AWS EBS (ELASTIC BLOCK STORE)

There are two types of block store devices are available for EC2.

1. Elastic Block Store (persistent, network attached virtual drive)
2. Instances Store Backed EC2:
    - Basically the virtual hard drive on the host allocated to this EC2 instance.
    - Limit to 10GB per device
    - Ephemeral storage (non-persistent storage)
    - The EC2 instance can't be stopped, can only be rebooted or terminated. Terminate will delete data.

- EBS volume behaves like RAW, unformatted, external block storage devices that you can attached to your EC2 instance.
- EBS volumes are block storage devices suitable for database style data that requires frequent reads and writes.
- EBS volumes are attached to your EC2 instances through the AWS network, like virtual hard drive.
- An EBS volume can attach to a single EC2 instances only at a time.
- Both EBS volumes and EC2 instances must be in the same AZ.
- An EBS volume data is replicated by AWS across multiple servers in the same AZ to prevent data loss resulting from any single AWS component failure.

EBS Volume Types:

1. SSD backed volume
2. HDD backed volume
3. Magnetic standard

SSD backed volume is also two types:

A. General purpose SSD (GP2)
B. Provisioned IOPS SSD (io1)

HDD backed volume is also two types:

A. Throughput optimized HDD (st1)
B. Cold HDD (SC1)

A. General Purposed SSD (gp2)

- GP2 is the default EBS volume type for the amazon EC2 instance.
- GP2 volumes are backed by SSDs.
- General purpose balances both price and performances.
- Ratio of 3IOPS/GB with up to 10,000 IOPS.
- Boot volume having low latency.
- Volume size: 1 GB to 16 GB.
- Price: $0.10/ GB/month

B. Provisioned IOPS SSD (io1)

- These volumes are ideal for both IOPS intensive and throughput intensive workloads that requires extremely low latency or for mission critical applications.
- Designed for I/O intensive applications such as large relational or NoSQL databases.
- Use if you need more than 10,000 IOPS.
- Can provision up to 32,000 IOPS per volume.
- Volume size: 4GB to 16TB
- Price : $ 0.125/GB/month

C. Throughput optimized HDD (st1)

- ST1 is backed by hard disk drives and is ideal for frequently accessed, throughput intensive workloads with large datasets.
- ST1 volumes deliver performance in term of throughput, measured in MB/S.
- Big data, data warehouse, log processing.
- It cannot be a boot volume.
- Can provisioned up to 500 IOPS per volume.
- Volume size: 500GB to 16 TB
- Price: $0.045/GB/month

D. Cold HDD (SC1)

- SC1 is also backed by HDD and provides the lowest cost per GB of all EBS volume types.
- Lowest cost storage for infrequent access workloads.
- Used in file servers.

- Cannot be a boot volume.
- Can provisioned up to 250 IOPS per volume.
- Volume size: 500 GB to 16TB
- Price: $0.025/GB/Month

Magnetic Standard:

- Lowest cost per GB of all EBS volume type that is bootable.
- Magnetic volumes are ideal for workloads where data is accessed infrequently and applications where the lowest storage cost is important.
- Price: $0.05/GB/month
- Volume size: 1GB to 1TB
- Max IOPS/volume: 40-200

EBS Snapshot of Root Volume and Non-root Volume:

- EBS snapshots are point-in-time images/copies of your EBS volume.
- Any data written to the volume after the snapshot process is initiated, will not be included in the resulting snapshot (but will be included in future incremental update.)
- Per AWS account up to 5000 EBS volumes can be created.
- Per account up to 10,000 EBS snapshots can be created.
- EBS snapshots are stored on S3, however you cannot access them directly. You can only access them through EC2 APIs.
- While EBS volumes are AZ specific, snapshots are region specific.
- Any AZ in region can use snapshot to create EBS volume.
- To migrate an EBS from one AZ to another, create a snapshot (region specific) and create an EBS volume from the Snapshot in the intended AZ.
- You can create a snapshot to an EBS volume of the same or larger size than the original volumes size from which the snapshot was initially created.

- You can take a snapshot of a non-root EBS volume while the volumes is in use on a running EC2 instance.
- This means, you can still access it while the snapshot is being processed.
- However the snapshot will only include data that is already written to your volume.
- The snapshot is created immediately but it may stay in pending status until the full snapshot is completed. This may takes few hours to complete specially for the first time snapshot if a volume.
- During the period when the snapshot status is pending you can still access the volume (non-root) but I/O might be slower because of the snapshot activity.

- While in pending state, an in progress snapshot will not include data from ongoing reads and writes to the volume.
- To take complete snapshot of your non-root EBS volume: stop of unmounts the volume.
- To create a snapshot for a root EBS volume you must stop the instance first then take the snapshot.

