AWS services

1. What is Amazon web services (AWS)?

Amazon Web Services (AWS) is Amazon’s cloud web hosting platform that offers flexible, reliable, scalable, easy-to-use, and cost-effective solutions

1. Amazon S3 service. (globally unique name)

(Simple Storage Service) is a scalable, high-speed, low-cost web-based service designed for online backup and archiving of data and application programs. It allows to upload, store, and download any type of files up to 5 TB in size. This service allows the subscribers to access the same systems that Amazon uses to run its own web sites. The subscriber has control over the accessibility of data, i.e. privately/publicly accessible.

**Buckets**

* Amazon s3 allows people to store objects (files) in “buckets” (directories)
* Buckets must have a globally unique name
* Buckets are defines at the region level
* Nam ing convention: no uppercase, no underscore, 3-36 characters long, not an IP, must start with **lowercase letter or number**

**Objects (files) have a key**

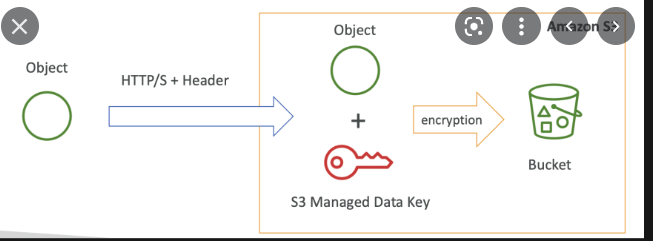
* The key is the Full path: s3://my-bucket/my\_file.txt
* The key is composed of prefix + objectname
* Maximum object size is 5TB (5000Gb)

**Version**

* Enable version your files in Amazon s3 when same key overwrite will increment the “version”:1, 2, 3,…(bucket level)
* It is best practice to version your bucket: protect against unintended deteles (restore a version), roll back to previous version
* **Note:** 
  + Any file that not versioned prior to enabling versioning will have version “null”
  + Suspending versioning does not delete the previous version

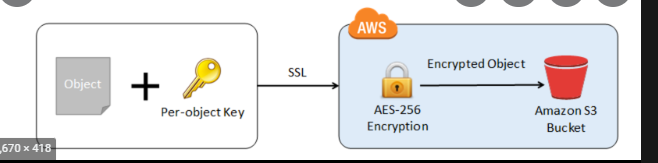
**S3 encryption (mã hóa) for objects (4 methods)**

* Sse-S3: encrypts S3 objects using keys handled & managed by AWS
  + Object is encrypted server side
  + AES-256 encrypion type
  + *Must set header:* “x-amz-server-side-encyption”: “AES256”



We have an object which is unencrypted, and we want to upload it to aws S3 and perform some SSE-SE encryption. To do this, we upload the object on aws s3. We can use HTTP/HTTPS for a call and we can have the header as we set. The services have encryption AES-256, and then aws s3 thanks to this header know to apply the AES in file, you had defined, on top of it. Finally, the object have their own encryption the file will be stored on your own bucket.

* SSE-KMS: leverage AWS key management service to manage encryption keys
* SSE-C: when you want to manage your own encryption keys
  + SSE-C: server-side encrytion using data keys fully managed by the customer outside of AWS
  + AWS S3 doesnot store the encryption key you provide
  + **HTTPS** must be used
  + Encyption key must provided in HTTP headers, for every HTTP request made



* Client side encryption
  + Client library such as the aws s3 encryption client
  + Clients must encrypt data themselves before sending to s3
  + Cleints must decrypt data themselves when retrieving from s3



* Encryption in transit : HTTP endpoint: non encrypted. **HTTPS endpoint**: encryption in flight. That means you are free use the endpoint you want, but HTTPS is recommended because **HTTPS is mandatory for SSE-C**
* **S3 CORS:** an origin is a schema (protocol), host (domain) and port (<https://www.example.com>) port 443 for https, 80 for http
  + CORS means Cross-origin resource sharing
  + Web browse based mechanism to allow requests to other origins while visiting the main origin
  + Same origin: <http://example.com/app1> & <http://example.com/app2>
  + Different origin <http://example.com/app1> & <http://sample.com/app1>

**Multi-Part Upload is recommended as soon as the file is over 100 MB.**

1. Amazon lambda

AWS Lambda is a responsive cloud service that inspects actions within the application and responds by deploying the user-defined codes, known as functions. It automatically manages the compute resources across multiple availability zones and scales them when new actions are triggered.

1. IAM

IAM : Identity and Access Management, Global service

AWS Identity and Access Management (IAM) cung cấp biện pháp kiểm soát quyền truy cập chi tiết trên toàn bộ phạm vi AWS. Với IAM, bạn có thể chỉ định những cá nhân có quyền truy cập, loại dịch vụ và tài nguyên mà họ có thể truy cập và điều kiện truy cập. Với các chính sách IAM, bạn có thể quản lý quyền cho lực lượng lao động và hệ thống của mình để đảm bảo các quyền với đặc quyền tối thiểu nhất.

**IAM User Groups can contain only IAM Users**.

MFA – multi fator authentication

Support for multi tokens on a single device: authentication, authy

IAM roles for services

For EC2 instances or AWS services

IAM sercurity tools: MFA + password security

* IAM credentials report (account level): a report that lists all your account’s users and the status of their variuos credentials
* IAM access advisor (user level): shows the service permissions granted to user and when those sevices were last accessed

Install aws CLI (command line IDE)

**AWS IAM in CLI**

aws –version

aws configure ->Add password, account

aws iam list-users -> list all user in the account (a json file)

Stop user’s permission

Alternative shell : Cloud shell (top of the right aws interfere) using by regions