WHIZLABS

AWS Certified: SysOps Administrator - Associate

Cheat Sheet

Quick Bytes for you before the exam!

*The information provided in the Cheat Sheet is for educational purposes only; created in our efforts to help aspirants prepare for the exam **AWS SysOps Administrator Associate certification**. Though references have been taken from **AWS documentation**, it's not intended as a substitute for the official docs. The document can be reused, reproduced, and printed in any form; ensure that appropriate sources are credited and required permissions are received.*

Index

—-Back to Index—

Management and Governance

Migration and Transfer

Networking & Content Delivery

Application Integration

Developer Tools

Billing & Cost Management

—-Back to Index—

Compute

AWS EC2

What is AWS EC2?

EC2 (Elastic Compute Cloud) is a scalable virtual machine in the cloud.

- Automatically scales instances based on traffic.
- Eliminates hardware investment.
- Allows launching multiple servers with full control over security, networking, and storage.

Overview of Key Features in Amazon EC2

Feature	Description
Instance Type	Provides a range of instance types for various use cases. Determines the processor and memory configuration of your EC2 instance.
EBS Volume	- Stands for Elastic Block Storage. - Block-level storage assigned to a single EC2 instance. - Persists independently from running EC2 instances. **Types:** - General Purpose (SSD) - Cold Hard Disk Drive - Magnetic - Provisioned IOPS (SSD) - Throughput Optimized Hard Disk Drive
Instance Store	Ephemeral block-level storage for EC2 instances. Used for faster processing and temporary storage of applications.
AMI	- Stands for Amazon Machine Image. - Defines the OS, dependencies, libraries, and data for EC2 instances. - Enables launching multiple instances with the same configuration.
Security Group	- Virtual firewall for EC2 instances. - Controls ports and traffic. - Active at the instance level; Network ACLs operate at the subnet level. - Allows rules only, cannot deny. - Stateful design. - Outbound traffic allowed by default; inbound rules require definition.
Key Pair	- A set of security credentials (public and private keys) for identity verification when connecting to an instance. - Public key attached to the instance; private key remains with the user. - Access is granted when keys match. - Keep the private key secure.
Pricing	Different pricing options: - On-Demand - Reserved Instances - Savings Plan - Spot Instances
Tags	- Key-value pairs assigned to AWS resources. - Help identify and organize resources effectively.

—-Back to Index—

AWS Lambda

What is AWS Lambda?

AWS Lambda is a **serverless compute service** that runs your code without the need for provisioning servers. It automatically scales with request count and follows a **pay-per-use model**, meaning no charges when the code isn't running. Lambda executes code for any application or backend service, triggered by events like updates in DynamoDB or S3 changes, or HTTP requests via API Gateway.

What is Serverless Computing?

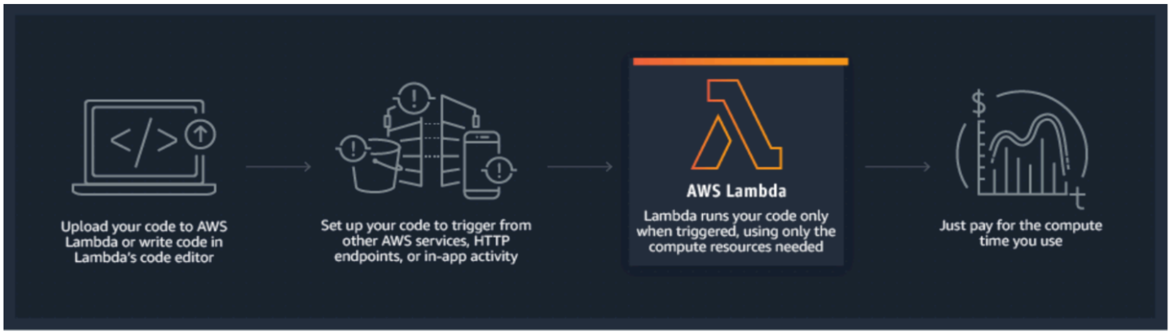
Serverless computing provides backend services on a **pay-per-use basis** without worrying about underlying infrastructure. Servers exist but are managed by the cloud vendor.

When to Use Lambda

- Ideal when you focus solely on your code while AWS manages compute resources like memory, CPU, and network.
- For custom compute management, consider EC2 or Elastic Beanstalk. Lambda abstracts server access and runtime customization.

How AWS Lambda Works

Aspect	Details
Lambda Functions	- Code is uploaded as a zip file or from an S3 bucket. - Functions are monitored via Amazon CloudWatch.
Lambda Layers	- Archive for additional code (e.g., libraries, dependencies, or runtimes). - Allows up to 5 layers per function. - Layers are immutable and can be shared publicly.
Lambda Events	- Entities that trigger functions, such as: - DynamoDB, SQS, SNS, CloudWatch, API Gateway, IoT, Kinesis.
Lambda@Edge	- Runs code closer to users through CloudFront, improving performance and reducing latency.


Upload your code to AWS Lambda or write code in Lambda's code editor
Set up your code to trigger from other AWS services, HTTP endpoints, or in-app activity
AWS Lambda
Lambda runs your code only when triggered, using only the compute resources needed
Just pay for the compute time you use

Supported Languages

- Node.js, Go, Java, Python, Ruby.

Pricing

- Charged based on **number of requests** and **execution duration** (per 100 ms).
- **Free Tier**: 1 million requests/month. 400,000 GB-seconds of compute time/month.

AWS Auto Scaling

AWS Auto Scaling monitors applications and automatically adjusts capacity for **consistent performance** and **cost efficiency**. It supports scaling for **EC2 Instances, ECS tasks, DynamoDB, and Aurora Read Replicas**.

Key Concepts

✔ **Launch Configuration vs. Launch Template**

- **Launch templates** offer the latest EC2 features and support on-demand & spot instances.
- **Launch configurations** lack some Auto Scaling features.

✔ **Lifecycle Hooks**

- Pause EC2 instances in **wait state** until an action completes or timeout ends.

✔ **Monitoring**

- **Health Checks** – Remove unhealthy instances from the target group.
- **CloudWatch Events & Metrics** – Track scaling actions and performance.
- **Notification Service** – Alerts for instance launch/termination.

Pricing

✔ **No additional cost** for Auto Scaling itself.
✔ **Pay only for the AWS resources used**.

Amazon EC2 Image Builder

EC2 Image Builder is a tool that is used for creating, customizing, managing, securing, and distributing Virtual Machine and container images for its use on AWS or on-premises environments.

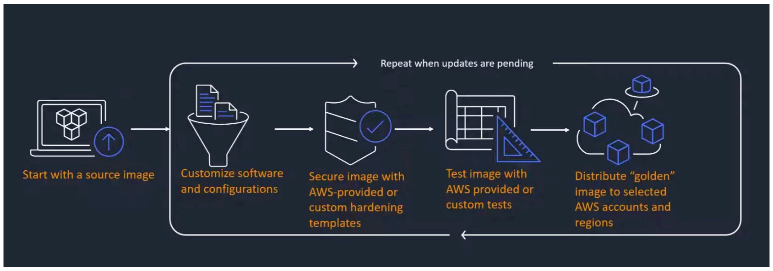
- Organizations can build standardized images, test, validate, and ship them for Production use using EC2 Image Builder.
- EC2 Image Builder is a managed service offering that simplifies the end-end Image-building workflow and ensures that the images are distributed across Accounts and regions that need it.

Features:

- EC2 Image Builder uses a Built-in image pipeline to automate the end-end workflow.
- The pipeline can be triggered manually, in a Schedule, when a source image or a component has been updated.
- The image pipeline workflow includes the build & test phases. The test phase validates whether the image will work as expected before shipping it for production use.
- With Image Builder, you can enhance the security of your deployments by applying AWS security settings for creating images that meet security criteria within an organization.
- Image Builder's integration with AWS RAM allows for easy sharing of Image Builder resources with AWS Accounts or through AWS Organizations.

Use cases:

- Automation for maintaining up-to-date secure images. Amazon EC2 Image Builder significantly reduces the effort here.
- Improving service uptime of images in production. Amazon EC2 Image Builder allows for testing of built images for validating applications on updated builds.
- Integrated Security - Amazon EC2 Image Builder simplifies securing VMs. Images can be configured to only include essential components.


Repeat when updates are pending
Start with a source image
Customize software and configurations
Secure image with AWS-provided or custom hardening templates
Test image with AWS provided or custom tests
Distribute "golden" image to selected AWS accounts and regions

Source: AWS Documentation

Exam Tip:

- Amazon EC2 Image Builder does not incur any cost. The cost comes with associated AWS resources that are used to create, store & share the images.
- Amazon EC2 Image Builder has integrations with AWS RAM, Amazon ECR & AWS Organizations that enable it to share automation scripts, recipes & images across AWS Accounts.
- The Base Image for Image Builder can be an existing AMI, Custom AMI, or AMI from an imported image from VMDK, VHDX, or OVF formats.

—-Back to Index—

Amazon EC2 Auto Scaling

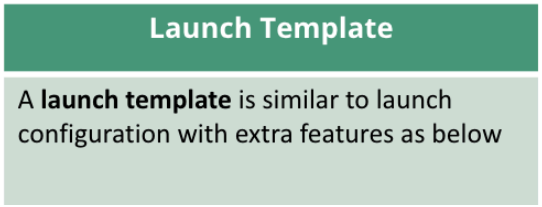
Amazon EC2 Auto Scaling is a region-specific service used to maintain application availability and enables users to automatically add or remove EC2 instances according to the compute workloads.

Features

- The Auto Scaling group is a collection of the minimum number of EC2 used for high availability.
- It enables users to use Amazon EC2 Auto Scaling features such as fault tolerance, health check, scaling policies, and cost management.
- The scaling of the Auto Scaling group depends on the size of the desired capacity. It is not necessary to keep DesiredCapacity and MaxSize equal.
- EC2 Auto Scaling supports automatic Horizontal Scaling (increases or decreases the number of EC2 instances) rather than Vertical Scaling (increases or decreases EC2 instances like large, small, medium).

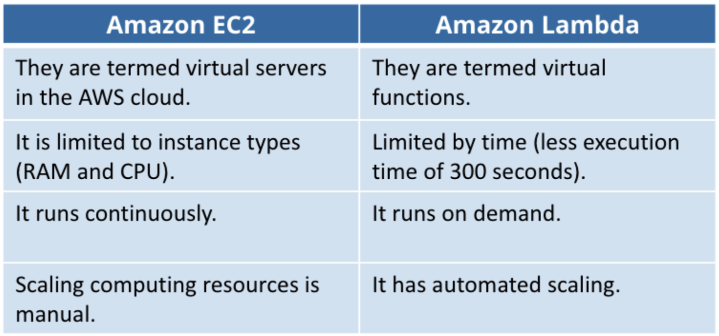
  E.g.,
  DesiredCapacity: '2' -
  There will be total 2 EC2 instances
  MinSize: '1' MaxSize: ‘2

- It scales across multiple Availability Zones within the same AWS region.



Launch Template

A **launch template** is similar to launch configuration with extra features as below



Amazon EC2	Amazon Lambda
They are termed virtual servers in the AWS cloud.	They are termed virtual functions.
It is limited to instance types (RAM and CPU).	Limited by time (less execution time of 300 seconds).
It runs continuously.	It runs on demand.
Scaling computing resources is manual.	It has automated scaling.

Storage

Amazon S3

What is Amazon S3?

