# AWS Cloud Practitioner Certification Guide - Part 2

## Amazon EC2 Storage Options

### Instance Stores

* **Definition**: Local storage physically attached to the host computer for an EC2 instance
* **Key Characteristics**:
* Temporary block-level storage
* Same lifespan as the instance
* When the instance is terminated, all data in the instance store is lost
* Ideal for temporary storage of information that changes frequently
* No additional cost (included with instance)
* Higher I/O performance than EBS in some cases

### Amazon Elastic Block Store (Amazon EBS)

* **Definition**: A service providing persistent block-level storage volumes for EC2 instances
* **Key Characteristics**:
* Data remains available even if EC2 instance is stopped or terminated
* Can be attached and detached from instances when needed
* Automatically replicated within its Availability Zone
* Can be encrypted for additional security
* Can be resized without disrupting the instance
* Multiple volume types available to optimize for performance or cost
* Charged based on provisioned capacity, not used capacity

#### EBS Snapshots

* **Definition**: Point-in-time backups of EBS volumes stored in Amazon S3
* **Key Characteristics**:
* Incremental backups: first backup copies all data, subsequent backups only save changed blocks
* Can be used to create new volumes or restore existing volumes
* Can be copied across regions for disaster recovery
* Can be automated using Amazon Data Lifecycle Manager
* Only charged for the storage used by the unique blocks in each snapshot

## Amazon S3 (Simple Storage Service)

### Core Concepts

* **Definition**: Object-level storage service that stores data as objects in buckets
* **Object Structure**:
* Data: the content being stored (file)
* Metadata: information about the data (creation date, size, content type)
* Key: unique identifier within the bucket (essentially the file name and path)

### S3 Storage Classes

#### S3 Standard

* **Use Cases**: Websites, content distribution, mobile applications, game development, big data analytics
* **Key Features**:
* High durability (99.999999999%, 11 9's) and availability (99.99%)
* Low latency and high throughput
* Sustains the loss of data in two simultaneous facilities
* Data stored in a minimum of three Availability Zones
* More expensive than other storage classes

#### S3 Standard-IA (Infrequent Access)

* **Use Cases**: Long-term storage, backups, disaster recovery
* **Key Features**:
* Same durability as S3 Standard (11 9's)
* Lower availability (99.9%) compared to S3 Standard
* Lower cost than S3 Standard
* Minimum storage duration charge of 30 days
* Retrieval fee for accessing data
* Stores data in a minimum of three Availability Zones

#### S3 One Zone-IA

* **Use Cases**: Non-critical, reproducible data with infrequent access needs
* **Key Features**:
* Same durability within the AZ (11 9's) but lower overall durability
* Lower availability (99.5%)
* Stores data in only a single Availability Zone (unlike other classes)
* 20% less expensive than S3 Standard-IA
* Minimum storage duration charge of 30 days
* Retrieval fee for accessing data

#### S3 Intelligent-Tiering

* **Use Cases**: Data with unknown or changing access patterns
* **Key Features**:
* Automatically moves objects between access tiers based on usage patterns
* If an object isn't accessed for 30 consecutive days, it's moved to infrequent access tier
* When accessed again, it's moved back to frequent access tier
* No retrieval fees, but monthly monitoring and automation fee
* Same durability and throughput as S3 Standard

#### S3 Glacier

* **Use Cases**: Data archiving, long-term backup, digital preservation
* **Key Features**:
* Extremely low cost storage for archival data
* Retrieval times from minutes to hours
* Minimum storage duration charge of 90 days
* Data retrieval options:
  + Expedited (1-5 minutes)
  + Standard (3-5 hours)
  + Bulk (5-12 hours)

#### S3 Glacier Deep Archive

* **Use Cases**: Long-term retention and digital preservation for data accessed once or twice a year
* **Key Features**:
* Lowest cost storage class (up to 95% less than Standard)
* Retrieval time of 12 hours or more
* Minimum storage duration charge of 180 days
* Data retrieval options:
  + Standard (12 hours)
  + Bulk (48 hours)

