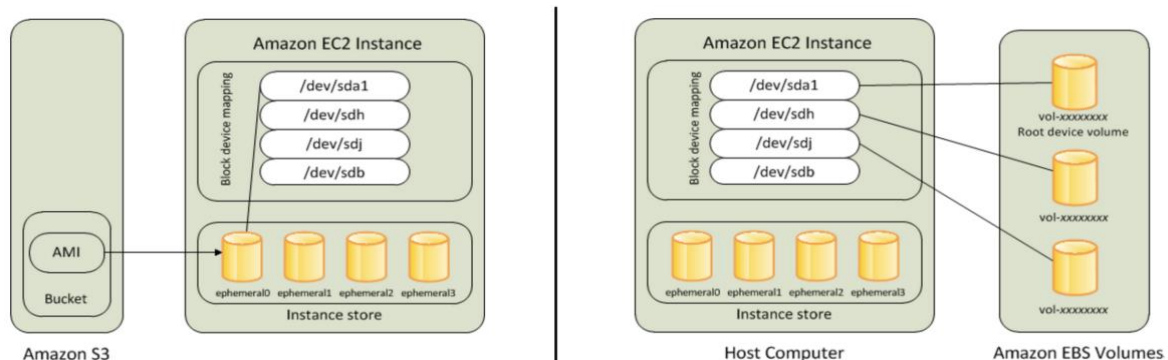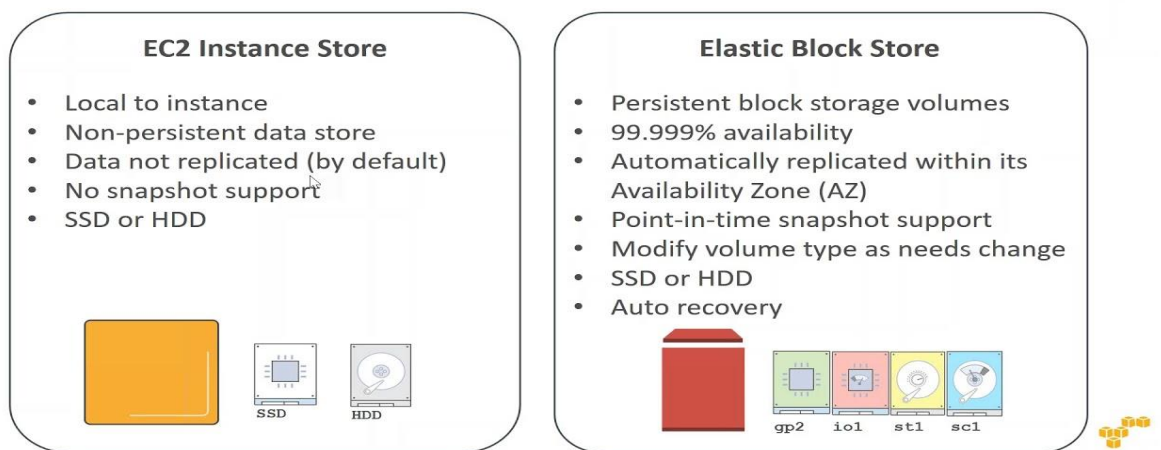# ELASTIC BLOCK STORE (EBS)

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

1. **Elastic Block Store** (persistent, network attached virtual drive, Block Access)
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.

EC2 Instance Store vs EBS

EC2 Instance Store
- Local to instance
- Non-persistent data store
- Data not replicated (by default)
- No snapshot support
- SSD or HDD

SSD   HDD

Elastic Block Store
- Persistent block storage volumes
- 99.999% availability
- Automatically replicated within its Availability Zone (AZ)
- Point-in-time snapshot support
- Modify volume type as needs change
- SSD or HDD
- Auto recovery

gp2   io1   st1   sc1

Amazon EC2 Instance

Block device mapping
/dev/sda1
/dev/sdh
/dev/sdj
/dev/sdb

AMI
Bucket

ephemeral0 ephemeral1 ephemeral2 ephemeral3
Instance store

Amazon S3

Amazon EC2 Instance

Block device mapping
/dev/sda1
/dev/sdh
/dev/sdj
/dev/sdb

ephemeral0 ephemeral1 ephemeral2 ephemeral3
Instance store

Host Computer

vol-xxxxxxxx
Root device volume

vol-xxxxxxxx

vol-xxxxxxxx

Amazon EBS Volumes

❖ EBS volume Types:

