S3 101 - Summary

A CLOUD GURU

- Remember that S3 is Object-based: i.e. allows you to upload files.
- Files can be from 0 Bytes to 5 TB.
- There is unlimited storage.
- Files are stored in Buckets.
- S3 is a universal namespace. That is, names must be unique globally.
- https://s3-eu-west-1.amazonaws.com/acloudguru

S3 Summary

S3 101 - Summary

A CLOUD GURU

- Read after Write consistency for PUTS of new Objects
- Eventual Consistency for overwrite PUTS and DELETES (can take some time to propagate)

S3 101 - Summary

A CLOUD GURU

- S3 Storage Classes/Tiers:
  - S3 (durable, immediately available, frequently accessed)
  - S3 - IA (durable, immediately available, infrequently accessed)
  - S3 - One Zone IA: Same as IA. However, data is stored in a single Availability Zone only
  - S3 - Reduced Redundancy Storage (data that is easily reproducible, such as thumbnails, etc.)
  - Glacier - Archived data, where you can wait 3 - 5 hours before accessing

S3 101 - Summary

A CLOUD GURU

- Remember the core fundamentals of an S3 object:
  - Key (name)
  - Value (data)
  - Version ID
  - Metadata
  - Subresources (used to manage bucket-specific configuration)
    - Bucket Policies, ACLs
    - CORS
    - Transfer Acceleration

S3 101 - Summary

A CLOUD GURU

- Object-based storage only (for files.)
- **Not suitable to install an operating system on.**
- Successful uploads will generate a HTTP 200 status code.

S3 Security - Summary

A CLOUD GURU

- By default, all newly created buckets are PRIVATE.
- You can set up access control to your buckets using:
  - Bucket Policies - Applied at a bucket level.
  - Access Control Lists - Applied at an object level.
- S3 buckets can be configured to create access logs, which log all requests made to the S3 bucket. These logs can be written to another bucket.

S3 Encryption - Summary

A CLOUD GURU

- Encryption In-Transit
  - SSL/TLS
- Encryption At Rest
  - Server Side Encyption
    - SSE-S3
    - SSE-KMS
    - SSE-C
  - Client Side Encyption

- Remember that we can use a Bucket Policy to prevent unencrypted files from being uploaded by using creating a policy which only allows requests which include the x-amz-server-side-encryption parameter in the request header.

S3 CORS - Summary

A CLOUD GURU

- Cross Origin Resource Sharing (CORS)
  - Used to enable cross origin access for your AWS resources
  - e.g. S3 hosted website accessing javascript or image files located in another S3 bucket
  - By default resources in one bucket cannot access resources located in another
  - To allow this we need to configure CORS on the bucket being accessed and enable access for the origin (bucket) attempting to access
  - Always use the s3 website URL, not the regular bucket URL:
  - http://acloudguru.s3-website-eu-west-1.amazonaws.com
  - https://s3-eu-west-1.amazonaws.com/acloudguru

S3 CloudFront - Summary

A CLOUD GURU

- Edge Location - This is the location where content will be cached. This is separate to an AWS Region/AZ.
- Origin - This is the origin of all the files that the CDN will distribute. Origins can be an S3 Bucket, an EC2 Instance, an Elastic Load Balancer, or Route53.
- Distribution - This is the name given the CDN, which consists of a collection of Edge Locations.
  - Web Distribution - Typically used for Websites.
  - RTMP - Used for Media Streaming.

S3 Performance Optimization - Summary

A CLOUD GURU

- Remember the 2 main approaches to Performance Optimization for S3:
  - GET-Intensive Workloads - Use CloudFront
  - Mixed-Workloads - Avoid sequential key names for your S3 objects. Instead, add a random prefix like a hex hash to the key name to prevent multiple objects from being stored on the same partition
    - mybucket/7eh4-*2018-03-04-15-00-00*/cust1234234/photo1.jpg
    - mybucket/h35d-*2018-03-04-15-00-00*/cust3857422/photo2.jpg
    - mybucket/o3n6-*2018-03-04-15-00-00*/cust1248473/photo2.jpg

S3 - Summary

A CLOUD GURU

- Read the FAQ!
- https://aws.amazon.com/s3/faqs/