## Amazon Elastic File System (Amazon EFS)

* **Definition**: A scalable, elastic, cloud-native NFS file system for use with AWS Cloud services and on-premises resources
* **Key Characteristics**:
* Grows and shrinks automatically as files are added and removed
* Can scale on demand to petabytes without disrupting applications
* Supports thousands of concurrent NFS connections
* Multi-AZ architecture for high availability
* Provides consistent performance at scale
* Pay only for the storage you use (no pre-provisioning required)
* Supports two storage classes: Standard and Infrequent Access
* Ideal for Linux workloads and shared file access
* **Use Cases**:
* Content management systems
* Web serving environments
* Data analytics applications
* Media processing workflows
* Development and test environments
* Situations where many services/resources need concurrent access to the same data

## Database Services

### Amazon Relational Database Service (Amazon RDS)

* **Definition**: A managed relational database service that simplifies database administration tasks
* **Supported Database Engines**:
* Amazon Aurora
* PostgreSQL
* MySQL
* MariaDB
* Oracle Database
* Microsoft SQL Server
* **Key Features**:
* Automated tasks: backups, software patching, automatic failure detection, recovery
* High availability with Multi-AZ deployment option
* Read replicas for read scaling and improved performance
* Automated backups with point-in-time recovery
* Database snapshots (manual backups)
* Encryption at rest and in transit
* Monitoring and metrics through CloudWatch
* Security through network isolation (VPC), IAM, security groups
* Scalable storage and compute resources

### Amazon Aurora

* **Definition**: Enterprise-class relational database compatible with MySQL and PostgreSQL
* **Key Features**:
* 5x throughput of standard MySQL and 3x throughput of standard PostgreSQL
* Up to 64TB of auto-scaling storage
* 6-way replication across 3 Availability Zones
* Automated backups, snapshots, and point-in-time recovery
* Serverless option for variable workloads
* Global database option for multi-region deployment
* Fast database cloning
* Up to 15 read replicas with sub-10ms replica lag

### Amazon DynamoDB

* **Definition**: Fully managed NoSQL database service for any scale
* **Key Features**:
* Non-relational database using key-value pairs
* Single-digit millisecond performance at any scale
* Serverless with automatic scaling
* Supports both document and key-value data models
* ACID transactions for multi-operation data accuracy
* Point-in-time recovery and on-demand backup
* In-memory caching with DynamoDB Accelerator (DAX)
* Global tables for multi-region, multi-master deployment
* Automatic encryption at rest

### Amazon Redshift

* **Definition**: Fully managed, petabyte-scale data warehouse service
* **Key Features**:
* Columnar storage technology for analytical queries
* Massively Parallel Processing (MPP) architecture
* SQL compatible query interface
* Integration with data lakes via Redshift Spectrum
* Ability to query both structured and semi-structured data
* Automatic backups to S3
* Continuous/incremental backup
* Ideal for business intelligence and big data analytics

### Additional Database Services

#### AWS Database Migration Service (AWS DMS)

* Enables migration of relational databases, non-relational databases, and other data stores
* Supports homogeneous migrations (same engine) and heterogeneous migrations (different engines)
* Minimal downtime during migration with continuous data replication
* Supports one-time migrations and ongoing replication

#### Amazon DocumentDB

* Document database service that supports MongoDB workloads
* Stores data in JSON-like documents with dynamic schemas
* Scalable, highly available, and durable
* Ideal for content management, catalogs, user profiles

#### Amazon Neptune

* Fully managed graph database service
* Purpose-built for highly connected datasets
* Supports popular graph models: Property Graph and W3C's RDF
* Use cases:
* Recommendation engines
* Fraud detection
* Knowledge graphs
* Social networking
* Network/IT operations analysis

#### Amazon Quantum Ledger Database (Amazon QLDB)

* Fully managed ledger database for transparent, immutable, and cryptographically verifiable transaction logs
* Central, trusted authority
* Complete history of all changes to application data
* Ideal for financial transactions, supply chain, registration/licensing records

#### Caching Services

##### Amazon ElastiCache

* Adds caching layers on top of databases to improve read times of common requests
* Supports two open-source engines:
* Redis: advanced data structures, high availability, backup/restore
* Memcached: multi-threaded performance, scale-out with multiple nodes

##### Amazon DynamoDB Accelerator (DAX)

* In-memory cache specifically for DynamoDB
* Improves response times from milliseconds to microseconds
* No application modifications required
* Fully managed, highly available cache

## AWS Shared Responsibility Model

### Overview

* Security and compliance are shared responsibilities between AWS and the customer
* AWS manages security "of" the cloud; customers are responsible for security "in" the cloud
* The model helps relieve customer's operational burden