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

1. **SSD backed volume is also two types:**

   a. General purpose SSD (GP2, GP3)
   b. Provisioned IOPS SSD (io1, io2)

2. **HDD backed volume is also two types:**

   a. Throughput optimized HDD (st1)
   b. Cold HDD (SC1)

	General Purpose SSD		Provisioned IOPS SSD		
Volume type	gp3	gp2	io2 Block Express ‡	io2	io1
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.999% durability (0.001% annual failure rate)	99.999% durability (0.001% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	• Low-latency interactive apps • Development and test environments		Workloads that require: • Sub-millisecond latency • Sustained IOPS performance • More than 64,000 IOPS or 1,000 MiB/s of throughput	• Workloads that require sustained IOPS performance or more than 16,000 IOPS • I/O-intensive database workloads	
Volume size	1 GiB - 16 TiB		4 GiB - 64 TiB	4 GiB - 16 TiB	
Max IOPS per volume (16 KiB I/O)	16,000		256,000	64,000 †	
Max throughput per volume	1,000 MiB/s	250 MiB/s *	4,000 MiB/s	1,000 MiB/s †	
Amazon EBS Multi-attach	Not supported		Supported		
Boot volume	Supported				

❖ SSD backed volume is also two types:

A. General Purposed SSD (Gp2, GP3): -

➢ 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, io2): -

➢ 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

❖ HDD backed volume is also two types:
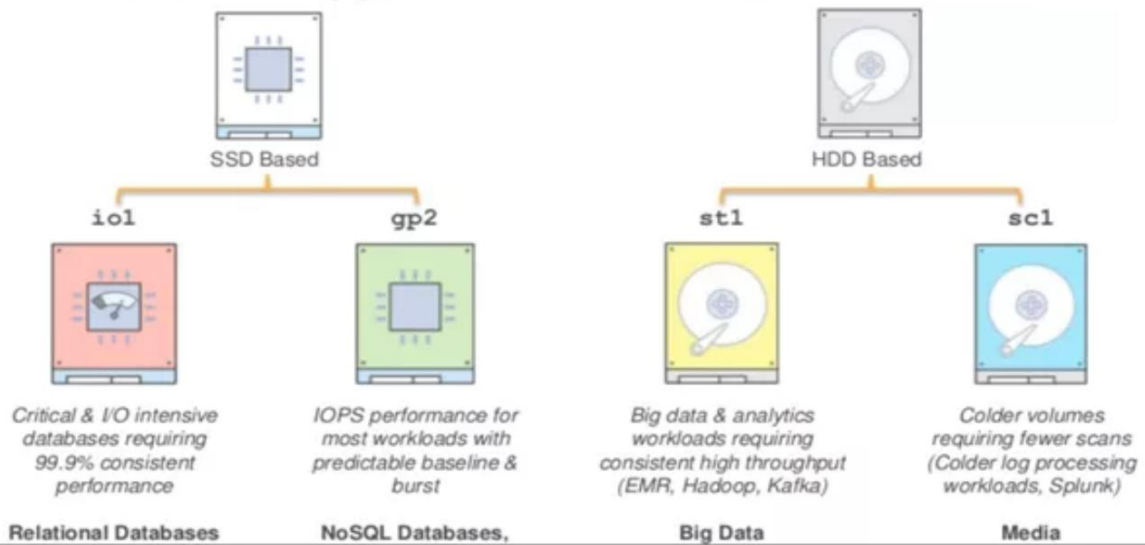
A) Throughput optimized HDD (st1)

➢ 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

B) 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

	Throughput Optimized HDD	Cold HDD
Volume type	st1	sc1
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	• Big data • Data warehouses • Log processing	• Throughput-oriented storage for data that is infrequently accessed • Scenarios where the lowest storage cost is important
Volume size	125 GiB - 16 TiB	125 GiB - 16 TiB
Max IOPS per volume (1 MiB I/O)	500	250
Max throughput per volume	500 MiB/s	250 MiB/s
Amazon EBS Multi-attach	Not supported	Not supported
Boot volume	Not supported	Not supported

