Identity Access Management and S3

Rahul Daware

April 9, 2019

Contents

1 Identity Access Management 101

IAM allows you to manage users and their level of access to the AWS console. It is important to understand IAM and how it works, both for the exam and for administering a company's AWS account in real life.

1.1 Features of IAM

- Centralised control of your AWS account
- Shared access to your AWS account
- Granular permissions
- Identity Federation (including Active Directory, Facebook, Linkedin etc)
- Multifactor authentication
- Provide temporary access for users/devices and services where necessary
- Allows you to set up your own password rotation policy
- Integrates with many different AWS services
- Supports PCI DSS Compliance

1.2 Key Terminology for IAM

- **Users** - End users such as people, employees of an organization etc.
- **Groups** - A collection of users. Each user in the group will inherit permissions of the group.
- **Policies** - Policies are made up of documents, called policy documents. These documents are in a format called JSON and they five permissions as to what a user/group/role is able to do.
- **Roles** - You create roles and then assign them to AWS resources

2 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.

2.1 Features of S3

- S3 is a universal namespace. That is, names must be unique globally.
- When you upload a file to S3, you will receive HTTP 200 code
- S3 is Object based. Think of objects just as files. Objects consist of the following:
  - Key (this is simply the 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, Torrents
- Tiered Storage Available
- Lifecycle Management
- Versioning

- Encryption
- MFA Delete
- Secure your data using **Access Control Lists** and **Bucket Policies**

2.2 How does data consistency work for S3?

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

2.3 S3 - Guarantees

- Build for 99.99% availability ofr the S3 platform.
- Amazon guarantee 99.9% availability.
- Amazon guarantees 99.999999999% durability for S3 information. (Remember 11 x 9s)

2.4 S3 Storage Classes

- **S3 Standard** : 99.99% availability, 99.99999999999% durability, stored redundantly across multiple devices in multiple facilities, and is designed to sustain the loss of 2 facilities concurrently.
- **S3 - IA(infrequetly 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**: For where you want a lower-cost option for infrequently accessed data, but do not require the multiple availability zone data resilience.
- **S3 - Intelligent Tiering**: Designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead.
- **S3 Glacier**: S3 Glacier is a secure, durable and low-cost storage class for data archiving. You can reliably store any amount of data at costs that are competitive with or cheaper than on-premises solutions. Retrieval times configurable from minutes to hours.
- **S3 Glacier Deep Archive**: S3 Glacier Deep Archive is Amazon S3's lowest cost storage class where a retrieval time of 12 hours is acceptable.