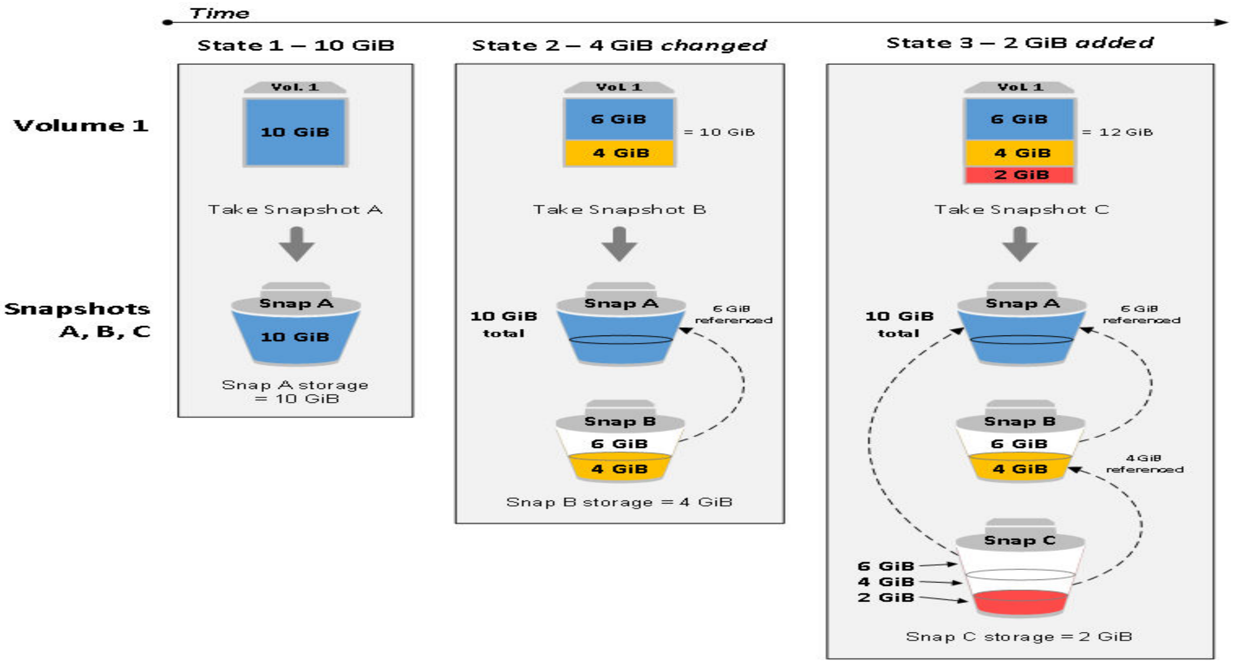
What is Amazon EBS Snapshot

We can back up the data on our Amazon EBS volumes to Amazon S3 by taking point-in-time snapshots.

An EBS snapshot is a point-in-time copy of your Amazon EBS volume, which is lazily copied to Amazon Simple Storage Service (Amazon S3). This means EBS Snapshots stored in S3.

EBS snapshots are incremental copies of data. This means that only unique blocks of EBS volume data that have changed since the last EBS snapshot are stored in the next EBS snapshot. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data.



When you delete a snapshot, only the data unique to that snapshot is removed. That means latest changes will be deleted.

Each snapshot contains all of the information that is needed to restore your data to a new EBS volume.

When you create an EBS volume based on a snapshot, the new volume begins as an exact replica of the original volume that was used to create the snapshot.

The replicated volume loads data in the background so that you can begin using it immediately.

If you access data that hasn't been loaded yet, the volume immediately downloads the requested data from Amazon S3, and then continues loading the rest of the volume's data in the background.

Snapshot events

You can track the status of your EBS snapshots through CloudWatch Events.

Multi-volume snapshots

Snapshots can be used to create a backup of critical workloads, such as a large database or a file system that spans across multiple EBS volumes.

Multi-volume snapshots allow you to take exact point-in-time, data coordinated, and crash-consistent snapshots across multiple EBS volumes attached to an EC2 instance.

You are no longer required to stop your instance or to coordinate between volumes to ensure crash consistency, because snapshots are automatically taken across multiple EBS volumes.

Note:

Charges for your snapshots are based on the amount of data stored. Because snapshots are incremental, deleting a snapshot might not reduce your data storage costs.

Data referenced exclusively by a snapshot is removed when that snapshot is deleted, but data referenced by other snapshots is preserved.

Encryption support for snapshots

EBS snapshots fully support EBS encryption.

Snapshots of encrypted volumes are automatically encrypted.

Volumes that you create from encrypted snapshots are automatically encrypted.