### AWS Responsibilities ("Security of the Cloud")

* Physical security of data centers
* Controlled physical access
* Power redundancy
* Environmental controls
* Hardware and software infrastructure
* Host operating system
* Virtualization layer
* Network infrastructure
* Storage infrastructure
* Services operation, management, and control
* Global infrastructure
* Regions
* Availability Zones
* Edge locations

### Customer Responsibilities ("Security in the Cloud")

* Data encryption (at rest and in transit)
* Network traffic protection
* Operating system, network, and firewall configuration
* Identity and Access Management
* Customer data
* Applications
* Security configuration and management
* Awareness and training
* Compliance with specific regulations and standards

### Responsibility Variation by Service Type

* **Infrastructure as a Service (IaaS)**
* Customer has more responsibility (e.g., EC2, EBS, VPC)
* Customer manages guest OS, applications, data
* **Platform as a Service (PaaS)**
* Shared responsibility (e.g., RDS, EMR, ElasticSearch)
* AWS manages platform, customer manages applications and data
* **Software as a Service (SaaS)**
* Customer has less responsibility (e.g., S3, DynamoDB, SQS)
* AWS manages the service, customer manages data and access

## Identity and Access Management (IAM)

### Core Components

#### IAM Users

* Entities created in AWS representing the person or service using it
* By default, newly created users have NO permissions
* Best practice: create individual users instead of using root account
* Authentication methods:
* Username and password
* Access keys (for programmatic access)
* Features:
* Permanent long-term credentials
* Can be assigned to specific people or applications
* Can belong to multiple groups

#### IAM Policies

* JSON documents defining permissions
* Types:
* Identity-based policies: attached to users, groups, or roles
* Resource-based policies: attached to resources like S3 buckets
* Permission boundaries: set maximum permissions
* Organization SCPs: control permissions for accounts in an organization
* Policy structure:
* Effect: Allow or Deny
* Action: specific API operations
* Resource: specific AWS resources
* Condition: circumstances when policy applies

#### IAM Groups

* Collections of IAM users
* Used to apply the same permission to multiple users
* A user can be a member of multiple groups
* Groups cannot be nested
* Groups cannot be identified as a "Principal" in a policy

#### IAM Roles

* Identity with specific permissions but not uniquely associated with one person
* Assumed by anyone who needs it (users, applications, services)
* Temporary credentials returned when assuming a role
* Use cases:
* Cross-account access
* Service-to-service delegation
* Identity federation
* Applications running on EC2 instances

#### Multi-Factor Authentication (MFA)

* Additional security layer beyond username and password
* Support for multiple MFA device types:
* Virtual MFA (e.g., Google Authenticator, Authy)
* Hardware key fob (e.g., Yubikey)
* Hardware key fob with display
* Best practice: enable MFA for all users, especially root account

### AWS Organizations

* Service for centrally managing and governing multiple AWS accounts
* Features:
* Centralized account management
* Consolidated billing
* Hierarchical grouping of accounts
* Centralized policy-based controls

#### Organization Structure

* **Root**: The parent container for all accounts
* **Organizational Units (OUs)**: Groupings of accounts for easier management
* Can be nested for hierarchical organization
* Allow for applying policies to entire groups of accounts
* Provide isolation between workloads/applications

#### Service Control Policies (SCPs)

* Centrally control permissions for accounts in the organization
* Limit permissions available to users and roles in member accounts
* Do not grant permissions, only restrict them
* Not applied to the management account
* Apply to all users and roles in attached accounts, including root
* Use cases:
* Prevent access to specific services
* Enforce data residency requirements
* Limit ability to modify security configurations

## Compliance and Security Services

### AWS Artifact

#### AWS Artifact Agreements

* Review, accept, and manage agreements with AWS
* Supports agreements for individual accounts and organizations
* Handles specific regulatory agreements (e.g., HIPAA BAA)

#### AWS Artifact Reports

* Access to AWS security and compliance documentation
* Third-party audit reports (e.g., SOC reports, PCI reports)
* Certification documentation
* Stays up-to-date with latest reports
* Provides evidence for your own audits

### Customer Compliance Center

* Resources for compliance questions
* Overview of AWS risk and compliance programs
* Customer compliance stories and use cases
* Whitepapers and documentation for compliance topics
* Auditor learning path resources

