Chapter 4: Simple Storage Service (S3)

Rahul Daware

May 12, 2018

Contents

1 What is S3?

S3 provides developers and IT teams with secure, durable, highly scalable object storage. Amazon S3 is easy to use, with a simple web services interface to store and retrieve any amount of data from anywhere on the web. S3 is a safe place to store your files. It is object based storage. The date is spread across multiple devices and facilities.

2 S3 - The Basics

- 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. (Buckets are folder in cloud. Each bucket has universal namespace. Each bucket will have a DNS address. Bucket names have to unique.
- S3 is a universal namespace. i.e. names must be unique globally.
- URL look like this : https://s3-eu-west-1.amazonaws.com/acloudguru
- When you upload a file to S3, you will receive a HTTP 200 if the upload was successful
- Built for 99.99% availability for the S3 platform
- Amazon guarantee 99.9% availability
- Amazon guarantees 11 9s durability for S3 information
- Tiered Storage available
- Lifecycle Management
- Versioning
- Encryption
- Secure your data using Access Control Lists and Bucket Policies

3 Data Consistency Model for S3

- Read after write consistency for PUTS of new objects
- Eventual consistency for overwrite PUTS and DELETES (can take some time to propogate)

4 S3 is a simple key-value store

S3 is object based. Objects consists of the following:

- Key (This is simply name of the object
- Value ((This is simply the data and is made up of a sequence of bytes
- Version ID (Important for versioning)
- Metadata (Data about data you are storing)
- Subresources
  - Access Control Lists
  - Torrent

5 S3 - Storage Tiers/Classes

- **S3 Standard** : 99.99% availability 11 9s durability, stored redundantly across multiple facilities, and is designed to sustain the loss of 2 facilities concurrently.
- **S3 -IA** : (Infrequently Accessed): For data that is accessed less frequently, but requires rapid access when needed. Lower fee than S3, but you are charged a retrieval fee.
- **S3 One Zone - IA** Want a lower cost option for infrequently accessed data, but do not require the multiple availability zone data resilience.
- **Glacier** Very cheap, but used for archival only. Expedited, standard or bulk. A standard retrievel time takes 3-5 hours.

6 S3 - Charges

Charged for:

- Storage (Per GB basis)
- Requests (No. of requests)
- Storage Management Pricing (Charged for tags on data)
- Data Transfer Pricing (Transferring data from one region to other)
- Transfer Acceleration : Amazon S3 Transfer acceleration enables fast, easy and secure transfers of files over long distances between your end users and an S3 bucket. Transfer acceleration takes advantage of Amazon CloudFront's globally distributed edge locations. AS the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

7 S3 Exam Tips for S3 101

- 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
- Read afte write consistency for PUTS of new objects
- Eventual Consistency for overwrite PUTS and DELETES (can take some time to propogate)
- Storage Classes/Tiers:
  - S3 (durable, immediately available, frequently accessed)
  - S3 -IA (Durable, immediately available, infrequently accessed)
  - S3 One Zone - IA (event chaeaper than IA, but onle in one AZ)
  - Glacier - Achived data, where you cn wait 3-5hours before accessing
- Remember core fundamentals of S3 object - Key (name), Value (data) , Version ID, Metadata, Subresources (ACL, Torrent)
- Object based storage only (for files)
- Not suitable to install an operating system on
- Successful uploads give HTTP 200 response

8 Create an S3 Bucket - Exam Tips

- Buckets are a univeral name space
- Upload an object to S3 receive a HTTP 200 code
- S3, S3 -IA, S3 - One Zone IA, S3 Reduced Redundancy Storage
- Encryption
  - Client Side Encryption
  - Server Side Encryption with Amazon S3 Managed Keys (SSE-S3), Server Side Encryption with KMS (SSE-KMS), Server Side Encryption with Customer provided keys (SSE-C)
- Control access to buckets using either a bucket ACL or using bucket policies
- By Default buckets are private and all objects stored inside them are private