- **Amazon S3 (Simple Storage Service)** is an object storage service that allows users to store any type of data in a scalable, secure, and low-cost environment.

Basics of S3

- **Object-Based Storage**: Stores files as objects in **buckets**.
- **Buckets**: Folders for objects, with sizes ranging from 0 to 5 TB.
- **Bucket Naming**: Must be globally unique.
- **Upload Success**: Returns HTTP 200 code for successful uploads.
- **Consistency**: Strong consistency for new objects, overwrites, deletes, and list operations.
- **Privacy**: Objects are private by default.

Properties of Amazon S3

- **Versioning**: Keeps multiple versions of objects within the same bucket.
- **Static Website Hosting**: Hosts static websites without requiring server-side technology.
- **Encryption**: Supports encryption at rest using S3 Managed Keys (SSE-S3) or KMS Managed Keys (SSE-KMS).
- **Object Lock**: Prevents version deletion for a defined period, enabled during bucket creation.
- **Transfer Acceleration**: Speeds up file transfer using Amazon CloudFront's edge locations.

Permissions & Management

- **Access Control List (ACL)**: Grants read/write permissions to other AWS accounts.
- **Bucket Policy**: JSON-based access policies for advanced permissions.
- **CORS (Cross-Origin Resource Sharing)**: Allows cross-origin access to S3 resources.

Charges: **Factors Affecting Charges**:

- Storage
- Requests
- Storage Management (Lifecycle Policies)
- Transfer Acceleration
- Data Transfer

Miscellaneous Topics

- **Access Points**: Makes S3 accessible over the internet.
- **Lifecycle Policies**: Transition objects between storage classes based on lifecycle configuration.
- **Replication**: Replicates data across buckets, either within the same region or across different regions.

—-Back to Index—

Storage class	Suitable for	Durability	Availability	Availability Zones	Min. storage days
S3 Standard	accessed data frequently	100%	99.99%	>= 3	None
S3 Standard-IA	accessed data infrequently	100%	99.90%	>= 3	30 days
S3 Intelligent-Tiering	Storage for unknown access patterns	100%	99.90%	>= 3	30 days
S3 One Zone-IA	Non-critical data	100%	99.50%	1	30 days
S3 Glacier	For long term Data Archival. e.g., 3 years – 5 years	100%	99.99%	>= 3	90 days
S3 Glacier Deep Archive	For long term Data Archival. e.g., 3 years – 5 years	100%	99.99%	>= 3	180 days
RRS (Reduced Redundancy Storage)	Frequently accessed for non-critical data but not recommended	99%	99.99%	>= 3	NA

AWS Backup

What is AWS Backup?

AWS Backup is a secure service that automates and manages data backup for AWS cloud resources and on-premises environments.

Features:

Feature	Description
Backup Management	Offers a backup console, APIs, and AWS CLI to manage backups for AWS resources (e.g., instances, databases).
Policy-Based Backup	Automates backup based on policies, tags, and resources.
Scheduled Backup Plans	Automates backups across AWS accounts and regions with customizable policies.
Incremental Backups	Reduces storage costs by performing full backups initially, followed by incremental backups.
Backup Retention Plans	Automatically retains and expires backups to optimize storage costs.
Backup Monitoring	Provides a dashboard in the AWS Backup console to track backup and restore activities.
Encryption	Supports separate encryption keys for multiple AWS resources.
Lifecycle Policies	Automates the transition of backups from Amazon EFS to cold storage.
Cross-Account Backup	Supports backup and restore across AWS accounts and organizations.
Cross-Region Backup	Enables backup and restore to different regions for disaster recovery and business continuity.
Monitoring & Auditing	Integrates with CloudWatch, CloudTrail, and SNS for monitoring, auditing, and notifications.

Use Cases

- **Hybrid Storage Backup**:
  - Uses AWS Storage Gateway volumes for secure, hybrid storage backup, compatible with Amazon EBS for restoring volumes.

Pricing

- **Charges**: Based on backup storage used and the amount of backup data restored.

Amazon EBS - Elastic Block Store

What is Amazon EBS?

Amazon Elastic Block Store (EBS) is a persistent block-level storage service for Amazon EC2 instances. It is AZ-specific, automatically replicated within its AZ for high availability and durability.

Types of EBS:

SSD-backed volumes (Solid State Drive)	**Optimized for transactional workloads** (small and frequent I/O) - IOPS	
Types SSD	**General Purpose SSD- gp2** (1 GiB — 16 TiB) IOPS : 3000 to 20000 Max / Volume	Boot volumes Development /Test Low-latency Apps Virtual Desktops
	Provisioned IOPS SSD (io1) low-latency or high-throughput Consistent IOPS (16,000+ IOPS) Transactional workloads	MongoDB / NoSQL MySQL / RDS Latency Critical Apps
HDD-backed volumes: (Magnetic Drive)	**Low-Cost throughput-intensive workloads** (Not Suitable for Low Latency(IOPS) -- i.e. booting)	
Types HDD	**Throughput Optimized HDD (st1)** Low Cost - Frequently accessed, throughput-intensive & Large-Sequential O/I -- 500 MB/s	Stream Processing Big Data Processing Data Warehouse
	Cold HDD (sc1) Lowest Cost - less frequently accessed data Throughput : 250 MiB/s	Colder Data requires fewer scans per day.

Features:

- **High Performance:** Single-digit millisecond latency.
- **Highly Scalable:** Scales to petabytes.
- **High Availability & Durability:** 99.999% uptime guarantee.
- **Encryption:** Seamless data encryption with AWS KMS.
- **Automated Backups:** Backups via EBS snapshots to S3 using lifecycle policies.
- **Quick Detach/Attach:** Easily detach from one EC2 instance and attach to another.

Pricing: Charges apply for provisioned capacity, snapshots, and data transfer between AZs/Regions.

EBS vs Instance Store:

- **Instance Store:** Ephemeral, temporary storage with high IOPS, data lost on instance stop/crash. Cannot create snapshots.
- **EBS:** Persistent, reliable storage that can be detached/reattached, boots faster, and supports snapshots.

Amazon EFS - Elastic File Storage

What is Amazon EFS?

Amazon Elastic File System (EFS) is a scalable, fully managed file system based on NFS. It offers persistent storage, scales up to petabytes, and supports parallel access from thousands of EC2 instances. EFS is a regional service, automatically replicated across multiple Availability Zones for high availability and durability.

Types of EFS Storage Classes:

Standard Storage	For frequently accessed files.
Infrequent Access Storage (EFS-IA)	For files not accessed every day Cost-Optimized (costs only $0.025/GB-month) Use EFS Lifecycle Management to move the file to EFS IA

EFS Access and Performance Modes:

- **Performance Modes:**
  - *General Purpose:* Low latency, lower throughput.
  - *Max I/O:* High throughput, higher latency.
- **Throughput Modes:**
  - *Bursting (default):* Throughput grows with file system size.
  - *Provisioned:* Fixed throughput capacity.

Features:

- Fully managed, scalable, and durable NFSv4-based system.
- High availability, low latency (SSD-based).
- POSIX compliant.
- Access across AZs, regions, VPCs, and on-premises via Direct Connect/VPN.
- Lifecycle management for better cost-performance.
- Integrated with AWS DataSync, CloudWatch, CloudTrail.
- Supports encryption in transit (TLS) and at rest (KMS).
- Not suitable for boot volumes or highly transactional databases.

Use Cases:

- Mission-critical apps, microservices, containers, media storage, database backups, analytics, and machine learning.

Best Practices:

- Monitor with CloudWatch, track with CloudTrail.
- Leverage IAM for security, separate latency-sensitive workloads.

Pricing: Pay for storage, access mode, and backup storage used.

Amazon FSx for Windows File Server

Key Features:

Feature	Description
Storage Type	Supports HDD and SSD with high throughput and low latency.
Protocol	Uses **Server Message Block (SMB)** for file access.
Access	Connects to **EC2, ECS, WorkSpaces, AppStream 2.0,** and on-premises via **Direct Connect/VPN.**
High Availability	Multi-AZ deployment with active-standby replication.
Failover Management	Automatic synchronous data replication for seamless failover.
Migration	Uses **AWS DataSync** for migrating self-managed file systems.
Authentication	Identity-based authentication via **Microsoft Active Directory (AD).**
Encryption	**Data at Rest:** AWS KMS; **Data in Transit:** SMB Kerberos session keys.

Use cases:

- **Enterprise File Sharing**
  Enables shared access to multiple datasets across multiple users.
- **Application Migration**
  Supports seamless migration of self-managed applications using **AWS DataSync**.
- **Microsoft SQL Server Workloads**
  Handles **SQL Server Failover** and **data replication** for business-critical applications.
- **Media Processing**
  Ensures **low latency** and **high throughput** for media workloads.
- **Analytics & BI**
  Supports **high-performance analytics**, business intelligence, and data processing applications.

Price details:

- Charges are applied monthly based on the storage and throughput capacity used for the file system's file system and backups.
- The cost of storage and throughput depends on the deployment type, either single-AZ or multi-AZ.

—-Back to Index—

Amazon FSx for Lustre

Key Features:

Feature	Description
Scalable Storage	Supports Lustre, a parallel and high-performance file system.
High Performance	Delivers **sub-millisecond latencies**, **millions of IOPS**, and **hundreds of GBps throughput**.
Storage Options	Offers both **SSD** and **HDD** choices.
Amazon S3 Integration	Uses **parallel data-transfer techniques** to process S3 data.
Automatic Updates	Syncs datasets in S3 as files, not objects, ensuring up-to-date data.
Unreplicated Systems	Allows selection of unreplicated file systems for short-term processing.
Machine Learning	Supports **Amazon SageMaker** for ML workloads.

Use cases:

- The workloads which require shared file storage and multiple compute instances use Amazon FSx for Lustre for high throughput and low latency.
- It is also applicable in media and big data workloads to process a large amount of data.

Price details:

- Charges are applied monthly in GB based on the storage capacity used for the file system.
- Backups are stored incrementally, which helps in storage cost savings.

Amazon S3 Glacier

Category	Description
Purpose	Long-term data archiving and backup.
Cost & Durability	Cheapest S3 storage class with 99.999999999% durability.
Data Types	Stores unlimited data (photos, videos, documents, TAR/ZIP files, data lakes, analytics, IoT, ML, compliance data).
Storage Distribution	Automatically distributes data across Availability Zones in a region.
Retrieval Options	Expedited: 1–5 minutes Standard: 3–5 hours Bulk: 5–12 hours

Features:

- **IAM Integration**: Grants user permissions for vault access.
- **CloudTrail Logging**: Tracks API call activities for auditing.
- **Vaults**: Store archives with options to create, delete, lock, list, retrieve, tag, and configure.
- **Access Policies**: Users can set policies for enhanced security.
- **Retrieval Jobs**: Uses **Amazon SNS** for job completion notifications.
- **S3 Glacier Select**: Queries specific archive objects instead of full retrievals.
- **Supported Format**: Works with **uncompressed CSV**, outputting results to S3.
- **SQL Support**: Uses **SELECT, FROM, WHERE** for queries.
- **Encryption**: Supports **SSE-KMS** and **SSE-S3**.
- **No Real-Time Retrieval**: Archives are not instantly accessible.

Use Cases:

- It helps to store and archive media data that can increase up to the petabyte level.
- Organizations that generate, analyze, and archive large data can make use of Amazon S3 Glacier and S3 Glacier Deep Archive storage classes.
- Amazon S3 Glacier replaces tape libraries for storage because it does not require high upfront cost and maintenance.