### Security Services

#### DDoS Protection

##### Denial of Service (DoS) Attack

* Deliberate attempt to make a website/application unavailable to users
* Usually by flooding with excessive traffic or exploiting vulnerabilities

##### Distributed Denial of Service (DDoS) Attack

* DoS attack from multiple sources simultaneously
* Can come from compromised systems ("bots" or "zombie" systems)
* Types:
* Layer 3/4 attacks (e.g., UDP floods, SYN floods)
* Layer 7 attacks (application layer attacks)

##### AWS Shield

* **AWS Shield Standard**:
* Free service for all AWS customers
* Protects against common, frequently occurring DDoS attacks
* Automatically applied to CloudFront, Route 53, ELB, AWS Global Accelerator
* **AWS Shield Advanced**:
* Paid service with additional protections
* 24/7 access to AWS DDoS Response Team (DRT)
* Cost protection against DDoS-related spikes in usage
* Detailed attack diagnostics
* Protects against larger and more sophisticated attacks
* Integrates with AWS WAF for Layer 7 protections

#### AWS Key Management Service (AWS KMS)

* Service for creating and managing cryptographic keys
* Enables encryption operations through these keys
* Features:
* Centralized key management
* FIPS 140-2 validated hardware security modules
* Automatic key rotation
* Permissions and access controls for keys
* Integration with many AWS services
* Audit capability with CloudTrail
* Supports:
* Symmetric encryption keys
* Asymmetric keys for encryption or signing
* Key import
* Custom key stores

#### AWS WAF (Web Application Firewall)

* Protects web applications from common exploits and bots
* Works with:
* Amazon CloudFront
* Application Load Balancer
* API Gateway
* AppSync
* Features:
* Rule creation based on:
  + IP addresses
  + HTTP headers
  + HTTP body
  + URI strings
  + SQL injection
  + Cross-site scripting (XSS)
* Rate-based rules to combat brute force attacks
* Custom rule creation
* Managed rule groups from AWS and third-party vendors
* Real-time metrics and sampled requests
* Full logging capability

#### Amazon Inspector

* Automated security assessment service
* Helps improve security and compliance of applications
* Automatically discovers workloads (like EC2 instances) and scans them
* Features:
* Security vulnerability checks
* Network accessibility checks
* Assessment against security benchmarks
* Continuous monitoring
* Risk score prioritization
* Integration with AWS Security Hub and EventBridge

## Monitoring and Management Tools

### Amazon CloudWatch

* Monitoring and observability service for AWS resources and applications
* Core components:
* **Metrics**: Data about the performance of systems
  + Collected for AWS resources and can be custom metrics
  + Stored for 15 months
  + Standard metrics collected at 5-minute intervals by default
  + Detailed monitoring available at 1-minute intervals (additional cost)
* **Alarms**: Watches a single metric over a specified time period
  + Can trigger actions based on the value relative to threshold
  + Actions include:
  + EC2 actions (stop, terminate, reboot, recover)
  + Auto Scaling actions
  + SNS notifications
  + Systems Manager actions
* **Dashboards**: Customizable home pages in the CloudWatch console
  + Create visualizations of metrics and alarms
  + Create multiple dashboards for different purposes
  + Share dashboards with people who don't have access to your AWS account
* **Logs**: Collect, monitor, analyze, and store log files
  + Centralize logs from systems, applications, and services
  + Set metric filters to extract values from logs
  + Define log retention policies
* **Events/EventBridge**: Stream of system events describing changes in AWS resources
  + Can trigger automated responses to operational events

### AWS CloudTrail

* Service that records API calls for your AWS account
* Enables governance, compliance, and operational auditing
* Types of events:
* **Management Events**: Operations performed on resources
  + Examples: configuring security, registering devices, setting up logging
  + Enabled by default
* **Data Events**: Resource operations performed on or within a resource
  + Examples: S3 object-level API activity, Lambda function execution
  + High-volume activities
  + Not enabled by default
* **Insights Events**: Unusual API call rate or error rate activity
  + Requires enabling CloudTrail Insights
  + Additional charges apply
* Features:
* Event history for past 90 days without additional configuration
* Trails for long-term storage in S3
* Log file validation to verify integrity
* Log encryption with KMS
* Real-time processing with CloudWatch Logs
* Organization-wide trails
* Integration with EventBridge for automated responses