9 S3 Versioning - Exam Tips

- Stores all versions of an object (including all writes and even if you delete an object)
- Great backup tool
- Once enabled, versioning cannot be disabled, only suspended
- Integrates with lifecycle rules
- Versioning's MFA Delete capability, which uses multi-factor authentication, can be used to provide an additional layer of security

10 S3 - Cross Region Replication Exam Tips

- Versioning must be enabled on both the source and destination buckets
- Regions must be unique
- Files in an existing bucket are not replicated automatically. All the subsequent updated files will be replicated automatically
- You cannot replicate to multiple buckets or use daisy chaining (at this time)
- Delete markers are replicated
- Deleting individual versions or delete markers will not be replicated
- Understand what cross region replication is at high level

11 S3 Lifecycle Management Lab

- Can be used in conjunction with versioning
- Can be applied to current versions and previous versions
- Following actions can now be done:
  - Transition to the standard -infrequent access storage class (minimum file size should be 128 KB and 30 days after the creation date)
  - Archive to the glacier storage class (30 days after IA, if relevant)
  - Permanently Delete

12 Cloudfront

What is a CDN?
A Content Delivery Network (CDN) is a system of distributed servers (network) that delivers webpages and other web content to a user based on the geographic locations of the user, the origin of the webpage and a content delivery server

- **Edge Location** - This is the location where the content will be cached. This is seperate to an AWS Region/AZ
- **Origin** - This is the origin of all the files that the CDN will distribute. This can be either an S3 bucker, an EC2 instance, an elastic load balancer or Route53
- **Distribution** This is the name given the CDN consists of a collection of Edge locations

What is CloudFront
Amazon CloudFront can be used to deliver your entire website, including dynamic, static, streaming, and interactive content using a global network of edge locations.Requests for your content are automatically routed to the nearest edge location, so content is delivered with best possible performance. Amazon CloudFront is optimized to work with other Amazon Web Services, like Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Load Balancing, and Amazon Route 53. Amazon CloudFront also works seamlessly with any non AWS origin server, which stors the original, definitive versions of your files.

Key Terminology

- Web Distribution - Typically used for websites
- RTMP - Used for media streaming
- Edge locations are not just READ only, you can write to them too.(i.e. put an object on to them)
- Objects are cached for the life of the TTL
- You can clear cached objects, but you will be charged.

13 S3 - Security and Encryption

- By default, all newly created buckets are PRIVATE
- You can setup acess control to your buckets using:
  - Bucket Policies
  - Access Control Lists
- S3 buckets can be configured to create access logs. This can be done to another bucket
- Four different methods of encryption in S3:
  - In Transit - SSL/TLS
  - At Rest
    - Server Side Encryption
      - S3 Managed Keys - **SSE-S3**
      - AWS Key Management Service, MAnaged Keys - **SSE-KMS**
      - Server Side Encryption with customer provided keys - **SSE-C**
    - Client side Encryption

14 Storage Gateway

AWS Storage Gateway is a service that connects an on-premise software appliance with cloud-based storage to provide seamless and secure integration between an oragnization's on-premise IT environment and AWS's storage infrastructure. The service enables you to securely store date to the AWS cloud for scalable and cost effective storage.

AWS Storage Gateway's software appliance is available for download as a virtual machine VM image that you install on a host in your datacenter. Storage Gateway supports either VMWare ESXi or Microsoft Hyper-V. Once you have installed your gatewat and associated it with your AWS account through the activation process, you can use the AWS Management Console to create the storage gateway option that is right for you.

