AWS Certification – Storage & Content Delivery – Cheat Sheet

Elastic Block Store – EBS

- is virtual network attached block storage
- volumes CANNOT be shared with multiple EC2 instances, use EFS instead
- persists and is independent of EC2 lifecycle
- multiple volumes can be attached to a single EC2 instance
- can be detached & attached to another EC2 instance in that same AZ only
- volumes are created in an specific AZ and CANNOT span across AZs
- snapshots CANNOT span across regions
- for making volume available to different AZ, create a snapshot of the volume and restore it to a new volume in any AZ within the region
- for making the volume available to different Region, the snapshot of the volume can be copied to a different region and restored as a volume
- provides high durability and are redundant in an AZ, as the data is automatically replicated within that AZ to prevent data loss due to any single hardware component failure
- PIOPS is designed to run transactions applications that require high and consistent IO for e.g. Relation database, NoSQL etc

S3

- Key-value based object storage with unlimited storage, unlimited objects up to 5 TB for the internet
- is an Object level storage (not a Block level storage) and cannot be used to host OS or dynamic websites (but can work with Javascript SDK)
- provides durability by redundantly storing objects on multiple facilities within a region
- support SSL encryption of data in transit and data encryption at rest
- regularly verifies the integrity of data using checksums and provides auto healing capability
- integrates with CloudTrail, CloudWatch and SNS for event notifications
- S3 resources
  - consists of bucket and objects stored in the bucket which can be retrieved via a unique, developer-assigned key
  - bucket names are globally unique
  - data model is a flat structure with no hierarchies or folders
  - Logical hierarchy can be inferred using the keyname prefix e.g. Folder1/Object1
- Bucket & Object Operations
  - allows retrieval of 1000 objects and provides pagination support and is NOT suited for list or prefix queries with large number of objects
  - with a single put operations, 5GB size object can be

    uploaded
    - use Multipart upload to upload large objects up to 5 TB and is recommended for object size of over 100MB for fault tolerant uploads
    - support Range HTTP Header to retrieve partial objects for fault tolerant downloads where the network connectivity is poor
    - Pre-Signed URLs can also be used shared for uploading/downloading objects for limited time without requiring AWS security credentials
    - allows deletion of a single object or multiple objects (max 1000) in a single call
- Multipart Uploads allows
    - parallel uploads with improved throughput and bandwidth utilization
    - fault tolerance and quick recovery from network issues
    - ability to pause and resume uploads
    - begin an upload before the final object size is known
- Versioning
    - allows preserve, retrieve, and restore every version of every object
    - protects individual files but does NOT protect from Bucket deletion
- Storage tiers
    - Standard
        - default storage class
        - 99.999999999% durability & 99.99% availability

    - Low latency and high throughput performance
    - designed to sustain the loss of data in a two facilities
  - Standard IA
    - optimized for long-lived and less frequently accessed data
    - designed to sustain the loss of data in a two facilities
    - 99.999999999% durability & 99.9% availability
    - suitable for objects greater than 128 KB kept for at least 30 days
  - Reduced Redundancy Storage
    - designed for noncritical, reproducible data stored at lower levels of redundancy than the STANDARD storage class
    - reduces storage costs
    - 99.99% durability & 99.99% availability
    - designed to sustain the loss of data in a single facility
  - Glacier
    - suitable for archiving data where data access is infrequent and retrieval time of several (3-5) hours is acceptable
    - 99.999999999% durability
- allows Lifecycle Management policies
  - transition to move objects to different storage classes and Glacier
  - expiration to remove objects

- Data Consistency Model
  - provide read-after-write consistency for PUTS of new objects and eventual consistency for overwrite PUTS and DELETES
  - for new objects, synchronously stores data across multiple facilities before returning success
  - updates to a single key are atomic
- Security
  - IAM policies – grant users within your own AWS account permission to access S3 resources
  - Bucket and Object ACL – grant other AWS accounts (not specific users) access to S3 resources
  - Bucket policies – allows to add or deny permissions across some or all of the objects within a single bucket
- Data Protection – Pending
- Best Practices
  - use random hash prefix for keys and ensure a random access pattern, as S3 stores object lexicographically randomness helps distribute the contents across multiple partitions for better performance
  - use parallel threads and Multipart upload for faster writes
  - use parallel threads and Range Header GET for faster reads
  - for list operations with large number of objects, its better to build a secondary index in DynamoDB
  - use Versioning to protect from unintended overwrites and deletions, but this does not protect against bucket

        deletion
    - use VPC S3 Endpoints with VPC to transfer data using Amazon internet network