Price details:

- Free Usage Tier - Users can retrieve with standard retrieval up to 10 GB of archive data per month for free.
- Data transfer out from S3 Glacier in the same region is free.

—-Back to Index—

AWS Snow Family

AWS Snow Family provides **secure and scalable** data migration and edge computing solutions for environments with limited or no internet connectivity. It includes **AWS Snowball and AWS Snowcone**

Variants

- **Snowball Edge Compute Optimized** – 40 vCPUs, block & object storage.
- **Snowball Edge Storage Optimized** – 52 vCPUs, block & object storage, optional GPU.

1. AWS Snowcone

A small, lightweight edge computing and data transfer device.

Features

- **8TB of usable storage**.
- Secure with **AWS KMS encryption**.
- Supports **Wi-Fi and wired** connectivity.
- Data transfers via **AWS DataSync or shipping to AWS**.
- **Battery-powered** for field deployments.

2. AWS Snowmobile

A **high-capacity** data transfer solution for **exabyte-scale** migrations.

Features

- **Up to 100PB** per Snowmobile.
- **Secure transport** with **GPS tracking, 24/7 monitoring, and military-grade encryption**.
- Transfers data **directly to AWS data centers**.
- Ideal for **large-scale cloud migrations**.

Service	Storage Capacity	Key Features	Use Cases	Pricing
AWS Snowball	50TB - 80TB	Secure, high-speed data transfer	Large-scale migrations, on-prem analytics	Per job, per day, region-based
AWS Snowcone	8TB	Small, portable, battery-powered	Edge computing, IoT data collection	Per job, per day, region-based
AWS Snowmobile	Up to 100PB	Exabyte-scale data migration	Data center migration, massive backups	Custom pricing

AWS Storage Gateway

A **hybrid cloud storage** service that integrates **on-premise storage** with AWS. Available as **AWS hardware or a virtual machine**.

Why Use AWS Storage Gateway?

- **Compliance & Licensing** – Meets regulatory requirements.
- **Cost Reduction** – Lowers storage and management costs.
- **Backup & Automation** – Simplifies application lifecycle and backups.
- **Hybrid Cloud & Migration** – Ensures seamless data transfer to AWS.

Types of AWS Storage Gateway

Type	Function	Key Features
Volume Gateway (iSCSI)	Virtual block storage for on-prem apps	Backups stored in Amazon S3 as snapshots
Stored Volume	Local storage with AWS S3 backup	Ensures high reliability and durability
Cached Volume	Hot data stored locally, rest in S3	Reduces storage costs
File Gateway (NFSv4 / SMB)	Object storage via S3	Mounts S3 as a virtual local file system
Tape Gateway (VTL)	Virtual tape storage for backup	Uses iSCSI-based Virtual Tape Library (VTL) for cost-effective archiving

Features

- **Cost-Effective** – Pay-as-you-go pricing.
- **Low Latency** – Local storage access for faster performance.
- **Hybrid Cloud** – On-prem control with cloud scalability.
- **Compliance & Security** – Meets regulatory and licensing needs.
- **Supports Standard Protocols** – NFS, SMB, iSCSI.

Use Cases

- **Backup & Disaster Recovery** – Reliable, scalable cloud backups.
- **Hybrid Cloud Storage** – On-premises storage integrated with AWS.
- **Cloud Migration** – Easy data movement between on-prem and AWS.

Pricing

- Based on **storage type and usage**. Pay only for what you use.

Database

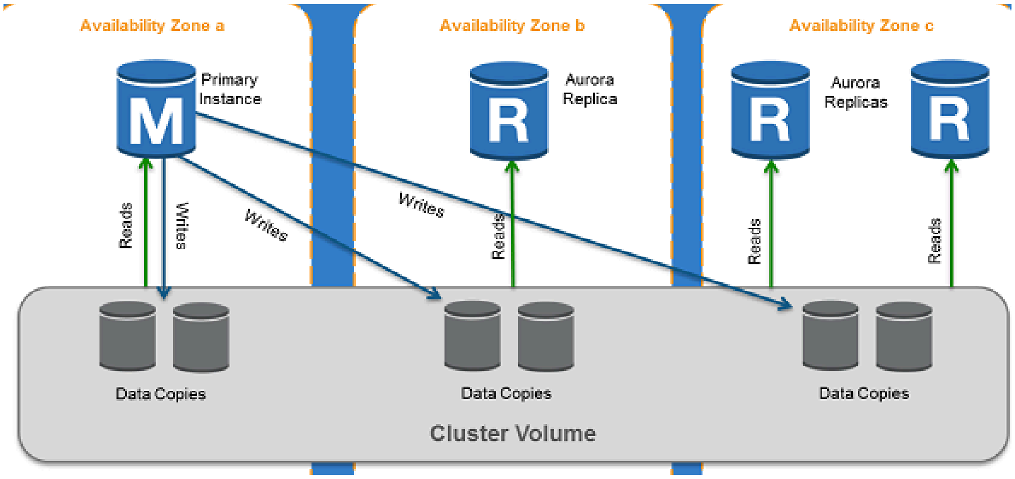
Amazon Aurora

What is Amazon Aurora?

Aurora is the fully managed RDS services offered by AWS**. It's only compatible with PostgreSQL/MySQL.** As per AWS, Aurora provides 5 times throughput to traditional MySQL and 3 times throughput to PostgreSQL.

Features:

- **Availability & Durability:**
  - Supported in regions with at least 3 AZs.
  - 99.99% availability with 6 copies of data (2 per AZ).
  - Up to 15 Read Replicas (RDS allows only 5).
  - Scales up to 128 TB per instance.
- **Aurora DB Cluster:**
  - **Primary DB Instance** – Handles read/write operations.
  - **Aurora Replica** – Read-only, auto-failover with <100 ms lag.
- **Security & Fault Tolerance:**
  - Data resides in VPC with AWS KMS encryption (at rest) and SSL (in transit).
  - **Fault tolerance:** Handles loss of 2 copies (write unaffected) and 3 copies (read unaffected).
  - **Self-healing storage:** Auto-detects and repairs disk errors.
- **Aurora Features:**
  - **Aurora Global Database** – Spans multiple regions for low-latency access and disaster recovery.
  - **Aurora Multi-Master** (MySQL only) – Enables write scaling across AZs, eliminating single points of failure.
  - **Aurora Serverless** – Auto-scales based on load, ideal for intermittent workloads.



Pricing: No upfront fees. On-demand costs more than reserved. Free backups (<1 day retention) and intra-AZ/inbound transfers. Outbound internet transfer is chargeable beyond 1 GB/month.

Amazon DynamoDB

DynamoDB is a **serverless** NoSQL **key-value** and **document** database with **single-digit millisecond latency**. It handles **20M requests/sec** and **10T requests/day** while automatically managing data traffic across servers.

Key Features:

- **Scalability:** Supports automatic scaling and multi-region replication.
- **Flexible Schema:** Stores multi-valued attributes dynamically.
- **Primary Key Types:**
  - **Partition Key:** Unique identifier (e.g., Student_ID).
  - **Partition + Sort Key:** Composite key for better organization.
- **Indexes:**
  - **Global Secondary Index (GSI):** Different partition/sort key from the table.
  - **Local Secondary Index (LSI):** Same partition key, different sort key.

Performance & Acceleration:

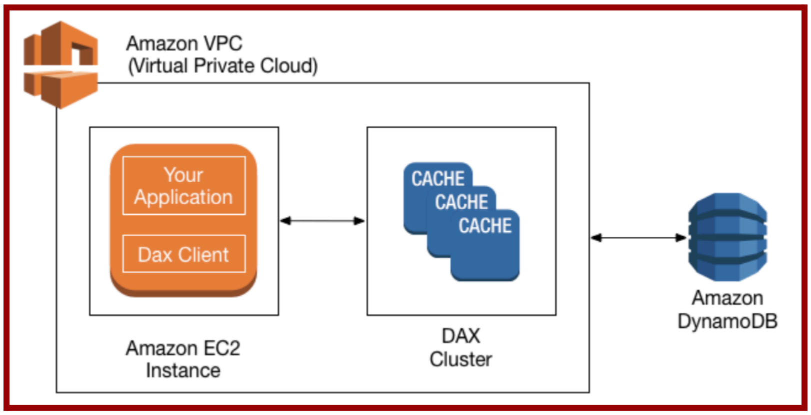
- **DynamoDB Accelerator (DAX):** In-memory caching for 10x performance boost (microseconds latency).
- Supports **horizontal scaling** (read replicas) and **vertical scaling** (node type changes).

Data Access & Operations:

- **Scan:** Retrieves multiple items but is slower than queries (up to **1MB** per operation).
- **Query:** Searches based on **primary key**, with optional **sort key** for filtering.
- **Streams:** Captures real-time item changes, retained for **24 hours**, accessed via **Lambda** or **KCL**.
- **Transactions:** ACID-compliant, supporting **up to 4MB** and **25 unique items** per transaction.

Consistency & Throughput Models:

- **Consistency:**
  - **Eventual Reads:** May return stale data but scales better.
  - **Strong Reads:** Always returns the latest data but has higher latency.
- **Throughput:**
  - **Read Capacity Unit (RCU):** 1 strong or 2 eventual reads (per 4KB).
  - **Write Capacity Unit (WCU):** 1 write per second (1KB).
  - **Provisioned Mode:** Pre-defined capacity for predictable workloads.
  - **On-Demand Mode:** Auto-scales for unpredictable workloads.



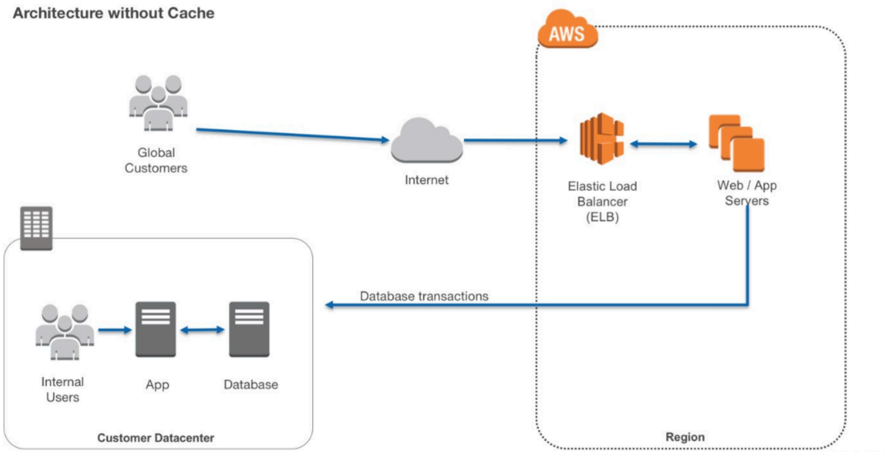
Pricing: **Pay-as-you-go** for disk space, data transfer, and provisioned throughput. Charges apply for **reserved capacity** and **on-demand usage**.

Amazon ElastiCache

ElastiCache is a **fully managed in-memory data store** that boosts **read-heavy workloads** by reducing latency. It supports **Redis** and **Memcached** engines, offering faster performance than disk-based databases.

Key Features:

- **High Availability:** Ensures data access even during maintenance or outages.
- **Key-Value Storage:** Unlike databases, data is retrieved via key-value pairs.
- **Automatic Node Replacement:** Failed nodes are replaced automatically.