Four Types of Storage Gateways:

- File Gateway (NFS) New
- Volumes Gateway (iSCSI)
  - Stored Volumes Gateway Stored Volumes
  - Cached Volumes Gateway Cached Volumes
- Tape Gateway (VTL) Gateway Virtual Tape Library

14.1 Gateway

Files are stored as objects in your S3 buckets, accessed through a Network File System (NFS) mount point. Ownership, permission, and timestamps are durably stored in S3 in the user-metadata of the object associated with the file. Once the objects are transferred to S3, they can be managed as native S3 objects, and bucket policies such has versioning, lifecycle management, and cross-region replication apply directly to objects stored in your bucket.

14.2 Volume Gateway

The volume interface presents your applications with disk volumes using the iSCSI block protocol. Data written to these volumes can be asynchronously backed up as point in time snapshots of your volumes, and stored in the cloud as Amazon EBS (Elastic Block Store) snapshots. Snapshots are incremental backups that capture only changed blocks. All snapshot storage is also compressed to minimized your storage charges.

Stored Volumes
Stored Volumes let you store your primary data locally, while asynchronouslt backing up that data to AWs. Stored volumes provide your on-primies applications with lo latency access to their entire datasets, while providing durable, off-site backups. You can create storage volumes and mount them as iSCSI devices from your on premises application servers. Data written to your stored volumes is stored on your on-premises storage hardware. This data is asynchronously backed up to Amazon Simple Storage Service (Amazon S3) in the form of Amazon Elastic Block Store (Amazon EBS) snapshots. 1 GB - 16TB in size of Stored Volumes.

Cached Volumes
Cached volumes let you use Amazon Simple Storage Service (S3) as your primary data storage while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low latency access to their freuently accessed data. You can create storage volumes up to 32 TB in size and attach to them as iSCSI devices from your on-premises aplication servers. Your gateway stores data that you write to these volumes in Amazon S3 and retains recently read data in your on-premises storage gateway's cache and upload buffer storage. 1GB -32TB in size for cached volumes.

Tape Gateway
Tape Gateway offers a durable, cost-effective solution to archive your data in the AWS cloud. The VTL

interface it provides lets you leverage your existing tape-based backup application infrastructure to store your date on virtual tape cartridges that you create on your tape gateway. Each tape gateway is preconfigured with a media changer and tape drives, which are available to your existing client backup applications as iSCSCI devices. You add tape cartridges as you need to archive your data. Supported by NetBackup, Backup Exec, Veeam etc.

Storage Gateway - Exam Tips

- **File Gateway** - For flat files, stored directly on S3.
- **Volume Gateway**
  - Stored Volumes - Entire dataset is stored on site and is asynchronously backed up to S3
  - Cached Volumes - Entire dataset is stored on S3 and the most frequently access data is cached on site
- **Gateway Virtual Tape Library (VTL)** - Used for backup and uses popular backup applications like NetBackup, Backup Exec, Veeam etc.

15 Snowball - Import Export Disc

AWS Import/Export Disk accelerates moving large amounts of data into and out of the AWS cloud using portable storage devices for transport. AWS Import/Export disk transfers your data directly onto and off of storage devices using Amazon's high speed internal network and bypassing the internet.

Types of Snowballs

- Snowball
- Snowball Edge
- Snowmobile

15.1 Snowball

Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of AWS. Using Snowball addresses common challenges with large scale data transfers including high network costs, lon transfer times and security concerns. Transferring data with snowall is simple, fast ans secure and ca n e as little as one-fifth the cost of high speed internet.

80 TB snowball in all regions. Snowball uses multiple layers of security designed to protect your data including tamper-resistant enclosures, 256-bit encryption, and an industry-standard Trusted Platform Module (TPM) designed to ensure both security and full chain of custody of your data. Once the data transfer job has been processed and verified, AWS performs a software erasure of the Snowball appliance.

15.2 Snowball Edge

AWS Snowball Edge is a 100TB data transfer device with on board storage and compute capabilities. You can use Snowball Edge to move large amounts of data into and out of AWS, as a temporary storage tier for large local datasets, or to support local workloads in remote or offline locations.