❖ 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
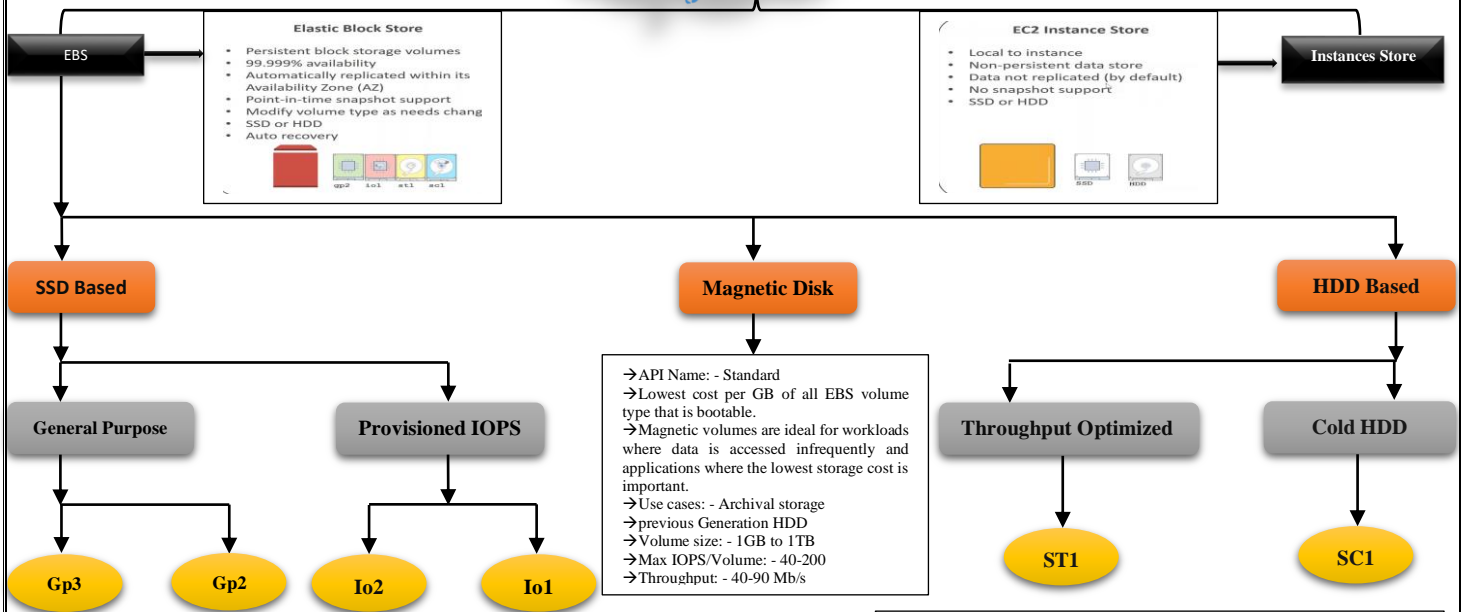➢ Volume size: 1GB to 1TB
➢ Max IOPS/volume: 40-200

	Solid State Drives (SSD)		Hard Disk Drives (HDD)		
Volume Type	General Purpose	Provisioned IOPS SSD	Throughput Optimized HDD	Cold HDD	EBS Magnetic
API Names	gp2	io1	st1	sc1	standard
Description	Balances price and performance	Highest SSD performance for Mission-critical low latency or high throughput	Low-cost. Designed for frequently accessed, throughput intensive workloads	Lowest HDD cost. Less frequently used workloads	
Use Cases	Most Workloads	Large Databases IOPS greater than 16,000 or Throughput greater than 250 MiB	Data Warehouses Big Data Log Processing	File Storage	Archival Storage
Volume Size	1GiB - 16TiB	4GB - 16 TiB	500GiB - 15TiB	500GiB - 15TiB	500GiB - 15TiB
Max IOPS	16,000	64,000	500	250	40-200

