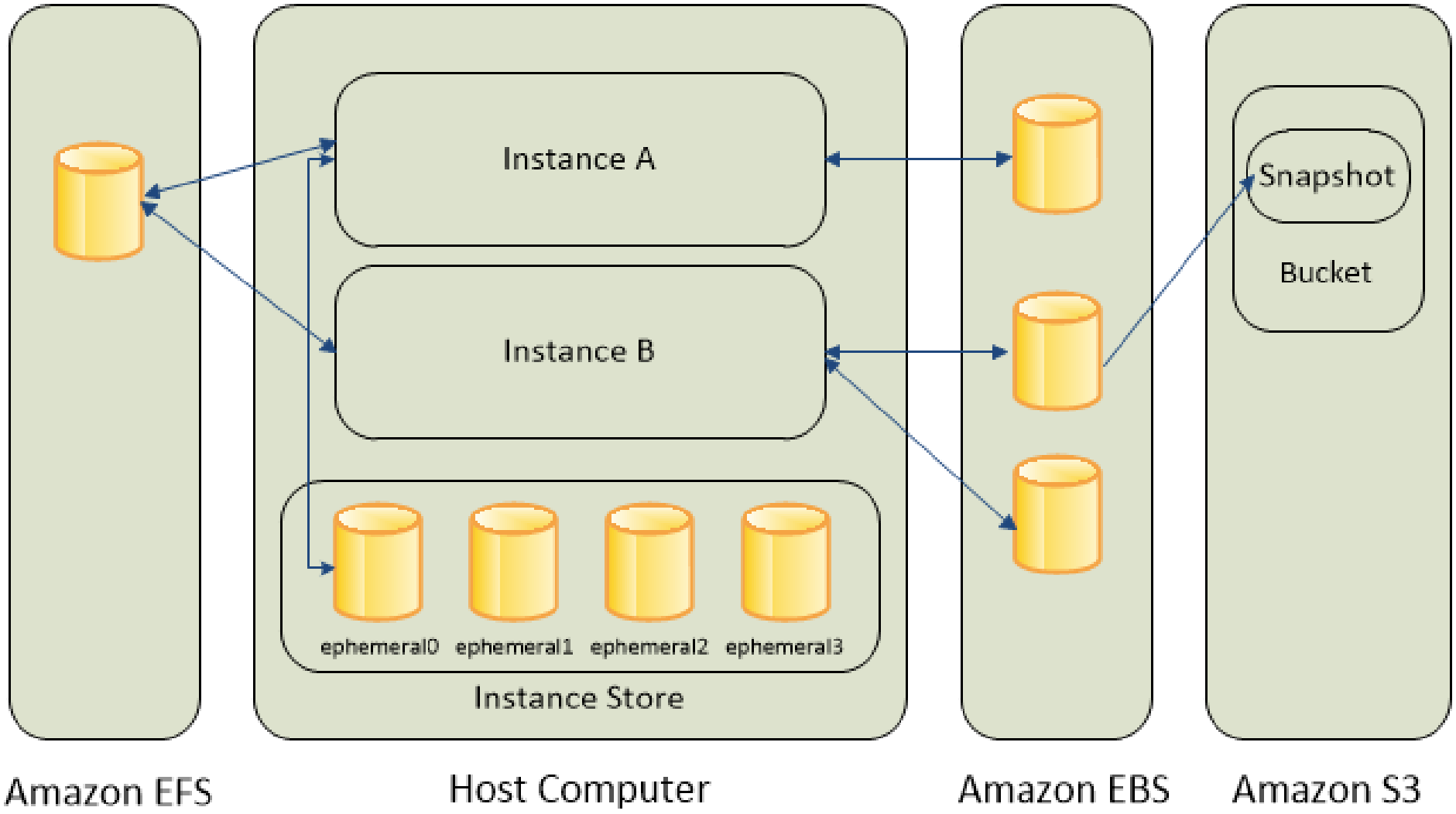
EC2 Elastic Block Storage

- EC2 Elastic Block Storage – EBS Overview
- EBS Volume Example
- EBS Volume Types
- EBS vs Instance Store
- IOPS Performance Instance Store vs. EBS
- EBS Encryption
- EBS Encryption Support
- EBS Snapshot
- How incremental snapshots work
- EBS Snapshot creation
- EBS Snapshot Encryption Create/Attach/Detach/Delete EBS volumes