### AWS Trusted Advisor

* Online tool that provides real-time guidance for optimizing AWS resources
* Five categories of checks:
* **Cost Optimization**: Identify opportunities to reduce costs
  + Examples: idle resources, over-provisioned instances
* **Performance**: Improve service performance
  + Examples: high utilization instances, CloudFront optimizations
* **Security**: Identify security vulnerabilities and close gaps
  + Examples: exposed access keys, overly permissive security groups
* **Fault Tolerance**: Improve application reliability
  + Examples: RDS backups, multi-AZ configurations
* **Service Limits**: Check if usage is approaching service limits
  + Examples: VPC limits, EBS volume limits
* Available checks vary by support plan:
* Basic and Developer Support: Limited core checks
* Business and Enterprise Support: Full set of checks

## AWS Pricing and Cost Management

### AWS Pricing Models

* **Pay-as-you-go**: Pay only for the resources you use, without long-term contracts
* **Save when you reserve**: Significant discounts for reservation commitments
* **Pay less by using more**: Volume-based discounts
* **Save as AWS grows**: Pricing gets lower as AWS achieves economies of scale

### Pricing for Common Services

* **EC2**: Charged based on:
* Instance hours/seconds (varies by instance type, size, and region)
* Storage (EBS volumes)
* Data transfer (outbound is charged, inbound is free)
* IP addresses
* Load balancing
* Pricing models:
  + On-Demand (highest flexibility, no commitment)
  + Reserved Instances (1 or 3-year terms, up to 72% savings)
  + Spot Instances (bid on unused capacity, up to 90% savings)
  + Savings Plans (commitment to usage, flexibility on instance family)
* **Lambda**: Charged based on:
* Number of requests
* Compute time (duration)
* Includes 1 million free requests and 3.2 million seconds per month
* Additional resources like memory affect compute cost
* **S3**: Charged based on:
* Storage amount (per GB)
* Number of requests
* Data transfer out
* Storage class
* Storage management features

### AWS Consolidated Billing

* Feature of AWS Organizations
* Combines usage across all accounts
* Single payment method
* Easier tracking of charges and allocations
* Volume pricing discounts across accounts
* No additional cost to use consolidated billing

### AWS Budgets

* Set custom cost and usage budgets
* Track progress against your budgets
* Receive alerts when thresholds are exceeded
* Plan for Reserved Instance utilization or coverage
* Set up to 5 free budgets
* Additional budgets available for a fee

### AWS Cost Explorer

* Visual tool to understand and manage AWS costs
* Features:
* View cost data for the past 13 months
* Forecast future costs based on historical data
* Filter and group data by various dimensions
* Save reports for future reference
* View Reserved Instance recommendations
* Access programmatically via API

### AWS Support Plans

* **Basic Support**:
* Included with all AWS accounts
* Access to documentation, whitepapers, support forums
* Limited Trusted Advisor checks
* Personal Health Dashboard
* **Developer Support**:
* Email access to customer support (business hours)
* Limited Trusted Advisor checks
* Response times: 12+ hours for general issues, 24+ hours for other issues
* **Business Support**:
* 24/7 phone, email, and chat access to support engineers
* Full Trusted Advisor checks
* Access to Infrastructure Event Management (additional fee)
* Response times: 1 hour for urgent cases, 4 hours for critical errors
* **Enterprise Support**:
* All Business Support features
* Designated Technical Account Manager (TAM)
* Concierge Support Team
* Response times: 15 minutes for business-critical systems, 1 hour for production systems

### AWS Marketplace

* Digital catalog with thousands of third-party software listings
* Types of products:
* Software Infrastructure
* DevOps tools
* Business applications
* Machine Learning algorithms
* IoT solutions
* Professional services
* Benefits:
* Find, test, and deploy software that runs on AWS
* Deploy pre-configured software quickly
* Solutions available in AMI, CloudFormation template, SaaS formats
* Flexible pricing options (hourly, monthly, annual)
* Private marketplace option for controlling approved software

## AWS Cloud Adoption Framework (AWS CAF)

### Overview

* Guidance to help organizations develop efficient plans for cloud adoption
* Based on AWS experience and best practices
* Six focus areas called "Perspectives"

### Business Perspective

* Ensures IT aligns with business needs and investments link to business results
* Key capabilities:
* Business case development
* Financial management
* Strategy alignment
* Benefits realization
* Business risk management
* Common roles:
* Business managers
* Finance managers
* Budget owners
* Strategy stakeholders