1. **General Purpose (SSD)** (gp2) for general usage without specific requirements
2. **Provisioned IOPS (SSD)** (io1) when you require really fast input & output
3. **Throughput Optimized HDD** (st1) magnetic drive optimised for quick throughput
4. **Cold HDD** (sc1) Lowest cost HDD volume for infrequently access workloads
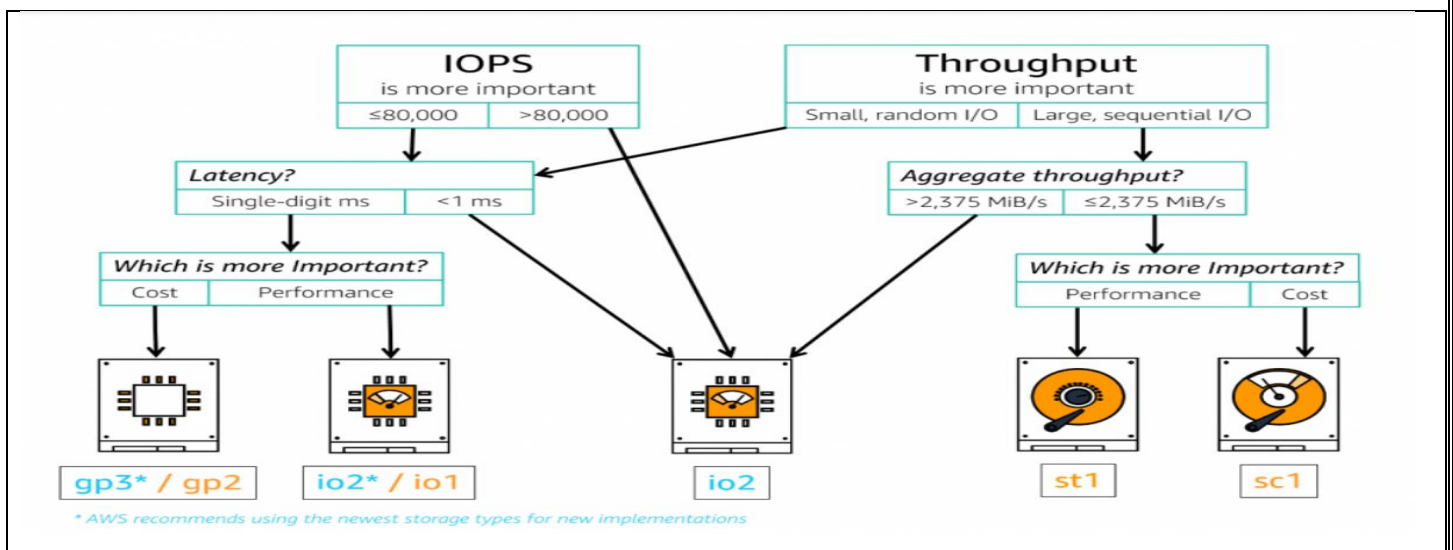5. **EBS Magnetic** (standard) previous generation HDD

[AMAZONE WEB SERVICES – 5-EBS]

Block Store Device

EBS

Elastic Block Store
- Persistent block storage volumes
- 99.999% availability
- Automatically replicated within its Availability Zone (AZ)
- Point-in-time snapshot support
- Modify volume type as needs chang
- SSD or HDD
- Auto recovery

gp2 io1 st1 sc1

EC2 Instance Store
- Local to instance
- Non-persistent data store
- Data not replicated (by default)
- No snapshot support
- SSD or HDD

SSD HDD

Instances Store

SSD Based

Magnetic Disk
- → API Name: - 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.
- → Use cases: - Archival storage
- → previous Generation HDD
- → Volume size: - 1GB to 1TB
- → Max IOPS/Volume: - 40-200
- → Throughput: - 40-90 Mb/s

HDD Based

General Purpose

Provisioned IOPS

Throughput Optimized

Cold HDD

Gp3 **Gp2** **Io2** **Io1**

ST1 **SC1**

Volume type	General Purpose SSD		Provisioned IOPS SSD		
	gp3	gp2	io2 Block Express ‡	io2	io1
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.999% durability (0.001% annual failure rate)	99.999% durability (0.001% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	• Low-latency interactive apps • Development and test environments		Workloads that require: • Sub-millisecond latency • Sustained IOPS performance • More than 64,000 IOPS or 1,000 MiB/s of throughput		• Workloads that require sustained IOPS performance or more than 16,000 IOPS • I/O-intensive database workloads
Volume size	1 GiB - 16 TiB		4 GiB - 64 TiB		4 GiB - 16 TiB
Max IOPS per volume (16 KiB I/O)	16,000		256,000		64,000 †
Max throughput per volume	1,000 MiB/s	250 MiB/s *	4,000 MiB/s		1,000 MiB/s †
Amazon EBS Multi-attach	Not supported		Supported		
Boot volume	Supported				