EC2 Elastic Block Storage – EBS Overview

- An EBS (Elastic Block Store) Volume is a network drive you can attach to your instances while they run
- Amazon EBS provides highly available, reliable, durable, block-level storage volumes that can be attached to a running instance
- It's a network drive (i.e. **not a physical drive**)
  - It uses the aws network to communicate the instance, which means there might be a bit of latency
  - It can be detached from an EC2 instance and attached to another one quickly
- It's locked to an **Availability Zone** (AZ)
  - An EBS Volume in us-east-1a cannot be attached to us-east-1b
  - To move a volume across, you first need to snapshot it
- Have a **provisioned capacity** (size in GBs, and IOPS)
  - You get billed for all the provisioned capacity
  - You can increase the capacity of the drive over time

EBS Volume Example



EBS Volume Types

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html
- **Solid state drives (SSD)**
  - Purpose SSD (gp3, gp2)
    - Provides a balance of price and performance.
    - Recommend these volumes for most workloads.
  - Provisioned IOPS SSD (io2, io1)
    - Provides high performance for mission-critical, low-latency, or high-throughput workloads.
- **Hard disk drives (HDD)**
  - Throughput Optimized HDD (st1)
    - A low-cost HDD designed for frequently accessed, throughput-intensive workloads.
  - Cold HDD (sc1)
    - The lowest-cost HDD design for less frequently accessed workloads.
- **Previous generation volume types**
  - Magnetic (standard)
    - Workloads where data is infrequently accessed

EBS vs Instance Store

- Some instance do not come with Root EBS volumes
- Instead, they come with “Instance Store” (= ephemeral storage)
- Instance store is physically attached to the machine (EBS is a network drive)
- Pros:
  - Better I/O performance (EBS gp2 has an max IOPS of 16000, io1 of 64000)
  - Good for buffer / cache / scratch data / temporary content
  - Data survives reboots
- Cons:
  - On stop or termination, the instance store is lost
  - You can’t resize the instance store
  - Backups must be operated by the user

IOPS Performance Instance Store vs. EBS

- Use Instance Store instead of EBS if very high IOPS rate is required
  - Instance store, although can not provide for data persistence, but it can provide for much higher IOPS compared to, network attached, EBS storage

EBS Encryption

- You can encrypt both the boot and data volumes of an EC2 instance
- When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:
  - Data at rest inside the volume
  - All data moving between the volume and the instance
  - All snapshots created from the volume
  - All volumes created from those snapshots

EBS Encryption Support

- Supported volume types
  - All EBS volume types.

