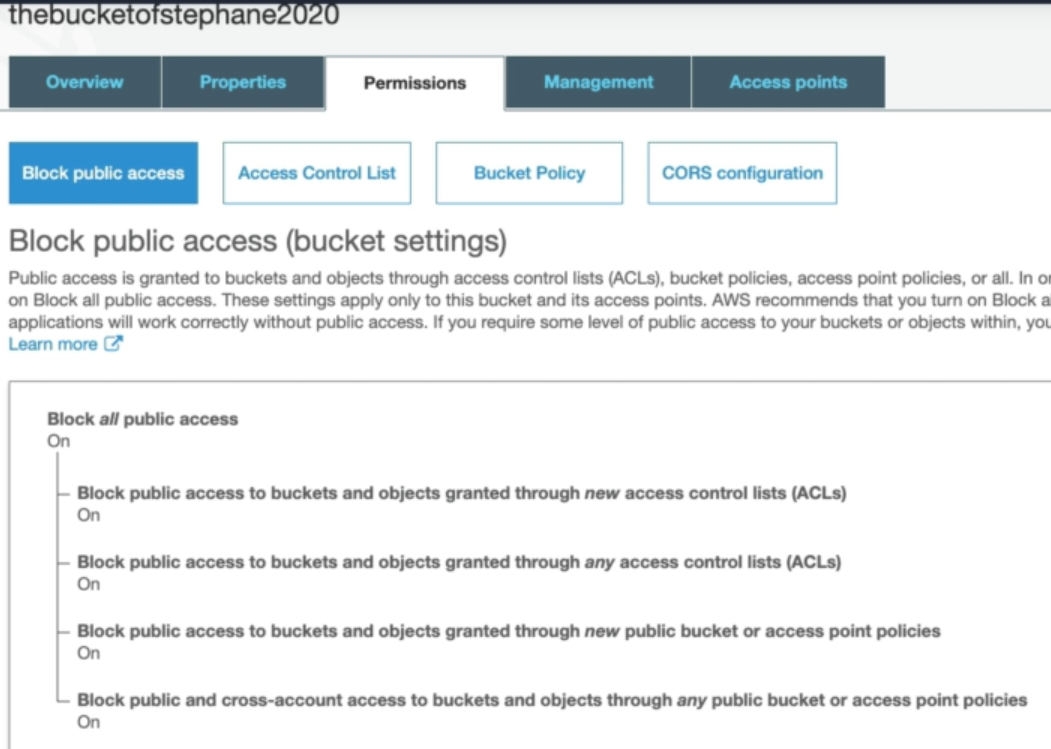
* We can also the condition downside as if the key is not equals to the value, then deny it as above.
* And finally, we can generate the policy. It will generate the JSON script.
* Now, copy the script and add it in the bucket permissions and save.
* Now, if we add any file with the key by passing the condition. Then only we can be able to upload it, otherwise it will be denied.
* We can also easily find these bucket policy statements in google.



* We also have the access control at the bucket level.



* We can also add ACL permissions at the object level as above.



* We can also edit the public access of the bucket as above.

**User level permissions:**

* We can also give bucket policy to specific users as by updating below json file.





* In **“access control lists”** option, we can add permissions to another account. In bucket policies, we can enable access with json file by generating from policy generator.
* We can also enable the permissions to an object in **“permissions”** section. There we can enable access for public access and access to other accounts.