Memcached vs. Redis:

Feature	Memcached	Redis
Data Persistence	Volatile	Non-volatile
Data Types	Simple	Complex (strings, hashes, geospatial)
Multi-Threading	Yes	No
Scaling	Add/remove nodes	Add shards (primary + replicas)
Multi-AZ	Not supported	Supported via read replicas
Failover	Not supported	Auto-switch to replica

Best Practices:

- Session Storage: Use Redis for web sessions to ensure data persistence.
- Database Caching: Use Memcached with RDS for faster query performance.
- Live Polling & Gaming: Cache frequently accessed data in Memcached.
- Hybrid Approach: Combine RDS with ElastiCache for backend optimization.

Pricing:

- Charged per node hour (partial hours billed as full).
- Free data exchange within the same AZ.
- Available as on-demand or reserved nodes.

—-Back to Index—

Amazon RDS

Amazon RDS Overview

Amazon RDS is a managed relational database service that simplifies operation, management, and scaling in the cloud. It automates tasks like patching, backups, and provisioning, offering cost-efficient scalability.

Supported Engines:

- MySQL, MariaDB, PostgreSQL – Open-source databases with easy AWS provisioning.
- MS SQL, Oracle – Commercial databases with provisioning and licensing options.
- Amazon Aurora – AWS-native MySQL/PostgreSQL-compatible engine, 5x faster than MySQL, 3x faster than PostgreSQL, supports 15 read replicas.

Instance Classes:

Type	Examples	Use Case
Standard	db.m6g, db.m5, db.m4	General-purpose workloads
Burstable	db.t3, db.t2	Baseline CPU with burst capability
Memory-Optimized	db.z1d, db.x1e, db.r5	Large datasets with high memory needs

High Availability & Performance:

Feature	Multi-AZ Deployment	Read Replicas
Replication	Synchronous	Asynchronous
Purpose	Disaster Recovery	Performance Enhancement
Scope	Two AZs in a region	Cross-AZ or cross-region
Failover	Automatic	Manual promotion

Storage Types:

- General Purpose (SSD): Baseline 3 IOPS/GiB, bursts up to 3,000 IOPS.
- Provisioned IOPS (SSD): High-performance storage, supports 1,000–30,000 IOPS.

Monitoring & Backups:

- Enhanced Monitoring: Disabled by default, incurs extra charges.
- Backups: Default retention 7 days (Console), 1 day (CLI/API), max 35 days.
- Manual Snapshots: 100 per region.

Pricing Factors:

- Active instances, storage, requests, backups, enhanced monitoring, cross-region replication.

—-Back to Index—

Security, Identity, & Compliance

AWS IAM

Identity and Access Management (IAM)

IAM is an AWS service that **securely controls access** to AWS resources by managing **users, groups, roles, and policies**.

Key Components

Principals

- **Root User** – Created with an AWS account, has full access.
- **IAM User** – Represents a person/service with assigned permissions.
- **IAM Group** – Collection of users with shared permissions.
- **IAM Role** – Temporary identity with policies, used by federated users or AWS services.

Policies

- **Identity-Based Policies** – Define access for users, groups, and roles.
  - **AWS Managed** – Predefined by AWS.
  - **Customer Managed** – Created by users for fine-grained control.
  - **Inline** – Directly attached to a user, group, or role.
- **Resource-Based Policies** – Control access at the resource level (e.g., S3 bucket).

Best Practices

✔ Grant **least privilege access**.
✔ Enable **MFA** for users.
✔ Monitor with **AWS CloudTrail**.
✔ Enforce **strong password policies**.
✔ **Use policy conditions for security.**

Pricing

IAM is **free**; charges apply only for AWS services used by IAM users.

AWS Directory Service

AWS Directory Service (AWS Managed Microsoft AD) enables **Microsoft Active Directory (AD) integration** with AWS services, supporting **authentication, schema extensions, and AD-dependent applications** like SharePoint and SQL Server.

Key Features

✔ **Trust relationships** – Extend on-premises AD authentication to AWS.
✔ **Patching without downtime** – Ensures high availability.
✔ **Supports Windows & Linux** domain-joining for EC2 instances.
✔ **Single Sign-On (SSO)** – Integrate AWS Managed AD with on-premises AD.

Limitations

❌ No **MFA**, **trust relationships**, **LDAPS communication**, or **PowerShell AD cmdlets**.

Additional Components

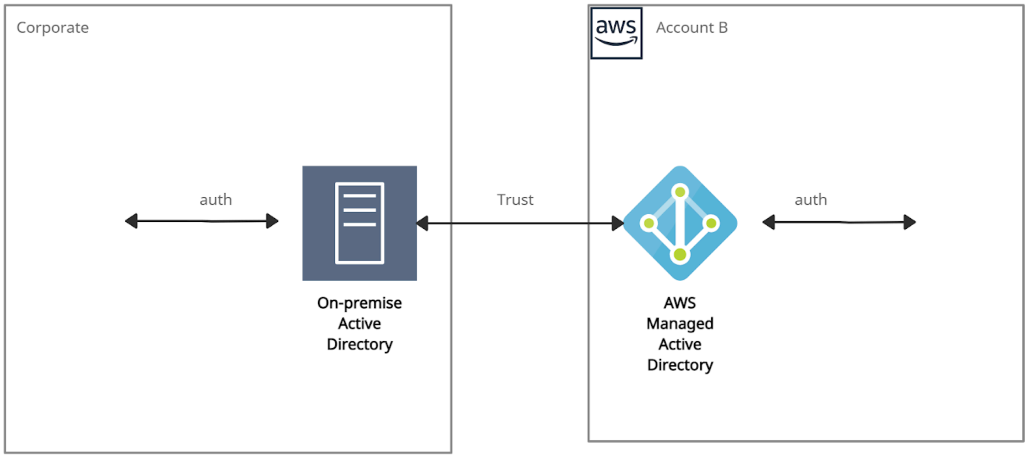
✔ **Amazon Cognito** – Provides **user authentication** via Cognito User Pools, supports **SAML-based federation** for external identities.
✔ **AD Connector** – Acts as a **gateway** redirecting directory requests to **on-premises AD**. Requires **VPN or Direct Connect**. Supports **MFA via RADIUS**.

Use Cases

✔ Sign in to AWS Cloud services with **AD credentials**.
✔ Provide **directory services** to AD-aware workloads.
✔ Enable **SSO** for Office 365 and cloud applications.
✔ Extend **on-premises AD to AWS** via **AD trusts**.

Pricing

✔ Varies by **region**.
✔ **Hourly charges** for shared directories.
✔ **Data transfer charges** for cross-region directory sharing.



AWS Managed AD

AWS Secrets Manager

AWS Secrets Manager securely stores, rotates, and retrieves sensitive credentials like database passwords, API keys, and OAuth tokens, replacing hardcoded secrets with API calls. It ensures encryption in transit and integrates with AWS KMS for encryption at rest.

Key Features

✔ Automated secret rotation for AWS databases (RDS, Aurora, Redshift, DocumentDB).
✔ Custom secret rotation via AWS Lambda for non-AWS services.
✔ Secure access control using IAM and resource-based policies.
✔ Monitoring & auditing with AWS CloudTrail and CloudWatch.

Access Methods

✔ AWS Console, CLI, SDKs, PowerShell, HTTPS API.

Use Cases

✔ Store encrypted secrets in SecretString/SecretBinary.
✔ Cache secrets using an open-source client for efficient access.
✔ Monitor changes with AWS Config.

Pricing

✔ Pay per stored secret and API calls.
✔ Additional charges for AWS KMS encryption keys.

—-Back to Index—

AWS Security Hub

AWS Security Hub provides a **centralized view of security alerts and compliance status** across AWS accounts and services, helping organizations adhere to **security best practices**.

Key Features

✔ **Aggregates security alerts** from AWS services like:

- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- AWS IAM Access Analyzer
- AWS Firewall Manager

  ✔ **Integrates with AWS Partner security solutions**.

  ✔ **Automated compliance checks** against:

- **PCI DSS** (Payment Card Industry Data Security Standard)
- **CIS AWS Foundations Benchmark** (43 best practices, e.g., IAM password policies).

  ✔ **Prioritizes findings** and suggests **remediation steps**.

Enabling Security Hub

✔ **AWS Management Console**

✔ **AWS CLI**

✔ **Infrastructure-as-Code tools (Terraform, etc.)**

✔ **Multi-region setup required** for full coverage.

Benefits:

- It collects data using a standard findings format and reduces the need for time-consuming data conversion efforts.
- Integrated dashboards are provided to show the current security and compliance status.

Price details:

- Charges applied for usage of other services that Security Hub interacts with, such as AWS Config items, but not for AWS Config rules that are enabled by Security Hub security standards.
- Using the Master account's Security Hub, the monthly cost includes the costs associated with all of the member accounts.
- Using a Member account's Security Hub, the monthly cost is only for the member account.
- Charges are applied only for the current Region, not for all Regions in which Security Hub is enabled.

AWS Key Management Service

AWS KMS is a **secure service** for creating and managing encryption keys, integrated with AWS services like Amazon S3 and EBS for **data encryption at rest**.

Key Concepts

✔ **Regional Keys** – Keys cannot be shared across regions.
✔ **Customer Master Keys (CMKs)** – Stores key metadata and is used for encryption.
✔ **Types of CMKs:**

- **Symmetric CMKs** – Single 256-bit key for encryption/decryption.
- **Asymmetric CMKs** – RSA/ECC key pairs for encryption/decryption or signing/verification.

CMK Management

✔ **Customer-Managed CMKs** – Fully controlled by users, visible in AWS KMS console.
✔ **AWS-Managed CMKs** – Created and managed by AWS, used by AWS services.

Envelope Encryption

✔ Encrypts plaintext with a **data key**, then encrypts the data key with a **master key**.
✔ Benefits:

- Protects data keys.
- Supports multiple master keys.
- Enhances security with multiple algorithms.

Features

✔ **Automatic key rotation** (yearly) without re-encryption.
✔ **AWS CloudTrail logging** for auditing.
✔ **Auto-scaling** to support encryption growth.
✔ **High availability** with multiple encrypted key copies.

Pricing

✔ **Free Tier** – 20,000 requests/month.
✔ **Customer-Managed CMKs** – $1/month per key.
✔ **AWS-Managed CMKs** – Free but limited to AWS service use.

AWS Certificate Manager (ACM)

AWS ACM provides, manages, renews, and deploys **SSL/TLS X.509 certificates** for secure web communications. Users can issue ACM certificates or import third-party certificates.

SSL Server Certificates

✔ **X.509 certificates** authenticate HTTPS transactions.
✔ Issued by a **Certificate Authority (CA)** and include server name, validity period, and public key.

Types of SSL Certificates

✔ **EV SSL** – Highest security, most expensive.
✔ **OV SSL** – Validates business credibility.
✔ **DV SSL** – Basic encryption.
✔ **Wildcard SSL** – Secures base domain + subdomains.
✔ **Multi-Domain SSL (MDC)** – Secures multiple domains/subdomains.
✔ **UCC** – Secures multiple domain names in one certificate.

Deployment Options

✔ **AWS Certificate Manager (ACM)** – Used for public certificates, deploys via **API Gateway, ELB, CloudFront**.
✔ **ACM Private CA** – Creates internal **PKI** to issue private certificates for internal authentication.