Snowball Edge connects to your existing applications and infrastructure using standard storage interfaces, streamlining the data transfer process and miniizing setup and integration. Snowball Edge can cluster together to form a local storage tier and processs your data on-premises, helping ensure your applications continue to run even when they are not able to access the cloud.

15.3 Snowmobile

AWS Snowmobile is an exabyte scale data trsnfer service used to move extremely large amounts of data to AWS. You can transfer up to 100 PB per snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi trailer truck. Snowmobile makes it eas to move massive volumes of data to the cloud, including video libraries, image repositories, or even a completed data center migration. Transferring data with snowmobile is secure, fast and cost effective.

Exam Tips

- Understand what snowball is
- Understand what import export is
- Snowball can do import to S3 and export from S3

16 S3 Transfer Acceleration

S3 Transfer Acceleration utilises the CloudFront Edge Network to accelerate your uploads to S3. Instead of uploading directly to your S3 bucket, you can use a distinct URL to upload directly to an edge location which will then transfer that file to S3.

17 Notes

- Read the S3 FAQs before taking the exam. It comes up a lot.
- Understand the difference between a region, an availability zone(AZ) and an edge location
  - A region is a physical location in the world which sonsists of two or more Availability Zones (AZs)
  - An AZ is one or more discrete data centers each with redundandt power, networking and connectivity, housed in seperate facilities
  - Edge locations are endpoints for AWS which are used for caching content. Typically this consists of CloudFront, Amazon's Content Delivery Network (CDN)
- Remember that S3 is object based i.e. allows you to upload files
- Files can be from 0 bytes to 5TB
- There is unlimited storage
- Files are stored in buckets
- S3 is a universal namespace, i.e. names must be unique globally.
- Bucket URL looks like : https://s3-eu-west-1.amazonaws.com/acloudguru
- Read after write consistency for PUTS of new objects
- Eventual Consistency for overwrite PUTS and DELETES (can take some time to propagate)
- S3 Storage Classes/Tiers
  - S3 - Durable, Immediately Available, Frequently Accessed)
  - S3 -IA (durable, imediately availablem infrequently accessed)
  - 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
- Remember the core fundamentals of S3

  - Key(name)
  - Value(data)
  - Version ID
  - Metadata
  - Access Control Lists

- Object based storage
- Not suitable to install an operating system on
- Stores all versions of an object (including all writes and even if you delete an object)
- Versioning is great backup tool
- Once enabled, versioning cannot be disabled, only suspended
- Versionng integrates with lifecycle rules
- Versioning's MFA Delete capability, which uses multi factor authentication, can be used to provide an additional layer of security
- Cross Region Replication, requires versioning enabled on source bucket as well as destination bucket
- Lifecycle management can be used in conjunction with versioning
- Lifecycle management can be applied to current and previoud versions
- Following actions can now be done :
  - Transition to the standard : Infrequent access storage class (128 KB and 30 days after the creation date)
  - Archive to the glacier storage class (30 days after IA, if relevant)
  - Permanently Delete
- CloudFront Edge Location - This is the location where content will be cached. This is seperate to an AWS Region/AZ
- Origin - This is the origin of all the files that CDN will distribute. This can be either an S3 Bucket, an EC2 instance, an elastic load balancer or Route 53
- 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
- Edge locations are not just READ only, you can write to them too. (i.e. put an objects on to them)
- Objects are cached for the life of TTL
- You can clear cached objects, but you will be charged.
- By default, all newly created buckets are PRIVATE
- You can setup access controls to your buckets using:
  - Bucket Policies
  - Access Control Lists
- S3 Buckets can be configured to create access logs which log all requests made to the S3 Bucket. This can be done to another bucket.
- Encryption (Read encryption section)

- Storage Gateway (Read Storage Gateway section)
- You can load files to S3 much faster by enabling multipart upload
- I can have 100 S3 buckets per account by default
- Read S3 FAQ before taking the exam. It comes up a LOT!