AWS Study Guide Line

**Simple Storage Service(S3)**

S3 (simple storage service) – S3 is a safe place to store your file basically it is object based and **global namespace.**

* S3 bucket creation and manage
* S3 bucket policy (Public Permission and ACL according to their existing user)
* S3 Object Encryption
* S3 versioning – store all version of objects (S3 versioning is used for bucket backup ) it is a great backup tool in S3 ) once versioning enabled we cannot disabled it since we can suspended)
* S3 versioning with MFA (multifactor authentication is additional layer of security)
* Lifecycle Management rules (current version and previous version concepts like we can change the storage class transition in diff storage type, expire and deletion of bucket etc.)
* S3 cross region replication- cross region replication is required versioning to be enabled first. Basically in this we can replicate our entire bucket in diff region with same or diff aws account) this is also a great backup tool like versioning
* S3 transfer acceleration – is basically faster transfer and upload service
* S3 bucket mount on EC2

**Steps are followed.**

1. Create an IAM ROLE with EC2 and S3 access policies
2. Launch an EC2 instance with all default setting and add ssh policy in SG to access your instances.
3. Create a bucket or may create direct on EC2 instances through command line

**# aws s3 mb s3://your-bucket-name**

1. Now access instance doing ssh by public IP and refer the below command to mount your s3 bucket on EC2.

**# yum update –y**

**# yum install automake fuse fuse-devel gcc-c++ git libcurl-devel libxml2-devel make openssl-devel –y**

**# git clone** [**https://github.com/s3fs-fuse/s3fs-fuse.git**](https://github.com/s3fs-fuse/s3fs-fuse.git)

**# ls ; cd s3fs-fuse ; ./autogen.sh ; ./configure –-prefix=/usr ; make ; make install**

**# mkdir -p /var/mybucket**

**# aws s3 mb s3://your-bucket-name**

**# s3fs bucket-name /mount-point -o iam\_role=(IAM\_ROLE\_NAME)**

**# df –h**

1. You will be able to see the 256T size of bucket has been mounted on s3fs File system.
2. Another way to mount s3 bucket through IAM user access key and secret key – all steps are same as above only you have to create one user in IAM give Programming permission and add the EC2 and S3 full permission policy and grant the access to the user to access s3 bucket in EC2.
3. So Here are the steps

**Create a file with name of /etc/passwd-s3fs**

* Edit it with vim editor and place the user access and secret key do save and exit.

**AKIAS4WPMAHNXVYQYE6E:EHy/MQEfLpHpE8AxBqD+fQhtsn+cwBAr05DbwVIM**

* Change file /etc/passwd-s3fs permission to 640

**# chmod 640 /etc/passwd-s3fs**

* While mounting the bucket just change the command

**# s3fs bucket-name –o allow\_other –o uid=1001 –o mp\_umask=002 –o multireq\_max=5 /your-bucket-name**