S3 Storage and Policy

Use Cases

- Backup And Storage
- Disaster Recovery
- Archive
- Hybrid Cloud Storage
- Application Hosting
- Media hosting
- Data Lakes and Big Analytics
- Software Delivery
- Static Website

S3 Bucket

- S3 Allow to store object (Files) in bucket
- Buckets must have globally Unique Name (Across All region all account)
- Bucket are defined at the region level
- S3 Looks like a global service but buckets are created in a region
- Naming convention
  - No Uppercase
  - No underscore
  - 3-63 characters long
  - Not an IP
  - Must start with lowercase letter or number

OverView

- Ibjects (files) have a Key
- The key is the FULL path
  - S3://bucketname/my_filesname.txt
  - S3://bucketname/my_filesname.png
  - S3://bucketname/myfolder/my_file.txt
- The Key is composed of "Directories" within buckets (Although the UI will trick you to think otherwise)
- Just Keys with very Long name that contain Slashes("/")

***** For Object values (Files)*****

- Max Object (Files) Size 5TB (5000GB)
- If upload more than 5GB, Must use "Multi-part Upload"
- Metadata (List of textkey / Valu Pairs -System or User metadata)
- Tags (Unicode key / Value pair – up to 10) – Useful for security /Lifecycle
- Version ID(if versioning is enabled)

*******S3 Security******

User Based

- IAM policies: which API calls should be allowed for a specific user from IAM Console
- IAM User require only IAM policy to access bucket
- Anonymous www website visitor require S3 Bucket Policy and Allow Public Access

Resourced Based

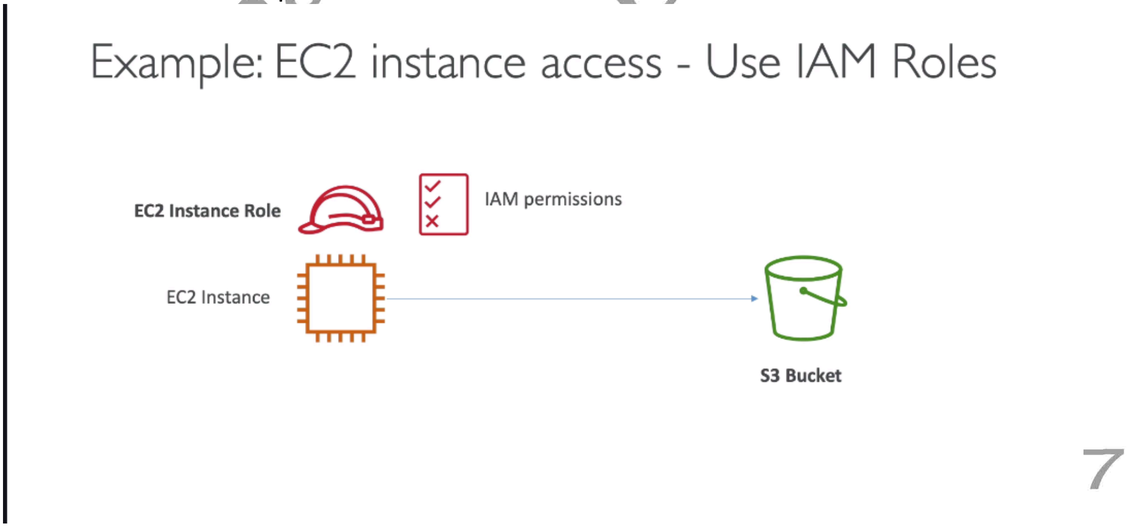
- Bucket Policies: Bucket wide rules from the S3 console =allow cross account
- Object Access Control List (ACL) finer grain
- Bucket Access Control List (ACL) – Less Common

Note: An IAM principal can access an S3 Object if

- The user IAM permission allow it OR the resource policy Allow it
- AND there's no explicit DENY

EC2 access S3 Bucket

- First.   - EC2 Attached IAM Role
- Second.- Setup IAM Role allow to S3 Access.



Example: EC2 instance access - Use IAM Roles

Note : Allow Also Cross Account to Access S3 Bucket but Require S3 Bucket policy to S3 Access Cross Account.

S3 Bucket Policy:

- Default any file or object does not allow public access
- But S3 Bucket Policy to Allow Public access require Get Object Policy to Access.

S3 Website

- Web site access allow in S3 bucket need Public Read Access. Require to set Get Object Policy for site or bucket.

  If You got a 403 (forbidden) error, Make sure the bucket policy to allows Public Reads! In-short “Get Object Policy “ require.

S3 Versioning

- Our can version allow for files
- It is Enabled at the Bucket level
- Same Key overwrite to version your bucket
- It is best practice to version your bucket
  - Protect against unintended deletes (Ability to restore a version)
  - Easy roll back to previous version
  -

Note:

- Any file that is not versioned prior(Previous) to enabled versioning will have version “Null”
- Suspended versioning does not delete the previous versions

S3 Access Logs

- For Audit purpose, you may want to log all access to s3 Bucket
- Any request made to S3, from any Account, Authorized or Denied will be logged into another S3 Bucket
- That data can be analysed using data analysis tools

Step

1. First create bucket when you want to store Log :”log-buckets”
2. Second go inside the bucket where store your files : “mydata” and then open “Properties”
3. And Enable Sever Access Logging and set Where to store bucket name.

S3 Replication (CRR & SRR)

- CRR - Cross Region Replication
- SRR – Same Region Replication
- Must Enable Versioning in Source and Destination
- Bucket can be in Different accounts
- Copying is asynchronous
- Must give proper IAM permission to S3

*** CRR- Use Cases: compliance, Lower Latency Access, Replication across account

***SRR- Use Cases: Log Aggregation, Live replication between production and test accounts