ACM-Integrated Services

✔ **Elastic Load Balancing, CloudFront, API Gateway, Elastic Beanstalk, AWS Nitro Enclaves, CloudFormation**.

Benefits

✔ **Automated creation & renewal** of SSL/TLS certificates.
✔ Simplifies **certificate issuance** and management.
✔ Ensures **data-in-transit security** and site authentication.

Pricing

✔ **Public ACM certificates** – Free when used with ACM-integrated services.
✔ **ACM Private CA** – Monthly charges for private CA operation and issued certificates.

Amazon Detective

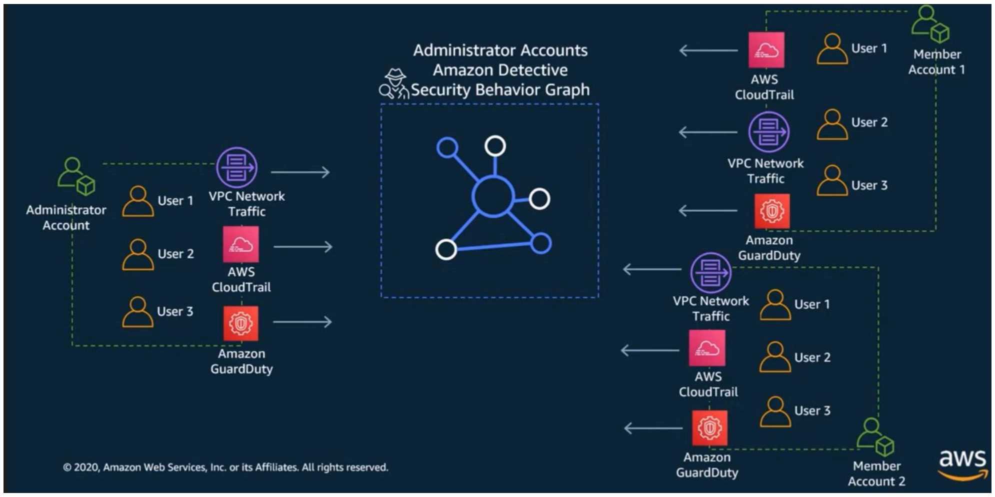
Amazon Detective is a service that makes it easy to analyze, investigate & quickly find out the root cause of security findings or suspicious activities within your AWS environment using ML, Statistical analysis, and Graph theory.
It does it by automatically collecting and processing events from VPC Flow logs, CloudTrail, and Amazon GuardDuty to create a unified view.

Features:

- **Multi-Account Integration:**
  - Enabled in an AWS Organizations Management account, where member accounts are invited and connected.
- **Security Behavior Graph:**
  - Aggregates CloudTrail events, VPC traffic, and GuardDuty findings from all member accounts into a central graph.
- **Contextual Insights:**
  - Provides security-related relationships and interactive visualizations using Generative AI for quick investigation and correlation of data.
- **Seamless Integration:**
  - Works with AWS security services such as GuardDuty, Security Hub, and Inspector to consolidate findings.
- **Cost-Effective:**
  - No need to enable or configure additional data sources, keeping costs low.

Exam Tip:

- GuardDuty must be active for at least 48 hours before enabling Amazon Detective.
- The data volume flowing into the Security Behavior Graph must remain below Detective's maximum limit.
- Amazon Detective is a regional service and must be enabled individually in each region.



Source: AWS Documentation

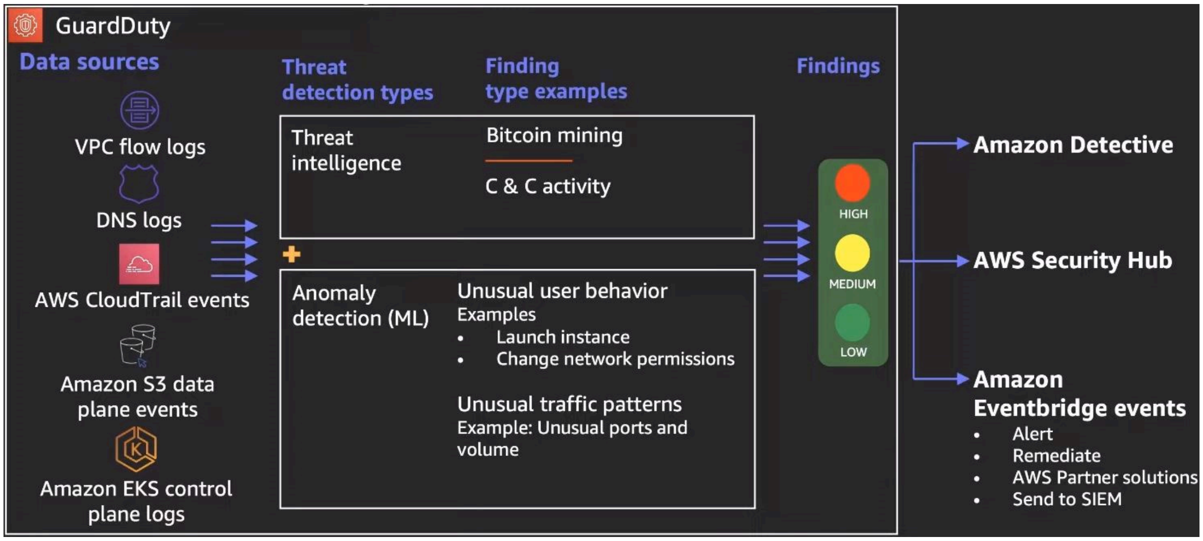
—-Back to Index—

Amazon GuardDuty

Amazon GuardDuty is a threat detection service which uses Machine Learning, Anomaly detection, and threat intelligence for identifying and prioritizing potential threats within your AWS accounts & resources.
It does it by monitoring different log sources like VPC flow logs, DNS logs, CloudTrail events, S3 data plane events, and EKS control plane logs and analyzing them.

Features

- **Threat Detection Service:** Uses machine learning, anomaly detection, and threat intelligence to identify potential threats.
- **Log Monitoring:** Analyzes VPC flow logs, DNS logs, CloudTrail events, S3 data plane events, and EKS control plane logs.
- **Prioritization:** Helps prioritize security issues across AWS accounts and resources.



Best Practices:

- Ensure GuardDuty has full log visibility by enabling VPC Flow Logs for all regions and critical network interfaces.
- Enable GuardDuty in every region to achieve comprehensive threat detection.
- Use CloudTrail to monitor GuardDuty activities and detect any tampering.
- Integrate GuardDuty with EventBridge and Lambda for automated risk mitigation.

Use Cases:

- Assist security analysts with investigation using GuardDuty's detailed security event findings, including context, metadata, and impacted resource details via integration with Amazon Detective.
- Detect malware by scanning files on EBS and monitoring suspicious behaviors in EC2 and container workloads.

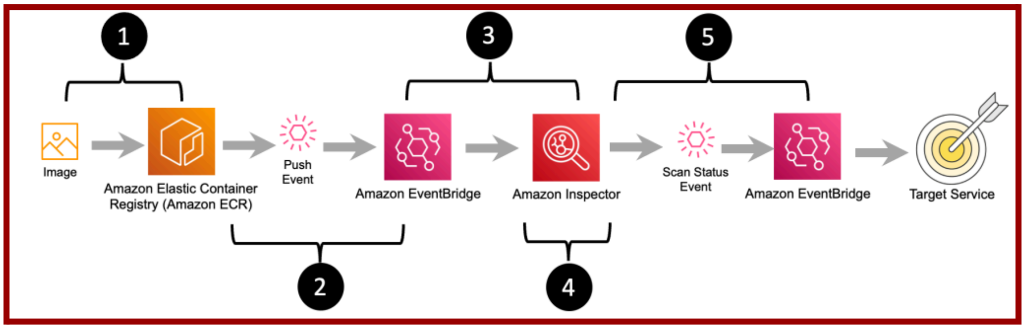
Exam Tip:

- When GuardDuty is enabled, its required log sources (VPC Flow Logs, DNS Logs, CloudTrail, S3 data plane events, and EKS control plane logs) are automatically enabled; you cannot add additional log sources.

Amazon Inspector

Amazon Inspector is a vulnerability management service which continuously scans AWS resources for software vulnerabilities and network accessibility.
When activated, Amazon Inspector discovers known vulnerabilities in EC2 instances, container images/ECR, Lambda functions and provides a consolidated view of vulnerabilities across compute environments.

Feature	Description
Vulnerability Scanning	- Automatically scans AWS resources (EC2, Lambda, container workloads) for vulnerabilities. - Uses Generative AI and automated reasoning to provide in-context code remediation suggestions.
Multi-Account Support & Integration	- Supports AWS Organizations via an Inspector Delegated Administrator (DA) account to configure and consolidate findings across member accounts. - Integrates with AWS Systems Manager Agent to collect software inventory and configurations.
Findings Management	- Generates a highly contextualized risk score for each finding. - Allows suppression of findings deemed acceptable through configurable rules. - Automatically closes findings once vulnerabilities are patched.
Monitoring & Automation	- Provides detailed, organization-wide monitoring to avoid gaps in coverage. - Integrates with AWS Security Hub and EventBridge to automate workflows like ticketing.
CI/CD Integration	- Scans Lambda functions for security vulnerabilities such as injection flaws and missing encryption. - Integrates with CI/CD tools like Jenkins for proactive container image assessments.



Source: AWS Documentation

Exam Tip:

- New Amazon Inspector expands its coverage to support container images residing in ECR's in addition to EC2 instances.
- The widely adopted Systems Manager Agent used by Amazon Inspector replaces the standalone Inspector Classic Agent.

AWS WAF

AWS WAF is a web application firewall that helps protect web applications from common web exploits and attacks.

It acts as a protective shield for your web applications, helping you safeguard them from threats like SQL injection, cross-site scripting (XSS), and other malicious activities.

Features:

- **Web Traffic Filtering:** AWS WAF allows you to filter and inspect web traffic coming to your applications. You can set up rules to allow, block, or monitor traffic based on various criteria, such as IP addresses, HTTP headers, request methods, and query strings.
- **Protection Against Common Attacks:** It protects a wide range of common web attacks, including SQL injection, XSS, and cross-site request forgery (CSRF).
- **Custom Rules:** You can create custom rules to address specific security requirements and business logic.
- **AWS WAF Managed Rules for AWS Organizations:** This feature allows you to centrally manage and deploy WAF rules across multiple AWS accounts within an AWS Organization.

Pricing:

- **Pricing Factors for AWS WAF:**
  - Number of web access control lists (web ACLs) you create.
  - Number of rules within each web ACL.
  - Volume of incoming web requests.
- **No Upfront Commitments:**
  - There are no prior commitments or contracts required for AWS WAF.
- **Separate Charges:**
  - AWS WAF costs are independent and do not include charges for services like Amazon CloudFront, AWS Cognito, Application Load Balancer (ALB), Amazon API Gateway, or AWS AppSync.

Management & Governance

AWS CloudFormation

AWS CloudFormation automates resource provisioning and management using **templates** to create, update, and delete stacks as a **single unit**. It integrates with **IAM for security** and **CloudTrail for API event tracking**.

Key Concepts

✔ **Templates** – JSON/YAML files for defining AWS resources.
✔ **Stack** – A collection of resources managed together.
✔ **Change Sets** – Preview changes before applying them.
✔ **Stack Updates** – Update only modified resources.
✔ **StackSets** – Manage stacks across multiple accounts/regions.
✔ **Nested Stacks** – Reuse common components within stacks.
✔ **CloudFormation Registry** – Supports third-party resource provisioning.