Volume type	Throughput Optimized HDD	Cold HDD
	st1	sc1
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	• Big data • Data warehouses • Log processing	• Throughput-oriented storage for data that infrequently accessed • Scenarios where the lowest storage cost is important
Volume size	125 GiB - 16 TiB	125 GiB - 16 TiB
Max IOPS per volume (1 MiB I/O)	500	250
Max throughput per volume	500 MiB/s	250 MiB/s
Amazon EBS Multi-attach	Not supported	Not supported
Boot volume	Not supported	Not supported

IOPS is more important
≤80,000   >80,000

Throughput is more important
Small, random I/O   Large, sequential I/O

Latency?
Single-digit ms   <1 ms

Aggregate throughput?
>2,375 MiB/s   ≤2,375 MiB/s

Which is more Important?
Cost   Performance

Which is more Important?
Performance   Cost

gp3* / gp2   io2* / io1   io2   st1   sc1

AWS recommends using the newest storage types for new implementations

❖ 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 take 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.

➢ Any data cached by the OS or in memory, will not be included, which means the snapshot will not be 100% consistent.

➢ You can remount the volume while the snapshot status pending (being processed)
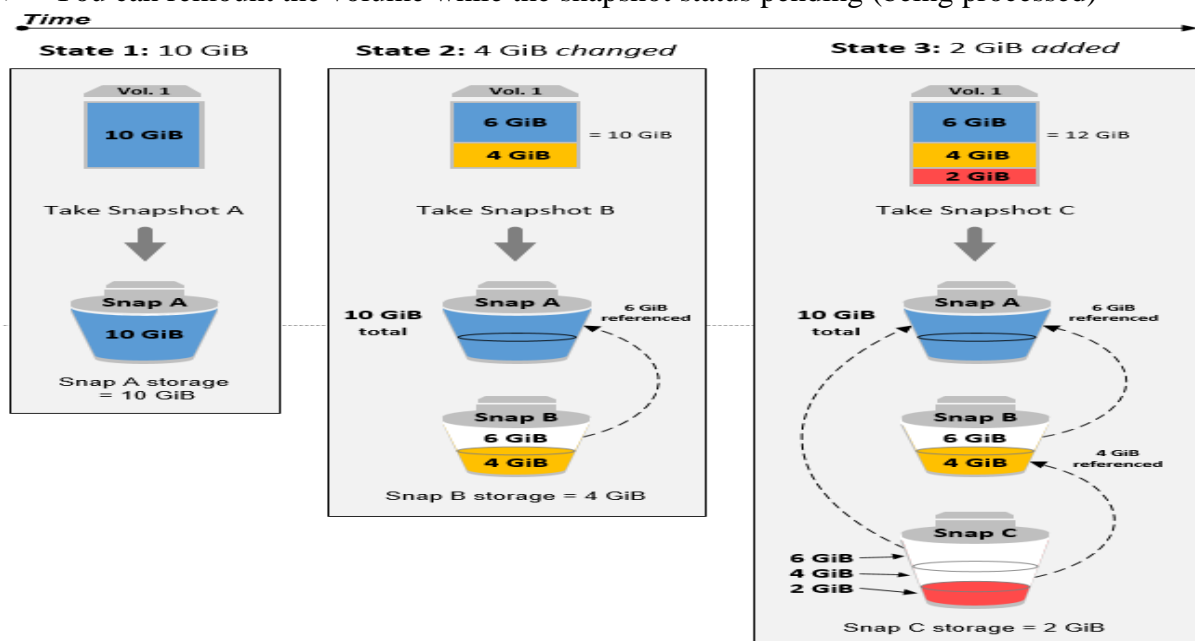
❖ Incremental Snapshot:

- ➤ 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.