Incremental Snapshot:

- EBS snapshots are stored incrementally.
- For low cost storage on S3 and a guarantee to be able to able fully restore data from the snapshot.
- What you need is a single snapshot then further snapshot will only carry the changed blocks (incremental updates).
- Therefore you do not need to have multiple full/complete copies of the snapshot.
- You are charged for:
    - Data transferred to S3 from your EBS volume you are taking snapshot.
    - Snapshot stored in S3.
    - First snapshot is a clone, subsequent snapshots are incremental.
    - Deleting snapshot will only remove data exclusive to that snapshot.

EBS Encryption:

- EBS encryption is supported on all EBS volume types and all EC2 instance families.
- Snapshots of encrypted volumes are also encrypted.
- Creating an EBS volume from an encrypted snapshot will result in an encrypted volume.
- Data encryption at rest means encrypting data while it is stored on the data storage device.
- There are many ways you can encrypt data on an EBS volume at rest, while the volume is attached to an EC2 instance:
    - Use 3rd party EBS volume
    - Encryption tods.
    - Use encrypted EBS volumes.
    - Use encrypted at the O.S level.

- Encrypt data at the application level before storing it to the volume.
- Use encrypt file system on the top of the EBS volume.
- Encrypt volume area accessed exactly like unencrypted ones, basically encryption is handled transparently.
- You can attach an encrypted and unencrypted volumes to the same EC2 instance.
- Remember that the EBS volumes area not physically attached to the EC2 instance, rather they are virtually attached through the EBS infrastructure.

- This means when you encrypt data on an EBS volume data is actually encrypted on the EC2 instance then transferred, encrypted to be stored on the EBS volume.
- This means data in transit between EC2 and encrypted EBS volume is also encrypted.
- There is no direct way to change the encryption state of the volume.
- To change the state you need to follow either of the following two ways:
    - Attach a new encrypted EBS volume to the EC2 instance that has the data to be encrypted.
    - Mount the new volume to the EC2 instance.
    - Copy the data for the un-encrypted volume to the new volume.
    - Both volumes must be on the same EC2 instance.

Or

- Create a snapshot of the unencrypted volume.
- Copy the snapshot and choose encryption for the new copy, this will create an encrypted copy of the snapshot.
- Use this new copy to create an EBS volume which will be encrypt too.
- Attach the new encrypted EBS volume to the EC2 instance.

Root EBS Volume Encryption:

- There is no direct way to change the encryption state of a volume.
- There is an indirect work around to this:
    - Launch the instance with the EBS volume required.
    - Do whatever patching of install applications.
    - Create an AMI from the EC2 instance.
    - Copy the AMI and choose encryption while copying.
    - This results it an encrypted AMI that is private (yours only).
    - Use the encrypted AMI to launch new EC2 instances which will have their EBS root volume3 encrypted.

EBS Encryption Key:

- To encrypt a volume or snapshot, you need an encryption key, these keys are called customer master key (CMK) and are managed by AWS key management service (KMS).
- When encrypting the first EBS volume, AWS KMS creates a default CMK key.
- This key is used for your first volume encryption of snapshots created from this volumes and subsequent volumes created from these snapshots.

- After that each newly encrypted volume is encrypted with a unique/ separate AES-256 bit encryption key. This key is used to encrypt the volume, its snapshot and any volumes created of its snapshots.

Changing Encryption Key:

- You cannot change the encryption (CMK) key used to encrypt an existing encrypted snapshot or encrypted EBS volume.
- If you want to change the key, create a copy of the snapshot and specify during the copy process that you want to re-encrypt the copy with a different key.
- This comes in handy when you have a snapshot that was encrypted using your default CMK key and you want to change the key in order to able to share the snapshot with other accounts.

Sharing EBS Snapshot:

- By default only the account owner can create volumes from the account snapshots.
- You can share your unencrypted snapshots with the AWS community by making them public.
- Also you can share your unencrypted snapshots with a selected AWS account by making them private then selecting the AWS accounts to share with.
- You cannot make your encrypted snapshots public.
- You cannot make a snapshot of an encrypted EBS volume public on AWS.
- You can share your encrypted snapshot with specific AWS account as follows:
    - Make sure that you use a non-default/custom CMK key to encrypt the snapshot, not the default CMK key (AWS will not allow the sharing if default CMK is used.)
    - Configure cross account permissions in order to give the account with which you want to share the snapshot access to the custom CMK key used to encrypt the snapshot.
    - Without this the other account will not be able to copy the snapshots nor will be able to create volumes of the snapshots.
- AWS will not allow you to share snapshots encrypted using your default CMK key.
- For the AWS account with whom an encrypted snapshot is shared.
    - They must first create their own copies of the snapshot.
    - Then they use that copy to restore/create EBS volume.
- You can make a copy of the snapshot when it has been fully saved to S3 (its status show as complete) and not during the snapshot's pending status (when data blocks are being moved to S3).
- Amazon S3 server side encryption (SSE) protect the snapshot data-in-transit while copying.
- You can have up to 5 snapshots copy request running in a single destination per account.