Pricing

✔ **Free for AWS resources**; charges apply for the services used.
✔ Supports _AWS::*, Alexa::*, and Custom:: namespaces_*; others incur costs.
✔ **Free tier:** 1000 handler operations/month.
✔ **Paid operations:** $0.0009 per handler operation.

Example: EC2 Instance Template

```
EC2Instance:
  Type: AWS::EC2::Instance
  Properties:
    ImageId: 1234xyz
    KeyName: aws-keypair
    InstanceType: t2.micro
    SecurityGroups:
      - !Ref EC2SecurityGroup
    BlockDeviceMappings:
      - DeviceName: /dev/sda1
        Ebs:
          VolumeSize: 50
```

AWS CloudTrail

AWS CloudTrail enables operational and risk auditing by tracking account activity across AWS services. It records actions as events from users, roles, and AWS services via the Console, CLI, SDKs, and APIs.

Integrations

✔ Amazon S3 – Stores and retrieves log files.
✔ Amazon SNS & SQS – Notifies on log file delivery.
✔ Amazon CloudWatch & IAM – For monitoring and security.
✔ CloudTrail Insights – Detects unusual API activity.
✔ Log Retention – Past 90 days of events can be viewed/downloaded.

Event Types

✔ Management Events (e.g., CreateSubnet, CreateDefaultVpc)
✔ Data Events (e.g., GetObject, DeleteObject, PutObject)
✔ Insights Events (e.g., deleteBucket, AuthorizeSecurityGroupIngress)

CloudTrail vs. CloudWatch

✔ CloudTrail – Logs all AWS actions for auditing.
✔ CloudWatch – Monitors AWS services for performance & health.

Pricing

✔ First copy of management events per region is free.
✔ Additional copies: $2.00 per 100,000 events.
✔ Data events: $0.10 per 100,000 events.
✔ Insights events: $0.35 per 100,000 analyzed events.

Amazon CloudWatch

Amazon CloudWatch monitors and manages AWS applications and infrastructure by collecting logs, metrics, and events. It supports **EC2, RDS, DynamoDB, and custom log files**.

Access Methods

✔ **CloudWatch Console**
✔ **AWS CLI, API, SDKs**

Integrations

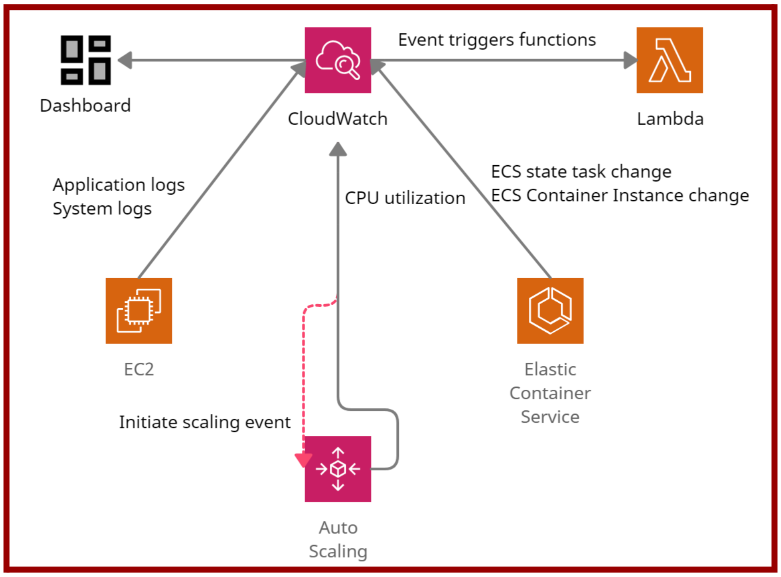
✔ **Amazon SNS** – Sends notifications
✔ **EC2 Auto Scaling** – Adjusts resources
✔ **AWS CloudTrail & IAM** – Security & auditing

Key Features

✔ **Custom Dashboards** – Visualize metrics
✔ **Alarms** – Trigger actions on threshold breaches
✔ **Cross-Account Visibility** – Unified monitoring across AWS accounts
✔ **Container Insights** – Monitors ECS, EKS, Kubernetes
✔ **Lambda Insights** – Tracks CPU, memory, disk, and network usage

CloudWatch Agent

✔ Collects **system-level metrics** from EC2/on-prem servers.
✔ Supports **StatsD (Linux/Windows)** and **collectd (Linux)** for custom metrics.
✔ Default namespace: **CWAgent** (configurable).



Amazon CloudWatch in action

AWS Config

AWS Config **monitors, evaluates, and records** AWS resource configurations, tracking changes over time.

Key Features

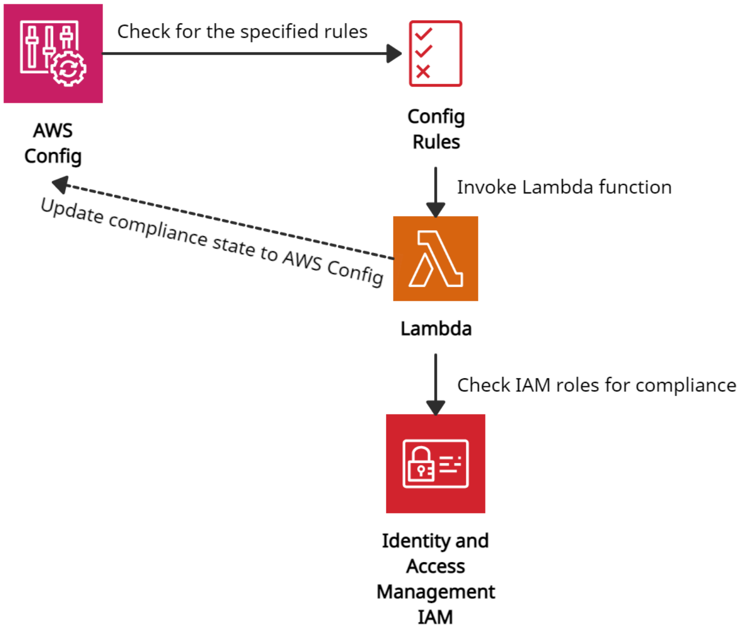
✔ **Configuration Snapshots** – Provides a complete resource inventory.
✔ **Change Tracking** – Records modifications and sends notifications.
✔ **Compliance Checks** – Uses **Managed** & **Custom Config Rules** (150 per region).
✔ **Integration** – Works with **IAM, S3, SNS, and CloudTrail** for auditing and alerts.
✔ **Aggregators** – Collects compliance data across multiple **accounts, regions, or AWS Organizations**.

Use Cases

✔ **Automates compliance checks** using Lambda-based custom rules.
✔ **Identifies security risks** and tracks historical configurations for analysis.

Pricing

✔ **$0.003 per configuration item recorded per region**.
✔ **Charges for Config rule evaluations** and **integrations with AWS services**.


Check for the specified rules
AWS Config
Config Rules
Invoke Lambda function
Update compliance state to AWS Config
Lambda
Check IAM roles for compliance
Identity and Access Management IAM

AWS Config in action

AWS License Manager

AWS License Manager **manages software licenses** for AWS and on-premises environments, supporting **Bring-Your-Own-License (BYOL)** for vendors like Microsoft, SAP, Oracle, and IBM.

Key Features

✔ **Custom Licensing Rules** – Prevents violations with **hard (blocks) & soft (alerts) limits**.
✔ **Dashboard Control** – Provides visibility and enforcement of license usage.
✔ **Dedicated Host Management** – Optimizes allocation & capacity utilization.
✔ **Managed Entitlements** – Controls license assignments for users/workloads.
✔ **Cross-Account Management** – Uses **AWS Organizations** for license sharing.
✔ **Integration** – Works with **EC2, RDS, Systems Manager, IAM, Marketplace, CloudFormation, X-Ray**.

Pricing

✔ No additional charges; **AWS resources follow standard pricing**.

AWS Organizations

AWS Organizations **manages multiple AWS accounts**, enforcing security, governance, and cost tracking.

Access Methods

✔ **Console, CLI, SDKs, API, PowerShell**

Key Features

✔ **Security Boundaries** – Uses multiple member accounts.
✔ **Organizational Units (OUs)** – Groups accounts for better management.
✔ **Service Control Policies (SCPs)** – Enforces security & governance.
✔ **Cost Allocation Tags** – Tracks AWS costs per account.

Integration with AWS Services

✔ **CloudTrail** – Auditing & logging
✔ **Backup** – Backup monitoring
✔ **Control Tower** – Cross-account security & policy view
✔ **GuardDuty** – Threat detection
✔ **Resource Access Manager (RAM)** – Resource sharing

Member Account Migration

1️⃣Remove from old Organization
2️⃣Send invitation from new Organization
3️⃣Accept invitation from member account

Pricing

✔ **Free service**; standard charges apply for AWS resources.
✔ **Consolidated billing** ensures volume discounts across accounts.

AWS Systems Manager

AWS Systems Manager **manages EC2 and on-premises systems at scale**, detects infrastructure issues, and automates patching for compliance. Works with **Windows & Linux**.

Key Features

✔ **Integration** – Works with CloudWatch & AWS Config
✔ **Software Discovery** – Audits installed software
✔ **Compliance Management** – Monitors patch levels & configurations
✔ **Resource Grouping** – Over 100 resource types into applications & units
✔ **Automated Workflows** – Reduces errors with centralized parameters
✔ **Security & Patching** – Runs commands & scheduled patching
✔ **Software Distribution** – Manages multiple versions safely

How it Works

- **SSM Agent** must be installed on controlled systems.
- **IAM Role** required for EC2 instances to allow SSM actions.

Pricing

✔ **App Config** – $0.2 per 1M API calls, $0.0008 per config received
✔ **Parameter Store** – Standard (Free), Advanced ($0.05/param/month)
✔ **Change Manager** – $0.296 per change request, $0.039 per 1K API calls

AWS Health dashboard

AWS Health Dashboard **provides real-time service events, scheduled changes, and account notifications**, enabling proactive issue resolution. Access updates via **AWS Health API (Premium Support), EventBridge, or the console**.

Key Features

✔ **Centralized Hub** – Integrates with 200+ AWS services for full visibility
✔ **Actionable Insights** – Helps troubleshoot & manage changes proactively
✔ **AWS Organizations Integration** – Consolidates service health across accounts
✔ **Automated Notifications** – Receive alerts via **EventBridge & ITSM tools**

Use Cases

✔ **Proactive Alerts** – Minimize disruptions with real-time updates
✔ **Lifecycle Event Monitoring** – Track planned events & resource-level actions
✔ **Efficient Event Tracking** – Automate monitoring via ITSM integrations
✔ **Incident Troubleshooting** – Identify AWS-related issues affecting applications

—-Back to Index—

AWS Control Tower

AWS Control Tower **extends AWS Organizations** by providing governance and multi-account management with a **Landing Zone** based on AWS best practices.