❖ Delete snapshot
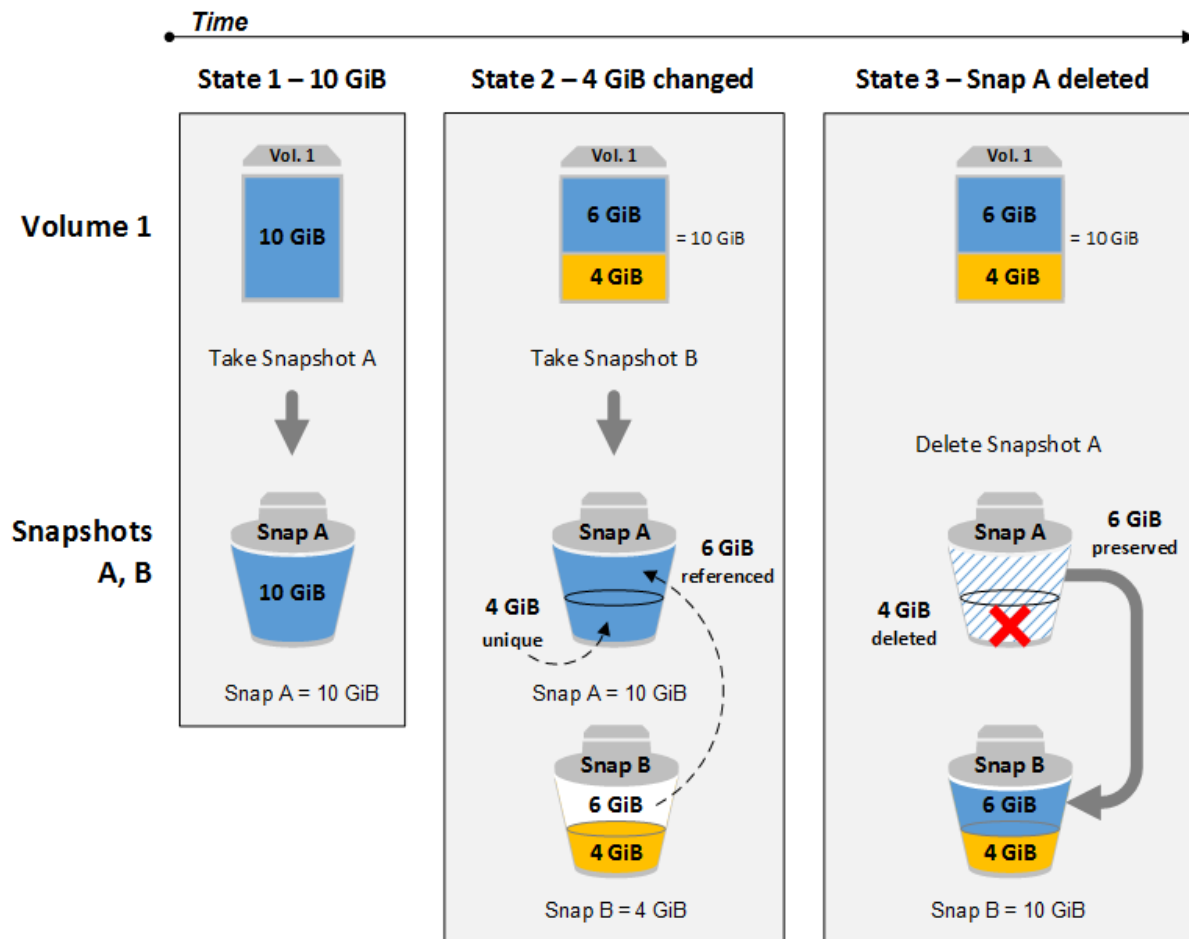
- **To migrate and EBS from one AZ to another AZ**
  - ➤ Create a snapshot (region specific)
  - ➤ Create an EBS volume from the snapshot in the intended AZ i.e., other AZ

- **To Migrate an EBS from one region to another Region**
  - ➤ Create a snapshot of the volume
  - ➤ Copy the snapshot and specify the new region
  - ➤ In the new region, create a volume out of the copied 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 encrypts 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 but the instance has to support encrypted volumes (earlier few instances did not had support of encryption)