### People Perspective

* Focuses on organizational change management, leadership, and workforce development
* Key capabilities:
* Resource management
* Incentive management
* Career management
* Training management
* Organizational change management
* Common roles:
* Human resources
* Staffing personnel
* People managers

### Governance Perspective

* Focuses on orchestrating cloud initiatives while maximizing benefits and minimizing risks
* Key capabilities:
* Portfolio management
* Program and project management
* Business performance measurement
* License management
* Budget & cost management
* Common roles:
* Chief Information Officer (CIO)
* Program managers
* Enterprise architects
* Business analysts
* Portfolio managers

### Platform Perspective

* Principles and patterns for implementing new solutions and migrating on-premises workloads
* Key capabilities:
* Platform architecture
* Data architecture
* Application architecture
* Infrastructure architecture
* Operations architecture
* Common roles:
* Chief Technology Officer (CTO)
* IT managers
* Solutions architects

### Security Perspective

* Ensures organization meets security objectives for visibility, audibility, control, and agility
* Key capabilities:
* Identity and access management
* Detective control
* Infrastructure security
* Data protection
* Incident response
* Common roles:
* Chief Information Security Officer (CISO)
* IT security managers
* IT security analysts

### Operations Perspective

* Enables, runs, uses, operates, and recovers IT workloads to meet business requirements
* Key capabilities:
* Service monitoring
* Application performance monitoring
* Resource inventory management
* Release management
* Reporting and analytics
* Common roles:
* IT operations managers
* IT support managers

## Migration and Innovation

### 6 R's of Migration

#### 1. Rehosting ("Lift and Shift")

* Moving applications without changes
* Advantages:
* Quick migration with minimal changes
* Easier to optimize/re-architect once in the cloud
* Can reduce costs by up to 30% without changes
* Common tools: AWS Application Migration Service, CloudEndure Migration

#### 2. Replatforming ("Lift, Tinker, and Shift")

* Making a few cloud optimizations without changing core architecture
* Examples:
* Moving a database to RDS
* Implementing auto-scaling
* Reducing administrative burden with managed services
* Advantages:
* Tangible benefits without major changes
* Keeps existing functionality
* Lower risk than refactoring

#### 3. Refactoring/Re-architecting

* Reimagining how the application is built using cloud-native features
* Advantages:
* Better performance, scalability, and reliability
* Easier to add features
* Takes full advantage of cloud capabilities
* Cost reduction for operations
* Disadvantages:
* Highest initial cost
* More complex and time-consuming

#### 4. Repurchasing

* Moving from traditional license to a software-as-a-service model
* Examples:
* CRM to Salesforce
* HR to Workday
* Custom built CMS to Contentful
* Advantages:
* Standardized software
* No maintenance or development costs
* Usually easy to use and train staff

#### 5. Retaining

* Keeping applications in source environment
* Common reasons:
* Applications that require major refactoring
* Legacy applications that are difficult to migrate
* Not yet ready to prioritize an application
* Compliance or regulatory requirements

#### 6. Retiring

* Removing applications that are no longer needed
* Advantages:
* Cost savings
* Security improvements
* Reduced system complexity
* Lower operational burden

### AWS Snow Family

#### AWS Snowcone

* **Specifications**:
* Small, rugged, secure, portable computing device
* 8 TB storage capacity
* 4GB memory, 2 vCPUs
* USB-C power or optional battery
* Can run edge computing workloads
* **Use Cases**:
* Edge computing in space-constrained environments
* Data collection in remote or harsh environments
* Content distribution
* IoT data aggregation

#### AWS Snowball Edge

* **Specifications**:
* Two types:
  + Storage Optimized: 80TB capacity, 40 vCPUs, 80 GB memory
  + Compute Optimized: 42TB capacity, 52 vCPUs, 208 GB memory, optional GPU
* Rugged, portable, rackable
* Dust, water, and impact resistant
* **Use Cases**:
* Large-scale data migrations
* Datacenter decommissions
* Disaster recovery
* Remote office backups
* Edge computing in locations with connectivity limitations

#### AWS Snowmobile

* **Specifications**:
* Exabyte-scale data transfer service (up to 100PB per truck)
* Secure shipping container transported on a semi-trailer truck
* Temperature controlled, GPS-tracked, 24/7 video surveillance
* **Use Cases**:
* Massive data center migrations
* Media and entertainment archive digitization
* Moving entire data center infrastructure to AWS