Key Features

✔ **Preconfigured OUs** – Security (Audit & Log Archive), Sandbox, and Production
✔ **Identity Integration** – Supports AWS Identity Center, SAML IdPs, and Microsoft AD
✔ **Guardrails** – Preventive (SCP-based) & Detective (AWS Config & Lambda-based)
✔ **Centralized Dashboard** – Monitors accounts, OUs, and compliance policies
✔ **Account Factory** – Standardized account provisioning with pre-approved configurations

Use Cases

✔ **New or Existing AWS Organization Deployment** – Works with both setups
✔ **Automated Governance & Compliance** – Ensures policy enforcement across accounts

AWS Trusted Advisor

AWS Trusted Advisor provides best practice checks in Cost Optimization, Security, Fault Tolerance, Performance, and Service Limits to enhance AWS infrastructure.

Key Features

✔ Cost Optimization – Identifies unused/idle resources and recommends Reserved capacity
✔ Security – Checks S3 permissions, security groups, and NACLs for vulnerabilities
✔ Fault Tolerance – Suggests Auto Scaling, Multi-AZ, and backup configurations
✔ Performance – Recommends throughput optimization and monitors resource utilization
✔ Service Limits – Alerts when resource usage exceeds 80%

Use Cases

✔ Reduce Costs – Detect idle resources and optimize usage
✔ Enhance Security – Identify misconfigurations and access risks
✔ Improve Performance – Optimize resource allocation and scaling

Migration & Transfer

AWS DataSync

Description: A managed service for secure, automated data migration between AWS, on-premises, edge locations, and other cloud providers.

Features

- Supports scheduling, bandwidth throttling, task filtering, and logging.
- Uses compression and parallel transfers for faster data movement.
- Provides in-flight (TLS) and at-rest encryption.
- Ensures data integrity verification.
- Integrates with CloudWatch, CloudTrail, and EventBridge.
- Pay-as-you-go pricing ($0.0125/GB).

Best Practices

- Evaluate tools, bandwidth, and source/destination before migration.
- Deploy & activate an **Agent** for on-premises to AWS transfers.
- Combine **DataSync** for archiving and **Storage Gateway** for local access.
- Use **Lambda** to trigger transfers when schedules are undefined.
- No Agent needed for AWS-to-AWS transfers (e.g., S3 → S3, S3 → EFS).

AWS Migration Hub

Description: A centralized platform for discovering, planning, and tracking application migrations, offering visibility across tools and processes.

Benefits

- **Streamlined Process:** Manage discovery, assessment, planning, execution, and tracking in one place.
- **Guided Expertise:** Use pre-built templates for faster migration.
- **Effective Resources:** Leverage specialized services for transformation.
- **Free to Use:** No cost for planning or tracking migrations.

Use Cases

- **Migration Planning:** Identify applications and develop migration strategies.
- **Migration Execution:** Use guided templates and services for seamless migration.
- **Application Modernization:** Refactor and manage applications efficiently.

Pricing

- **Free** for discovery, planning, and tracking migrations.
- Users pay for migration tools and AWS resources.
- **Refactor Spaces:**
  - 3 environments free for 3 months (2,160 hours/month).
  - After free tier: **$0.028/hour** per environment ($20/month if run continuously).
  - **API Requests:** $0.000002/request, with **500,000 free/month** in AWS Free Tier.

—-Back to Index—

AWS Transfer Family

Category	Description
Service Overview	AWS Transfer Family is a fully managed, secure service that enables file transfers to/from AWS storage (S3, EFS) and on-premises systems using SFTP, FTPS, and FTP. It simplifies migration of file transfer workloads without impacting existing integrations.
SFTP	Secure File Transfer Protocol that uses SSH for encrypted file transfers.
FTPS	FTP over a TLS-encrypted channel, providing secure file transfers.
FTP	Standard File Transfer Protocol without encryption; typically used within a VPC via VPC endpoints for enhanced security.
Key Features	- Fully managed endpoints for S3 and EFS - Global high availability - Compliance with regional regulations - Pay-as-you-go pricing - Custom Identity Providers using API Gateway & Lambda
Use Cases	- Secure file transfers with IAM roles for S3 access - Migrating existing file transfer hostnames using Route 53 - Public access for SFTP/FTPS and restricted internal FTP access via VPC endpoints

Networking & Content Delivery

Amazon API Gateway

Category	Description
Overview	Amazon API Gateway creates, publishes, monitors, and secures APIs at any scale, powering both serverless and microservices architectures.
API Types	**REST APIs:** HTTP-based, stateless communication with standard methods (GET, POST, PUT, PATCH, DELETE). **WebSocket APIs:** Stateful, full-duplex communication.
Endpoint Types	**Edge-Optimized:** Global low latency with CloudFront. **Regional:** Optimized for same-region requests with CDN/WAF. **Private:** Restricted to VPC access.
Security	Secured using resource policies, IAM, Lambda authorizers, and Cognito user pools.
Integrations	Works with EC2, Lambda, CloudTrail, CloudWatch, AWS WAF, and X-Ray.
Pricing	Charges apply for API caching; auth failures, missing API keys, and throttled requests are free.

Amazon CloudFront

Category	Description
Overview	Amazon CloudFront is a CDN that securely delivers content worldwide with low latency and high transfer speeds by caching data at edge locations.
Integrations	Works with AWS services such as S3, EC2, ELB, Route 53, and Elemental Media Services.
Origins	Retrieves content from Amazon S3, EC2, ELB, or custom HTTP origins.
Edge Computing	Supports Lambda@Edge for custom code execution, dynamic load-balancing, and enhanced security at the edge.
Security	Provides HTTPS encryption (including field-level), AWS Shield Standard for DDoS protection, AWS WAF, and Origin Access Identity (OAI) to secure S3 content.
Access Controls	Uses signed URLs, signed cookies, and geo-restrictions to control access to content.
Pricing	Charged for data transfer out, HTTP/HTTPS requests, custom SSL certificates, field-level encryption, and Lambda@Edge execution. Free for inter-region transfers, ACM, and shared certificates.

AWS Transit Gateway

Overview:

- Central hub to interconnect multiple VPCs.
- Simplifies complex VPC peering and hybrid connectivity.
- Manages AWS routing configurations in one place.

Connectivity:

- Supports multiple Transit Gateways per region (cannot peer within a single region).
- Connects with AWS Direct Connect gateway (across different AWS accounts).
- Enables IPsec VPN connections via VPN attachments.
- Supports IPv6 CIDRs for VPC attachments.

Management:

- Create via AWS CLI, Management Console, or CloudFormation.
- Transit Gateway Network Manager monitors networking resources and remote branch connections.
- Allows multi-user gateway connections for redundancy.

Transit Gateway vs. VPC peering:

Transit Gateway	VPC peering
● It has an hourly charge per attachment in addition to the data transfer fees. ● Multicast traffic can be routed between VPC attachments to a Transit Gateway. ● It provides Maximum bandwidth (burst) of 50 Gbps per Availability Zone per VPC connection. ● Security groups feature does not currently work with Transit Gateway.	● It does not charge for data transfer. ● Multicast traffic cannot be routed to peering connections. ● It provides no aggregate bandwidth. ● Security groups feature works with intra-Region VPC peering.

AWS Direct Connect

Establishes a dedicated network connection from an on-premises environment to one or more AWS VPCs in the same region. Bypasses the public Internet for a more consistent network experience.

Virtual Interfaces:

- **Private VIF:** Connects to an Amazon VPC using private IP addresses.
- **Public VIF:** Connects to AWS services (except in China) using public IP addresses.

Connection Options:

- AWS Managed VPN, Direct Connect, Direct Connect + VPN, VPN CloudHub, Transit VPC, VPC Peering, AWS PrivateLink, VPC Endpoints.

Direct Connect Gateway:

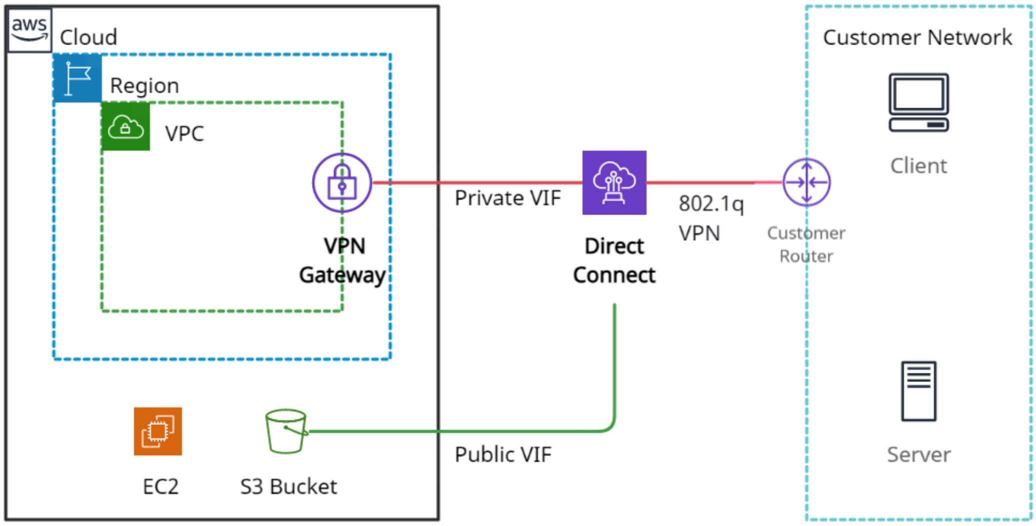
- Globally available service to connect multiple VPCs across regions or AWS accounts.
- Integrates with:
  - **Transit Gateway:** Connects multiple VPCs to an on-premises network within the same region.
  - **Virtual Private Gateway:** Provides edge routing for VPCs.

Key Features:

- Configurable via the AWS Management Console.
- Provides scalable dedicated connections (1 Gbps and 10 Gbps options).
- Ensures consistent connectivity with improved performance.

Pricing:

- Pay-as-you-go with no minimum fee.
- Charged per dedicated connection port hour (uniform globally, except Japan).
- Data Transfer OUT charges vary based on the AWS Region.



Amazon Direct Connect

AWS Elastic Load Balancer

Distributes incoming traffic across multiple targets (EC2, containers, Lambda, IPs) across one or more Availability Zones for high availability, scalability, and security.

Types:

- **Application Load Balancer:** Ideal for web apps; routes traffic based on request content.
- **Network Load Balancer:** Suited for high-performance apps; supports TCP, UDP, and TLS protocols.
- **Gateway Load Balancer:** Designed for third-party appliances (e.g., security, analytics).
- **Classic Load Balancer:** Legacy option for EC2; AWS recommends using ALB or NLB.

Key Components:

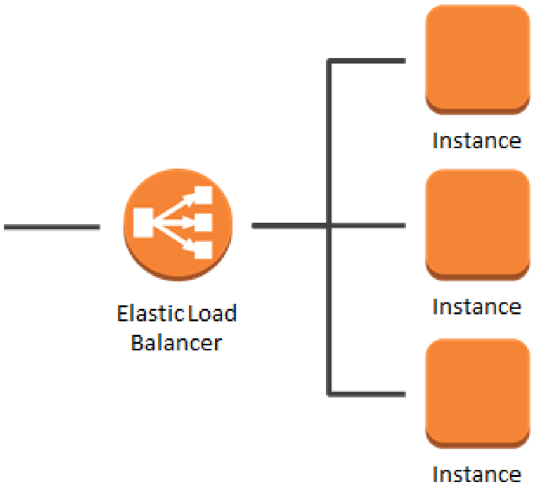
- **Listeners:** Monitor incoming requests on specified protocols/ports (HTTP, HTTPS).
- **Target Groups:** Define the destination for traffic (instances, IPs, Lambda functions).
- **Health Checks:** Regularly monitor target health and remove unhealthy targets.