➢ 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.
- 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.
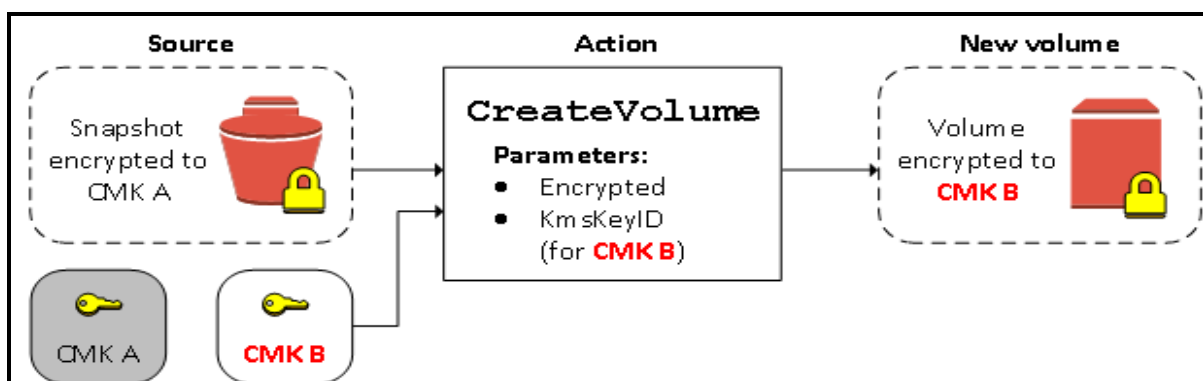
❖ EBS Encryption -At Rest

➤ Data encryption at rest means encrypting data while its 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 third party encryption tools/software for EBS volume (SSD or HDD).
➤ Use encrypted EBS volumes
➤ Use encryption at the OS level (using data encryption plugins/drivers).
➤ Encrypt data at the application level before storing to the volume.
➤ Use encrypted file system in top of the EBS volume.

❖ EBS Encryption -Data in Transit

➤ When you encrypt data on an EBS volume, data is actually encrypted on the EC2 instance then transferred to store it on the EBS volume.
➤ So, data transit between EC2 and Encrypted EBS volume is also encrypted.

❖ 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 these 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.
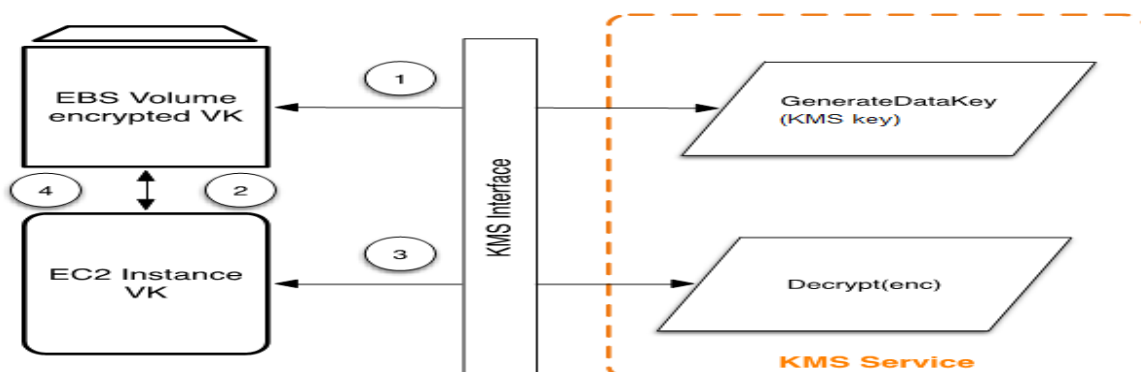
❖ Changing Encryption Key:

➢ 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.

➢ When you share your snapshot of a volume you are actually sharing all the data on that volume used to create the snapshot.

➢ 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.
- Mark the snapshoot private then enter the AWS account with which you want to share 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.

❖ Copying EBS Snapshots

➢ If you try to copy an encrypted snapshot without having permissions to the encryption key, the copy process will "fail silently"

➢ So, you cannot create EBS volumes from encrypted snapshot without having permissions to the encryption key

➢ Use cases of coping snapshots:

- Geographic expansionS
- Disaster Recovery
- Migrating to another region
- Encryption (of unencrypted volumes)
- Data retention and auditing requirement