Advanced AWS Workshop

Instructor: Govind Kumar
Date: 12-May-2025 | Time: 9:00 PM - 11:30 PM IST

AWS Storage Services

Learn about the various storage options in AWS and when to use each one.

Advanced EC2 Features

Master snapshots, AMIs, and advanced EC2 management techniques.

Load Balancing

Distribute traffic across multiple EC2 instances for high availability.

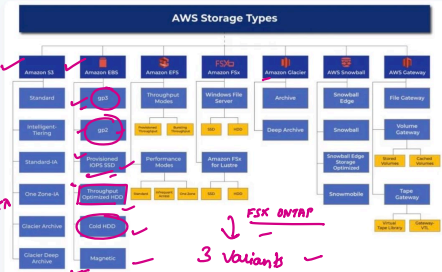
AWS Storage Services Overview

Storage Options in AWS

AWS offers a variety of storage services to meet different needs:

- **Amazon EBS (Elastic Block Store):** Block-level storage volumes for EC2 instances
- **Amazon S3 (Simple Storage Service):** Object storage for any amount of data
- **Amazon EFS (Elastic File System):** Fully managed file system for EC2
- **Amazon FSx:** Fully managed file systems for Windows and Lustre
- **Amazon S3 Glacier:** Low-cost archive storage
- **AWS Storage Gateway:** Hybrid storage integration

> Choosing the right storage service depends on factors like access patterns, performance requirements, durability needs, and cost constraints.



AWS Storage Services Comparison

Understanding IOPS

Input/Output Operations Per Second

IOPS is a critical performance metric for storage systems:

- **Definition:** The number of read/write operations a storage device can perform per second
- **Importance:** Directly impacts application performance, especially for databases and I/O-intensive workloads
- **EBS Volume Types:** Different EBS volume types offer varying IOPS capabilities:
  - General Purpose SSD (gp3): Up to 16,000 IOPS
  - Provisioned IOPS SSD (io2): Up to 64,000 IOPS
  - Throughput Optimized HDD (st1): Not optimized for IOPS
  - Cold HDD (sc1): Not optimized for IOPS
- **Measuring IOPS:** Tools like CloudWatch, fio, and dd can help measure actual IOPS

> When selecting storage for performance-sensitive applications, consider both IOPS and throughput requirements.

Volume Type	Max IOPS	Max Throughput	Latency	Durability	Pricing Tier
gp3	16,000	1,000 MiB/s	~1-2ms	99.8-99.9%	Medium-Low
gp2	16,000	250 MiB/s	~1-2ms	99.8-99.9%	Medium
io2 Block Express	256,000	4,000 MiB/s	<1ms	99.999%	Highest
io2	64,000	1,000 MiB/s	~1-2ms	99.999%	High
io1	64,000	1,000 MiB/s	~1-2ms	99.8-99.9%	High
st1	500-1,000	500 MiB/s	~5-10ms	99.8-99.9%	Low
sc1	250	250 MiB/s	~10-20ms	99.8-99.9%	Lowest

IOPS Comparison Across EBS Volume Types

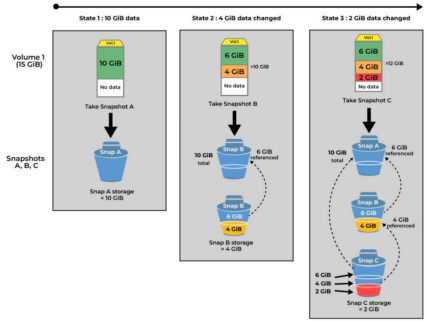
EC2 Snapshots and Backups

Protecting Your EC2 Data

EC2 snapshots are point-in-time copies of your EBS volumes:

- **EBS Snapshots:** Incremental backups that only save blocks that have changed
- **Benefits:** Data protection against accidental deletion or corruption
  - Migration of data across regions or accounts
  - Creating new volumes with the same data
- **Best Practices:**
  - Create regular snapshots using AWS Backup or automated scripts
  - Stop the instance or detach the volume for consistent snapshots
  - Use lifecycle policies to automate snapshot management
  - Tag snapshots for better organization
- **Snapshot Lifecycle:** Create, retain, and delete snapshots based on your backup strategy

> While snapshots are stored incrementally, deleting a snapshot only removes data not needed by other snapshots.



