EBS

#3 General

- Volume is raw block storage
- You can mount EBS Volume to only one instance at a time. Use EFS if you need shared.
- Availablity Zone specific, you can only attach to EC2 instance in the same AZ
- Can be copied (using snapshots)
- Can be encrypted
- MAX 16TB!!!

Volumes – Availability Zone

- Raw Block storage, no file system just bytes :-). Have to formated
- Can be attached/detached while EC2 is running
- Volumes that are created from encrypted snapshots are automatically encrypted, and volumes that are created from unencrypted snapshots are automatically unencrypted. If no snapshot is selected, you can choose to encrypt the volume.
- You can't change CMK of the volume or snapshot - you have to copy

To encrypt unencrypted volume (root):
- Stop the instance
- Create Snapshot
- Copy Snapshot & Encrypt
- Create Volume from encrypted snapshot (same AZ!!!)
- Detach old volume
- Attach new volume (/dev/xvda)
- Delete old ones
- Result

EBS Volume Types
- General Purpose SSD - GP2 - 3 IOPS per GB, burst up to 3000 PS
- Provisioned IOPS SSD - IO1 - IO intensive, use if need more than 10,000 IOPS, mp burst
- Throuput Optimized HDD - ST1 - Big Data, Log Processing, Magnetic drive, can't be boot volume
- Cold HDD storage - SC1 - low cost, infrequently accessed, can't be boot
- Magnetic (Standard) - Low cost per gigabyte, for infrequent access, bootable

- You can create IAM policy to enforce encryption
- You have to detach to delete.
- You can change volume:
    - size
    - type (SSD to Provisioned)
    - IOPS provisioned

Encryption
    - happens on EC2 instance
    - symetric AES-256
    - Encryption is supported on all EBS Volume Types
    - Encryption is supported on specific Instance Types (most new ones). Requires AES cpu instructions
    - No performance difference between encrypted and unencrypted
    - Key per volume
    - Any snapshots of this volume and any subsequent volumes created from those snapshots also share that key
    - You can't change volume or snapshot key, but you can do that when copy

Snapshots – Regional

- Can be tagged after is created, not during creation time
- Point in time snapshots of EBS volume
- Backed up by S3
- Can be encrypted
- Encrypted snapshot can't be public
- You can share encrypted snapshots with specific account
    - use CMK (customer key)
    - give access to customer key to specific account
    - crate snapshot
    - give specific account access to snapshot
- When you create a snapshot of a Throughput Optimized HDD (st1) or Cold HDD (sc1) volume, performance may drop as far as the volume's baseline value while the snapshot is in progress. This behavior is specific to these volume types
- For other that st1 and sc1 volume types an in-progress snapshot is not affected by ongoing reads and writes to the volume.

RAID

- RAID 0 - performance
- RAID 1 - fault tolerance
- RAID 5 - not recomended because of parity