Amazon Data Lifecycle Manager for EBS Snapshots

Amazon Data Lifecycle Manager (DLM) for EBS Snapshots provides a simple, automated way to back up data stored on Amazon EBS volumes.

You can use Amazon Data Lifecycle Manager to automate the creation, retention, and deletion of snapshots taken to back up your Amazon EBS volumes.

You can define backup and retention schedules for EBS snapshots by creating lifecycle policies based on tags. With this feature, you no longer have to rely on custom scripts to create and manage your backups.

Lifecycle Policies

creating lifecycle policies consists of these core settings.

1. Resource type

The type of AWS resource managed by the policy.

Use VOLUME to create snapshots of individual volumes.

Use INSTANCE to create multi-volume snapshots from the volumes for an instance.

2. Target tags

The tags that must be associated with an EBS volume or an EC2 instance for it, to be managed by the policy.

3. Schedule

The start time and interval for creating snapshots.

The first snapshot is created by a policy within one hour after the specified start time.

Subsequent snapshots are created within one hour of their scheduled time.

4. Retention

You can retain snapshots based on 2 things

either the total count of snapshots

or the age of each snapshot.

Automating snapshot management helps you to

1. Protect valuable data by enforcing a regular backup schedule.

2. Retain backups as required by auditors or internal compliance.

3. Reduce storage costs by deleting outdated backups.

Considerations/Limitations of Amazon Data Lifecycle Manager

Your AWS account has the following quotas related to Amazon Data Lifecycle Manager.

1. You can create up to 100 lifecycle policies per region.

2. You can up to 45 tags per resource.

3. You can create 1 schedule per lifecycle policy.

Considerations/Limitations apply to lifecycle policies

1. A policy does not begin creating snapshots until you set its activation status to *enabled*. You can configure a policy to be enabled upon creation.

2. The first snapshot is created by a policy within one hour after the specified start time. Subsequent snapshots are created within one hour of their scheduled time.

3. If you modify a policy by removing or changing its target tag, the EBS volumes with that tag are no longer affected by the policy.

4. If you modify the schedule name for a policy, the snapshots created under the old schedule name are no longer affected by the policy.

5. If you modify a retention schedule based on time to use a new time interval, the new interval is used only for new snapshots. The new schedule does not affect the retention schedule of existing snapshots created by this policy.

6. You cannot change the retention schedule of a policy from the count of snapshots to the age of each snapshot. To make this change, you must create a new policy.

7. If you disable a policy with a retention schedule based on the age of each snapshot, the snapshots whose retention periods expire while the policy is disabled are retained indefinitely. You must delete these snapshots manually. When you enable the policy again, Amazon Data Lifecycle Manager resumes deleting snapshots as their retention periods expire.

8. If you delete the resource to which a policy with count-based retention applies, the policy no longer manages the previously created snapshots. You must manually delete the snapshots if they are no longer needed.

9. If you delete the resource to which a policy with age-based retention applies, the policy continues to delete snapshots on the defined schedule, up to the last snapshot. You must manually delete the last snapshot if it is no longer needed.

10. You can create multiple policies to back up an EBS volume or an EC2 instance. For example, if an EBS volume has two tags, where tag A is the target for policy A to create a snapshot every 12 hours, and tag B is the target for policy B to create a snapshot every 24 hours, Amazon Data Lifecycle Manager creates snapshots according to the schedules for both policies.

Considerations apply to lifecycle policies and fast snapshot restore

1. A snapshot that is enabled for fast snapshot restore remains enabled even if you delete or disable the lifecycle policy, disable fast snapshot restore for the lifecycle policy, or disable fast snapshot restore for the Availability Zone. You can disable fast snapshot restore for these snapshots manually.

2. If you enable fast snapshot restore and you exceed the maximum number of snapshots that can be enabled for fast snapshot restore, Amazon Data Lifecycle Manager creates snapshots as scheduled but does not enable them for fast snapshot restore. After a snapshot that is enabled for fast snapshot restore is deleted, the next snapshot Amazon Data Lifecycle Manager creates is enabled for fast snapshot restore.

3. When you enable fast snapshot restore for a snapshot, it takes 60 minutes per TiB to optimize the snapshot. We recommend that you create a schedule that ensures that each snapshot is fully optimized before Amazon Data Lifecycle Manager creates the next snapshot.

4. You are billed for each minute that fast snapshot restore is enabled for a snapshot in a particular Availability Zone. Charges are pro-rated with a minimum of one hour.

Considerations apply to lifecycle policies and Multi-Attach enabled volumes

1. When creating a lifecycle policy based on instance tags for Multi-Volume snapshots, Amazon Data Lifecycle Manager initiates a snapshot of the volume for each attached instance. Use the *timestamp* tag to identify the set of time-consistent snapshots created from the attached instances.