AWS Snapshot or EBS Snapshot : -

Amazon Elastic Block Store (EBS) Snapshots provide a simple and secure data protection solution that is designed to protect your block storage data such as EBS volumes, boot volumes, as well as on-premises block data. **EBS Snapshots are a point-in-time copy of your data, and can be used to enable disaster recovery, migrate data across regions and accounts, and improve backup compliance.**

You can create and manage your EBS Snapshots through the AWS Management Console, AWS Command Line Interface (CLI), or the AWS SDKs. Amazon EBS Snapshots also integrate with Amazon Data Lifecycle Manager (DLM), which allows you to define policies that help you [automate snapshot lifecycle management](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html). EBS Snapshots are stored incrementally, which means you are billed only for the changed blocks stored.

Benefits: -

### **Simple and automated**

Amazon EBS Snapshots are a convenient way to back up your EBS volumes. The snapshots are automatically saved to Amazon Simple Storage Service (Amazon S3) for long-term retention. AWS further simplifies the lifecycle management of your snapshots through integration with DLM, which allows you to create policies so that you can automate multiple tasks including creation, deletion, retention, and sharing of snapshots.

### **Cost-effective**

Amazon EBS Snapshots are incremental, storing only the changes since the last snapshot, making them cost effective and ideal for frequent backups. You can use tools such as AWS Cost Explorer to track snapshot usage and spend, and further optimize storage costs as needed. Save up to 75% in snapshot storage costs by using [**EBS Snapshots Archive**](https://aws.amazon.com/ebs/snapshots/faqs/#Snapshots_Archive) for the long-term retention (over 90 days) of seldom-accessed snapshots.

### **Secure**

Amazon EBS offers a simple encryption solution for your EBS resources that does not require you to build, maintain, and secure your own key management infrastructure. You can easily configure your AWS account to enforce encryption of any new EBS volumes and snapshots you create, including snapshots of your on-premises data.

### **Highly available and durable**

Amazon EBS Snapshots are a convenient way to back up your EBS volumes. The snapshots are automatically saved to Amazon S3 for long-term retention. S3 is designed for 99.99999999% (11 nines) durability, ensuring higher availability of your EBS Snapshots. [Recycle Bin](https://aws.amazon.com/ebs/snapshots/faqs/#Recycle_Bin) for EBS Snapshots enhances durability by allowing you to recover accidentally deleted snapshots with a single click or an API call.

Use cases

### **Disaster Recovery**

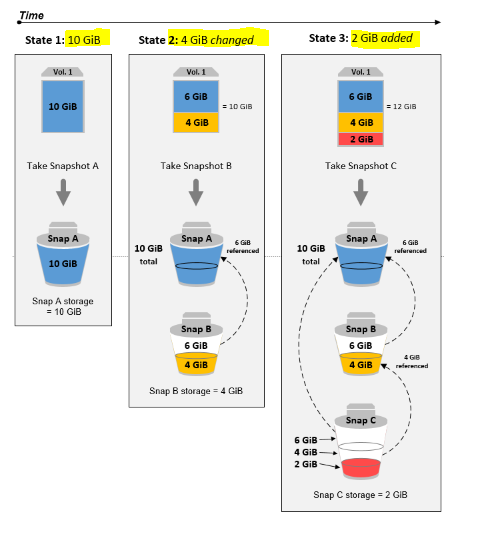
Amazon EBS Snapshots allows you to improve disaster recovery workflows for your workloads running on premises and on AWS at low costs. You can directly create snapshots of your EBS volumes or your data on-premises, and then use these snapshots for recovery in the cloud. With the Fast Snapshot Restore feature, you can quickly restore data from these snapshots into EBS volumes and achieve low recovery time objectives.

### **Data Migration**

With Amazon EBS Snapshots, you can easily move your data across regions, accounts, and Availability Zones. You can copy any snapshot accessible to you to another region or account, including snapshots created by you or shared with you. You can also copy snapshots that are used to create Amazon Machine Images (AMIs) available on AWS Marketplace, which can then be use to launch new EC2 instances in other regions or accounts. Additionally, you can migrate your on-premises data to AWS, by creating snapshots of that data and recovering them into EBS volumes.

### **Backup Compliance**

With Amazon EBS Snapshots, you protect your valuable data by enforcing a regular backup schedule using DLM policies. You can set policies to retain backups as required by auditors to help improve internal compliance. Additionally, EBS Snapshots integrates with [AWS Cloud Trail](https://aws.amazon.com/cloudtrail/) so that you can log, monitor, and retain account activity related to actions taken for your snapshots.