EC2 Snapshot Creation and Restoration Process

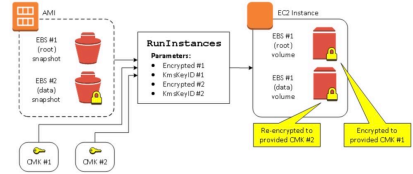
AMI Copy and Encryption

Working with Amazon Machine Images

AMIs can be copied and encrypted for various purposes:

- **AMI Copying:** Copy AMIs across regions for disaster recovery
  Copy AMIs across accounts for organizational needs
  Create new AMIs with different configurations
- **AMI Encryption:** Encrypt unencrypted AMIs during the copy process
  Use AWS KMS keys for encryption
  Change the encryption key for already encrypted AMIs
- **Process:** Select source AMI
  Choose destination region
  Set encryption options
  Initiate copy process

> AMI encryption helps protect sensitive data and meet compliance requirements.



AMI Copy and Encryption Workflow

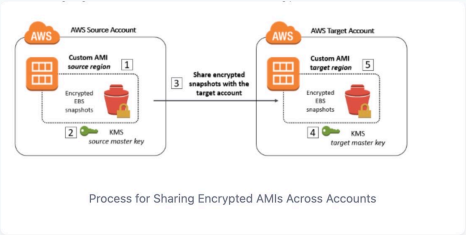
Sharing an Encrypted AMI

Cross-Account AMI Sharing

Sharing encrypted AMIs with other AWS accounts requires specific steps:

- **Prerequisites:** You must own the customer managed KMS key used to encrypt the AMI
  - You cannot share AMIs encrypted with the default AWS managed key
- **Sharing Process:**
  - Modify the KMS key policy to allow the target account
  - Grant the target account permission to use the KMS key
  - Modify the AMI permissions to share with the target account
  - Share any associated snapshots
- **Security Considerations:**
  - The target account can create volumes and instances from the AMI
  - The target account cannot re-share the AMI
  - Consider using cross-account roles for more controlled access

> Properly sharing encrypted AMIs ensures secure collaboration while maintaining control over your resources.



Process for Sharing Encrypted AMIs Across Accounts

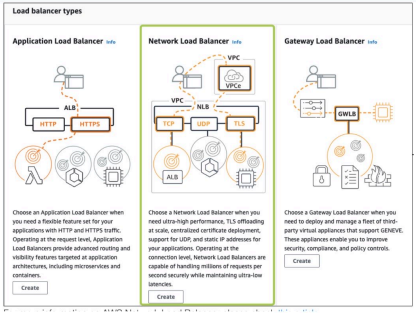
Load Balancers in AWS

Types of AWS Load Balancers

AWS offers several types of load balancers to distribute traffic:

- **Application Load Balancer (ALB):** Operates at Layer 7 (HTTP/HTTPS)
  - Supports path-based routing, host-based routing
  - Ideal for microservices and container-based applications
- **Network Load Balancer (NLB):** Operates at Layer 4 (TCP/UDP/TLS)
  - Ultra-high performance and low latency
  - Handles millions of requests per second
- **Gateway Load Balancer (GWLB):** Operates at Layer 3 (IP protocol)
  - Used for deploying and managing virtual appliances
  - Supports firewalls, intrusion detection, deep packet inspection
- **Classic Load Balancer (CLB):** Legacy load balancer (not recommended for new applications)
  - Operates at both Layer 4 and Layer 7
  - Limited features compared to newer load balancers

> Choosing the right load balancer depends on your application architecture, traffic patterns, and performance requirements.



Comparison of AWS Load Balancer Types