EBS, EBS Volumes and EBS Snapshots

- An Amazon EBS volume is a durable, block-level storage device that you can attach to your instances. After you attach a volume to an instance, you can use it as you would use a physical hard drive.
- EBS volumes are flexible. For current-generation volumes attached to current-generation instance types, you can dynamically increase size, modify the provisioned IOPS capacity, and change volume type on live production volumes.
- You can use EBS volumes as primary storage for data that requires frequent updates, such as the system drive for an instance or storage for a database application.
- You can also use them for throughput-intensive applications that perform continuous disk scans. EBS volumes persist independently from the running life of an EC2 instance.
- You can attach multiple EBS volumes to a single instance. The volume and instance must be in the same Availability Zone.
- Depending on the volume and instance types, you can use multi-Attach to mount a volume to multiple instances at the same time.
- Amazon EBS provides the following volume types: General Purpose SSD (gp2 and gp3), Provisioned IOPS SSD (io1 and io2), Throughput Optimized HDD (st1), Cold HDD (sc1), and Magnetic (standard).
- They differ in performance characteristics and price, allowing you to tailor your storage performance and cost to the needs of your applications. For more information, see Amazon EBS volume types.
- Your account has a limit on the number of EBS volumes that you can use, and the total storage available to you. For more information about these limits, and how to request an increase in your limits.

Benefits of using EBS volumes

EBS volumes provide benefits that are not provided by instance store volumes.

- Data availability
- Data persistence
- Data encryption
- Data security
- Snapshots

- Flexibility

Data Availability

- ❖ When you create an EBS volume, it is automatically replicated within its Availability Zone to prevent data loss due to failure of any single hardware component.
- ❖ You can attach an EBS volume to any EC2 instance in the same Availability Zone. After you attach a volume, it appears as a native block device like a hard drive or other physical device.
- ❖ At that point, the instance can interact with the volume just as it would with a local drive. You can connect to the instance and format the EBS volume with a file system, such as ext3, and then install applications.
- ❖ If you attach multiple volumes to a device that you have named, you can stripe data across the volumes for increased I/O and throughput performance.
- ❖ You can attach io1 and io2 EBS volumes to up to 16 Nitro-based instances. For more information, see Attach a volume to multiple instances with Amazon EBS Multi-Attach. Otherwise, you can attach an EBS volume to a single instance.
- ❖ You can get monitoring data for your EBS volumes, including root device volumes for EBS-backed instances, at no additional charge.
- ❖ For more information about monitoring metrics, see Amazon CloudWatch metrics for Amazon EBS. For information about tracking the status of your volumes, see Amazon CloudWatch Events for Amazon EBS.

Data Persistence

- ❖ An EBS volume is off-instance storage that can persist independently from the life of an instance. You continue to pay for the volume usage if the data persists.
- ❖ EBS volumes that are attached to a running instance can automatically detach from the instance with their data intact when the instance is terminated if you uncheck the Delete on Termination check box when you configure EBS volumes for your instance on the EC2 console.
- ❖ The volume can then be reattached to a new instance, enabling quick recovery. If the check box for Delete on Termination is checked, the volume(s) will delete upon termination of the EC2 instance. If you are using an EBS-backed instance, you can stop and restart that instance without affecting the data stored in the attached volume.

- The volume remains attached throughout the stop-start cycle. This enables you to process and store the data on your volume indefinitely, only using the processing and storage resources when required. The data persists on the volume until the volume is deleted explicitly.
- The physical block storage used by deleted EBS volumes is overwritten with zeroes before it is allocated to another account.
- If you are dealing with sensitive data, you should consider encrypting your data manually or storing the data on a volume protected by Amazon EBS encryption. For more information, see Amazon **EBS encryption.**
- By default, the root EBS volume that is created and attached to an instance at launch is deleted when that instance is terminated.
- You can modify this behavior by changing the value of the flag Delete on Termination to false when you launch the instance.
- This modified value causes the volume to persist even after the instance is terminated and enables you to attach the volume to another instance.
- By default, additional EBS volumes that are created and attached to an instance at launch are not deleted when that instance is terminated.
- You can modify this behavior by changing the value of the flag Delete on Termination to true when you launch the instance. This modified value causes the volumes to be deleted when the instance is terminated.

Data Encryption

- For simplified data encryption, you can create encrypted EBS volumes with the Amazon EBS encryption feature.
- All EBS volume types of support encryption. You can use encrypted EBS volumes to meet a wide range of data-at-rest encryption requirements for regulated/audited data and applications.
- Amazon EBS encryption uses 256-bit Advanced Encryption Standard algorithms (AES-256) and an Amazon-managed key infrastructure.
- The encryption occurs on the server that hosts the EC2 instance, providing encryption of data-in-transit from the EC2 instance to Amazon EBS storage. For more information, see Amazon EBS encryption.
- Amazon EBS encryption uses AWS Key Management Service (AWS KMS) master keys when creating encrypted volumes and any snapshots created from your encrypted volumes.
- The first time you create an encrypted EBS volume in a region, a default master key is created for you automatically.

- This key is used for Amazon EBS encryption unless you select a customer master key (CMK) that you created separately using AWS KMS.
- Creating your own CMK gives you more flexibility, including the ability to create, rotate, disable, define access controls, and audit the encryption keys used to protect your data. For more information, see the AWS Key Management Service Developer Guide.

Data Security

- Amazon EBS volumes are presented to you as raw, unformatted block devices.
- These devices are logical devices that are created on the EBS infrastructure, and the Amazon EBS service ensures that the devices are logically empty (that is, the raw blocks are zeroed, or they contain cryptographically pseudorandom data) prior to any use or re-use by a customer.
- If you have procedures that require that all data, be erased using a specific method, either after or before use (or both), such as those detailed in DoD 5220.22-M (National Industrial Security Program Operating Manual) or NIST 800-88 (Guidelines for Media Sanitization), you can do so on Amazon EBS.
- That block-level activity will be reflected down to the underlying storage media within the Amazon EBS service.

Snapshots

- Amazon EBS provides the ability to create snapshots (backups) of any EBS volume and write a copy of the data in the volume to Amazon S3, where it is stored redundantly in multiple Availability Zones.
- The volume does not need to be attached to a running instance to take a snapshot. As you continue to write data to a volume, you can periodically create a snapshot of the volume to use as a baseline for new volumes.
- These snapshots can be used to create multiple new EBS volumes or move volumes across Availability Zones. Snapshots of encrypted EBS volumes are automatically encrypted.
- When you create a new volume from a snapshot, it's an exact copy of the original volume at the time the snapshot was taken.
- EBS volumes that are created from encrypted snapshots are automatically encrypted. By optionally specifying a different Availability Zone, you can use this functionality to create a duplicate volume in that zone.
- The snapshots can be shared with specific AWS accounts or made public. When you create snapshots, you incur charges in Amazon S3 based on the volume's

total size. For a successive snapshot of the volume, you are only charged for any additional data beyond the volume's original size.

- Snapshots are incremental backups, meaning that only the blocks on the volume that have changed after your most recent snapshot are saved.
- If you have a volume with 100 GiB of data, but only 5 GiB of data have changed since your last snapshot, only the 5 GiB of modified data is written to Amazon S3. Even though snapshots are saved incrementally, the snapshot deletion process is designed so that you need to retain only the most recent snapshot.

Flexibility

- EBS volumes support live configuration changes while in production.
- You can modify volume type, volume size, and IOPS capacity without service interruptions. For more information, see Amazon EBS Elastic Volumes.