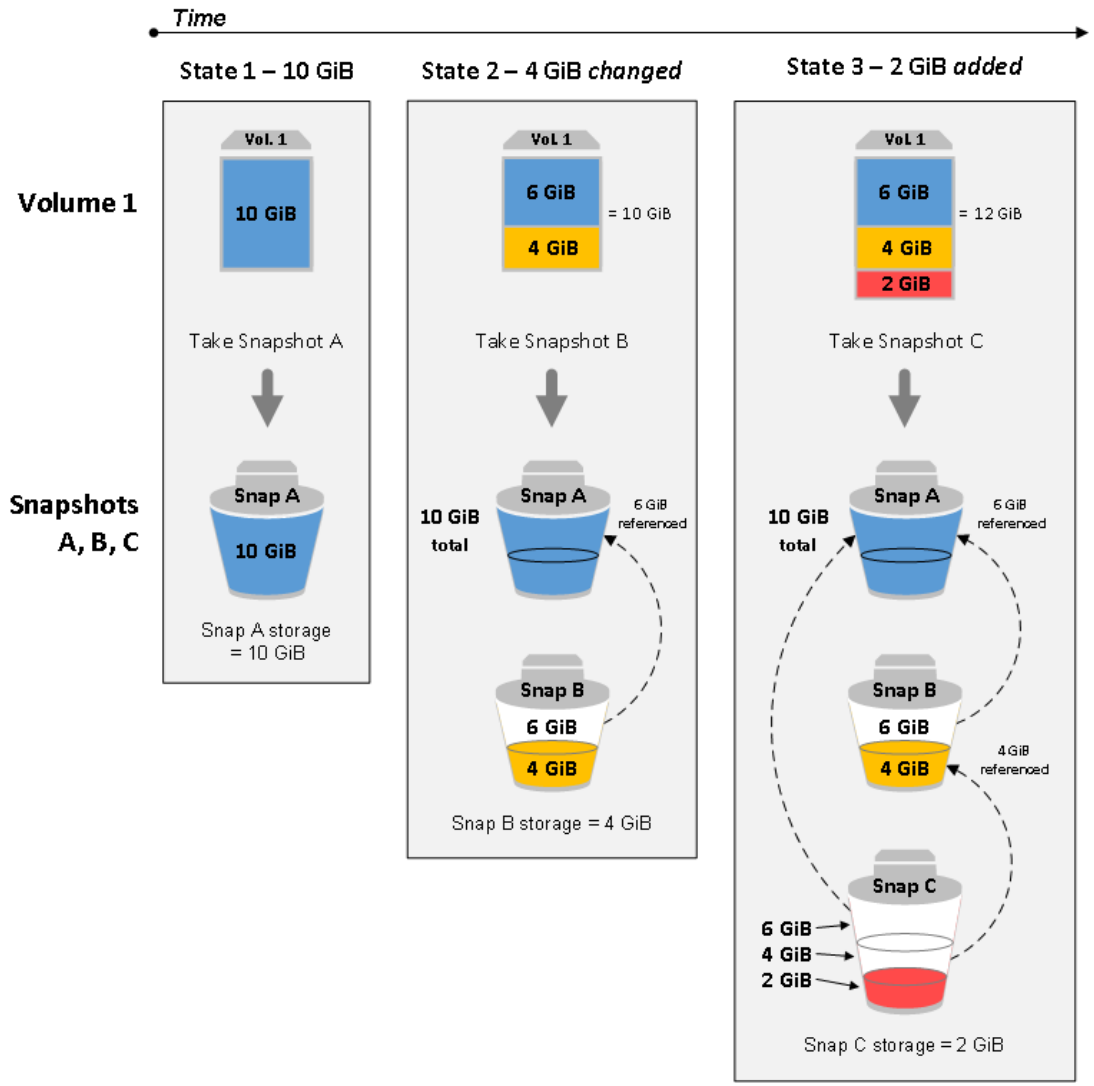
- Supported instance types
  - Amazon EBS encryption is available on
    - All current generation instance types
    - Previous generation instance types: **A1, C3, cr1.8xlarge, G2, I2, M3, and R3**.

- Demo

EBS Snapshot

- EBS provides the ability to create snapshots (backups) of any EBS volume and write a copy of the data in the volume to S3, where it is stored redundantly in multiple Availability Zones
- Snapshots can be used to create new volumes, increase the size of the volumes or replicate data across Availability Zones
- Snapshots are incremental backups and store only the data that was changed from the time the last snapshot was taken.
- Snapshots size can probably be smaller then the volume size as the data is compressed before being saved to S3
- Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot in order to restore the volume.
- EBS Snapshots can be used to migrate or create EBS Volumes in different AZs or regions.

How incremental snapshots work



EBS Snapshot creation

- Snapshots can be created from EBS volumes periodically and are point-in-time snapshots.
- Snapshots are **incremental** and only store the blocks on the device that changed since the last snapshot was taken
- Snapshots occur **asynchronously**; the point-in-time snapshot is created immediately while it takes time to upload the modified blocks to S3
- Recommended ways to create a Snapshot from an EBS volume are
  - Pause all file writes to the volume
  - Unmount the Volume -> Take Snapshot -> Remount the Volume
  - Stop the instance – Take Snapshot (for root EBS volumes)

EBS Snapshot Encryption

- EBS snapshots fully support EBS encryption.
- Snapshots of encrypted volumes are automatically encrypted
- Volumes created from encrypted snapshots are automatically encrypted
- All data in flight between the instance and the volume is encrypted
- Unencrypted snapshot you own, can be encrypted during the copy process
- Encrypted snapshot that you own or have access to, can be encrypted with a different key during the copy process.

Create/Attach/Detach/Delete EBS volumes (Demo)

- Methods of creating a volume
  - Create and attach EBS volumes when you launch instances by specifying a block device mapping.
  - Create an empty EBS volume and attach it to a running instance.
  - Create an EBS volume from a previously created snapshot and attach it to a running instance.
- Detach an Amazon EBS volume from an instance
- Delete an Amazon EBS volume