Amazon Data Lifecycle Manager: -

Amazon Data Lifecycle Manager provides an automated, policy-based lifecycle management solution for Amazon Elastic Block Store (EBS) Snapshots and EBS-backed Amazon Machine Images (AMIs). Automate the creation of point-in-time copy of your block storage data with user-defined policies that you can customize based on data protection needs. Amazon Data Lifecycle Manager requires no scripting or special training. The graphical user interface (GUI) makes it easier to automate the creation, retention, and deletion of EBS Snapshots and AMIs. This can be done at regular frequencies and with custom cron expressions. This feature removes the need to manage your code, mitigating the human error associated with maintaining scripts.

When combined with the monitoring features of Amazon CloudWatch and AWS CloudTrail, Amazon Data Lifecycle Manager provides a complete lifecycle management and backup solution for Amazon Elastic Compute Cloud (EC2) instances and individual EBS volumes at no additional cost.

Use Cases and Benefits

### **Protect data and meet compliance**

Protect your data by enforcing a regular backup schedule. Amazon Data Lifecycle Manager provides automated process control with a data protection plan for your valuable data. Gain the ability to create streamlined disaster recovery polices that back up your data to isolated accounts. Amazon Data Lifecycle Manager provides an effective solution for Amazon EBS users to retain backups for audit or compliance needs.

### **Automate back up and monitoring**

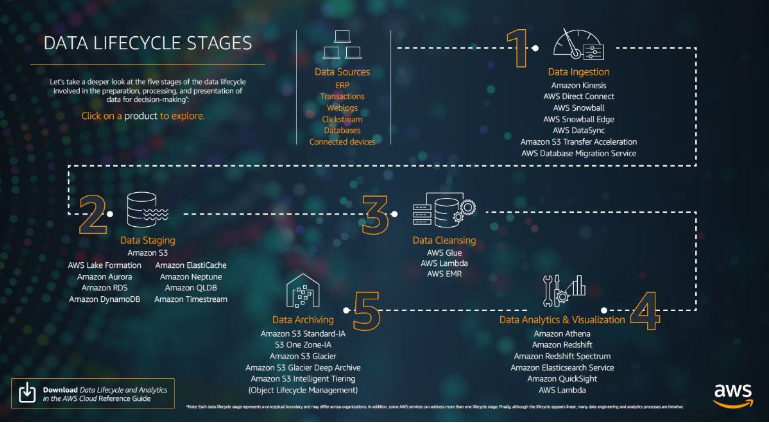
Define policy and schedule to automate the creation, retention, and deletion of EBS Snapshots and AMIs at regular intervals. You can monitor your Amazon Data Lifecycle Manager policies using Amazon CloudWatch, which collects raw data and processes it into readable, near real-time metrics. You can use these metrics to see exactly how many EBS Snapshots and EBS-backed AMIs are created, deleted, and copied by your policies over time. You can also set alarms that send notifications or take action when specified thresholds are met. As part of Amazon EBS, Amazon Data Lifecycle Manager is SOC, PCI, Federal Risk and Authorization Management Progam (FedRAMP), and ISO compliant—it is also HIPAA eligible.

### **Reduce storage costs**

Save costs by consistently applying customized policies to back up your EBS volumes based on criticality of data. Amazon Data Lifecycle Manager helps you manage your EBS resources more efficiently. You can build a policy to facilitate daily creation and retention schedules of EBS Snapshots for your most critical applications—a less frequent schedule can be applied to cold data. You can also regularly clean up snapshots by creating policy-controlled deletion of outdated snapshots to reduce storage costs. For EBS-backed AMIs, Amazon Data Lifecycle Manager will automatically deregister the AMIs at the end of their retention and delete the underlying snapshots. This prevents you from otherwise having to manually delete snapshots and potentially incurring cost if forgotten.

### **Built for flexibility**

Gain the flexibility to use API, AWS Command Line Interface (CLI), AWS SDKs, Terraform, and AWS CloudFormation to create and manage policies. With Amazon Data Lifecycle Manager, you also have the flexiblity to run policies for three different resource types: individual EBS volumes, a group of EBS volumes attached to an EC2 instance, or an EC2 instance. You can also create event-based policies to automate copying of snapshots to separate accounts, and encrypt the snapshots with a different AWS Key Management Service (KMS) key. This adds an additional layer of protection to your data if any accounts are compromised.



AWS Backup: -

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the back up of data across AWS services in the cloud as well as on premises using the AWS Storage Gateway.

AWS Backup FAQs

<https://aws.amazon.com/backup/faqs/?nc=sn&loc=6#Write-Once-Read-Many_.28WORM.29>