Glacier

- suitable for archiving data, where data access is infrequent and a retrieval time of several hours (3 to 5 hours) is acceptable (Not true anymore with enhancements from AWS)
- provides a high durability by storing archive in multiple facilities and multiple devices at a very low cost storage
- performs regular, systematic data integrity checks and is built to be automatically self healing
- aggregate files into bigger files before sending them to Glacier and use range retrievals to retrieve partial file and reduce costs
- improve speed and reliability with multipart upload
- automatically encrypts the data using AES-256
- upload or download data to Glacier via SSL encrypted endpoints

CloudFront

- provides low latency and high data transfer speeds for distribution of static, dynamic web or streaming content to web users
- delivers the content through a worldwide network of data centers called Edge Locations
- keeps persistent connections with the origin servers so that the files can be fetched from the origin servers as quickly as

possible.

- dramatically reduces the number of network hops that users' requests must pass through
- supports multiple origin server options, like AWS hosted service *for e.g. S3, EC2, ELB* or an on premise server, which stores the original, definitive version of the objects
- single distribution can have multiple origins and Path pattern in a cache behavior determines which requests are routed to the origin
- supports Web Download distribution and RTMP Streaming distribution
  - Web distribution supports static, dynamic web content, on demand using progressive download & HLS and live streaming video content
  - RTMP supports streaming of media files using Adobe Media Server and the Adobe Real-Time Messaging Protocol (RTMP) ONLY
- supports HTTPS using either
  - dedicated IP address, which is expensive as dedicated IP address is assigned to each CloudFront edge location
  - Server Name Indication (SNI), which is free but supported by modern browsers only with the domain name available in the request header
- For E2E HTTPS connection,
  - Viewers -> CloudFront needs either self signed certificate, or certificate issued by CA or ACM
  - CloudFront -> Origin needs certificate issued by ACM

for ELB and by CA for other origins

- Security
    - Origin Access Identity (OAI) can be used to restrict the content from S3 origin to be accessible from CloudFront only
    - supports Geo restriction (Geo-Blocking) to whitelist or blacklist countries that can access the content
    - Signed URLs
        - for RTMP distribution as signed cookies aren't supported
        - to restrict access to individual files, *for e.g., an installation download for your application.*
        - users using a client, *for e.g. a custom HTTP client,* that doesn't support cookies
    - Signed Cookies
        - provide access to multiple restricted files, *for e.g., video part files in HLS format or all of the files in the subscribers' area of a website.*
        - don't want to change the current URLs
    - integrates with AWS WAF, a web application firewall that helps protect web applications from attacks by allowing rules configured based on IP addresses, HTTP headers, and custom URI strings
- supports GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE to get object & object headers, add, update, and delete objects
    - only caches responses to GET and HEAD requests and, optionally, OPTIONS requests

  - does not cache responses to PUT, POST, PATCH, DELETE request methods and these requests are proxied back to the origin
- object removal from cache
  - would be removed upon expiry (TTL) from the cache, by default 24 hrs
  - can be invalidated explicitly, but has a cost associated, however might continue to see the old version until it expires from those caches
  - objects can be invalidated only for Web distribution
  - change object name, versioning, to serve different version
- supports adding or modifying custom headers before the request is sent to origin which can be used to
  - validate if user is accessing the content from CDN
  - identifying CDN from which the request was forwarded from, in case of multiple CloudFront distribution
  - for viewers not supporting CORS to return the Access-Control-Allow-Origin header for every request
- supports Partial GET requests using range header to download object in smaller units improving the efficiency of partial downloads and recovery from partially failed transfers
- supports compression to compress and serve compressed files when viewer requests include Accept-Encoding: gzip in the request header
- supports different price class to include all regions, to

include only least expensive regions and other regions to exclude most expensive regions
- supports access logs which contain detailed information about every user request for both web and RTMP distribution

AWS Import/Export

- accelerates moving large amounts of data into and out of AWS using portable storage devices for transport and transfers data directly using Amazon's high speed internal network, bypassing the internet.
- suitable for use cases with
  - large datasets
  - low bandwidth connections
  - first time migration of data
- Importing data to several types of AWS storage, including EBS snapshots, S3 buckets, and Glacier vaults.
- Exporting data out from S3 only, with versioning enabled only the latest version is exported
- Import data can be encrypted (optional but recommended) while export is always encrypted using Truecrypt
- Amazon will wipe the device if specified, however it will not destroy the device