Use Cases:

- Balancing traffic across multiple servers for web applications.
- Building hybrid cloud solutions by load balancing across AWS and on-premises resources.
- Supporting AWS migrations with auto-scaling and dynamic capacity management.

Pricing:

Billed hourly (or partial hour) plus based on Load Balancer Units (LCUs).



Amazon Route 53

- Managed DNS service that routes users to servers via domain names.
- Acts as a domain name registrar and DNS server.

Hosted Zones:

- **Public Hosted Zone:** Routes traffic on the Internet.
- **Private Hosted Zone:** Routes traffic within a VPC.

Record Types:

- Common: A (IPv4), AAAA (IPv6), CNAME, Alias.
- Others: CAA, MX, NAPTR, NS, PTR, SOA, SPF, SRV, TXT.

Routing Policies:

- **Simple:** Single resource routing (no health checks).
- **Weighted:** Routes based on assigned weights; supports health checks.
- **Failover:** Routes to secondary resource if primary fails.
- **Geo-location/Geo-proximity:** Routes based on geographic location.
- **Latency-based:** Routes to lowest-latency destination.
- **Multi-value Answer:** Distributes responses across multiple IPs.

Use Cases:

- Domain registration and DNS hosting.
- Managing public and private DNS zones.
- Routing based on performance, location, and health.

Pricing:

- No long-term contracts; annual fees for registered domains.
- Charges vary for different query types (standard, latency, geo, etc.).

Route53 CNAME vs. Alias

CNAME	Alias
● It points a hostname to any other hostname. ● (app.mything.com -> abc.anything.com) ● It works only for the non-root domains. ● (abcxyz.maindomain.com) ● Route 53 charges for CNAME queries. ● It points to any DNS record that is hosted anywhere.	● It points a hostname to an AWS Resource. ● (app.mything.com ->abc.amazonaws.com) ● It works for the root domain and non-root domain. (maindomain.com) ● Route 53 doesn’t charge for Alias queries. ● It points to an ELB, CloudFront distribution, Elastic Beanstalk environment, S3 bucket as a static website, or another record in the same hosted zone.

AWS VPC

A dedicated virtual network in AWS where you can launch and manage resources in an isolated environment.

Security:

- **Security Groups:**
  - *Default:* Allow all inbound/outbound traffic.
  - *Custom:* Block inbound by default, allow outbound.
- **Network ACLs:**
  - *Default:* Allow all traffic.
  - *Custom:* Deny all traffic by default.

Core Components:

- **Subnets:**
  - Logical IP address divisions.
  - *Public Subnet:* Has internet access via an Internet Gateway.
  - *Private Subnet:* No direct internet access; requires NAT for outbound connectivity.
- **Route Tables:**
  - Direct network traffic.
  - Public subnets use routes to an Internet Gateway; private subnets use NAT.
- **NAT Devices:**
  - **NAT Instance:** EC2 instance deployed in a public subnet for outbound IPv4 traffic.
  - **NAT Gateway:** Managed by AWS for scalable outbound connectivity.
- **DHCP Options Set:**
  - Automatically configures network parameters like domain name and DNS servers.
- **PrivateLink & Endpoints:**
  - Provide secure, private connectivity to AWS services without using the public internet.
- **Egress-Only Internet Gateway:**
  - Enables outbound-only IPv6 traffic.
- **VPC Peering:**
  - Connects two VPCs (within or across regions) for seamless resource communication.
- **VPN Connections:**
  - **AWS Site-to-Site VPN:** Securely connects on-premises networks to your VPC.
  - **AWS Client VPN:** Provides remote user connectivity to AWS resources.

Use Cases:

- Hosting public websites and multi-tier applications.
- Disaster recovery.
- Hybrid cloud setups and secure communication between different networks.

Pricing:

- VPC creation is free.
- Charges apply for NAT Gateway usage, data processing, and traffic mirroring.

Application Integration

Amazon EventBridge

Amazon EventBridge is a serverless event bus service that connects applications with data from multiple sources.

Functions of Amazon EventBridge:

Loosely Coupled, Event-Driven Architecture

- Facilitates the creation of distributed systems where components interact via events without being tightly integrated.

Seamless Event Delivery

- Connects applications and transmits events without requiring custom code, streamlining integration between services.

Real-Time Data Streaming

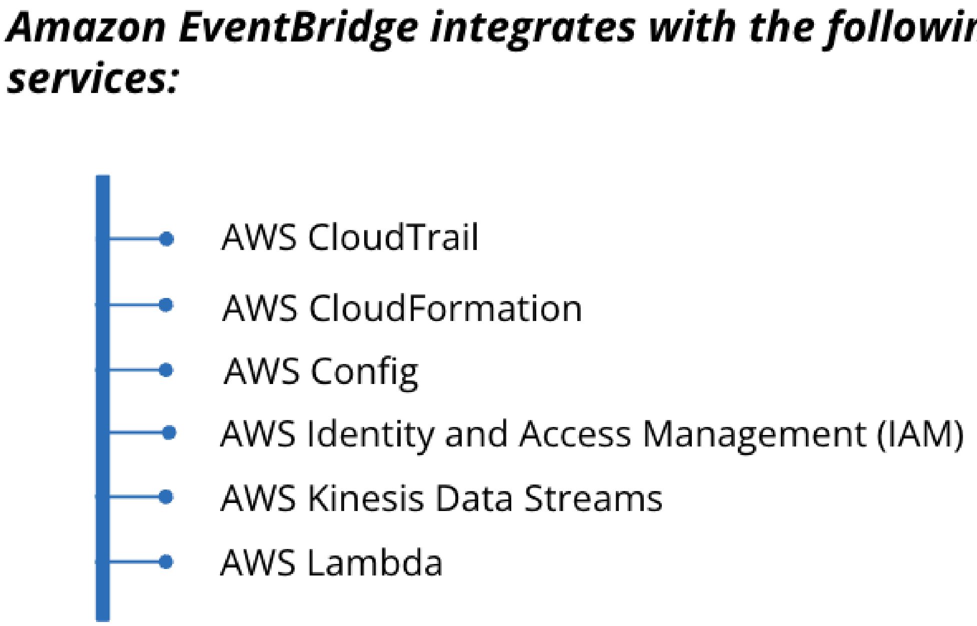
- Delivers live data streams from SaaS applications or AWS services to various targets such as EC2 instances, ECS tasks, or CodeBuild projects.

Routing Rules Configuration

- Allows you to define rules that determine how events are routed to appropriate targets, enabling reactive application architectures.

EventBridge Schema Registry

- Stores a collection of event schemas.
- Provides the ability to download code for these schemas, allowing developers to represent events as objects within their IDE for easier integration and use.



Amazon EventBridge integrates with the following services:

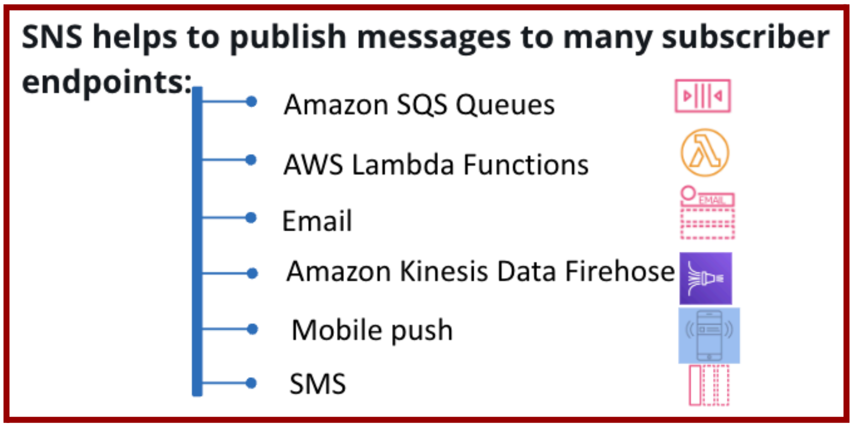
- AWS CloudTrail
- AWS CloudFormation
- AWS Config
- AWS Identity and Access Management (IAM)
- AWS Kinesis Data Streams
- AWS Lambda

Amazon SNS

- Amazon Simple Notification Service (Amazon SNS) is a serverless notificationservice that offers message delivery from publishers to subscribers.

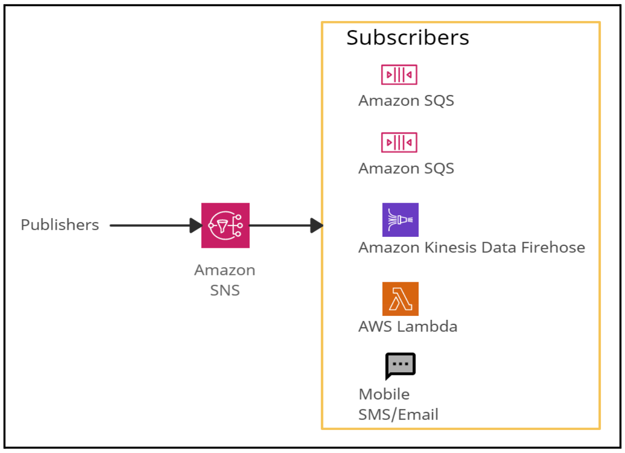
Features

- **Asynchronous Communication:** Enables asynchronous messaging between publishers and subscribers via topics.
- **Application-to-Application Integration:** Supports application-to-application subscriptions using services like Amazon SQS and other AWS offerings.
- **Application-to-Person Notifications:** Facilitates application-to-person notifications through subscriptions such as Mobile SMS and Email.
- **One-to-Many Communication:** The producer sends one message to one SNS topic.
- **Fan-out Delivery:** Multiple receivers (subscribers) listen for notifications on that SNS topic.
- **Guaranteed Delivery:** All subscribers will receive all messages published to the topic.
- **Scalability:** A single message can be efficiently delivered to a large number of subscribers (e.g., 1 message, 1 topic, 10 subscribers results in the message being delivered to all 10 subscribers).



SNS helps to publish messages to many subscriber endpoints:

- Amazon SQS Queues
- AWS Lambda Functions
- Email
- Amazon Kinesis Data Firehose
- Mobile push
- SMS



Source: AWS Documentation

Amazon Simple Queue Service (SQS)

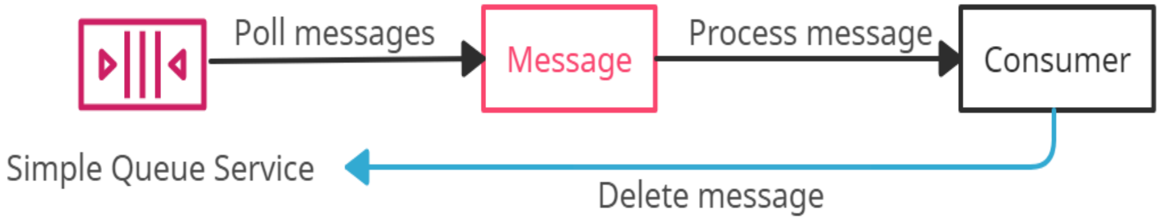
Amazon Simple Queue Service (SQS) is a serverless service used to decouple (loose couple) serverless applications and components.

SQS Queue Types:

Queue Type	Key Features
Standard Queue	- Supports unlimited transactions per second. - Delivers messages in a non-deterministic order. - May deliver messages more than once (at-least-once delivery).
FIFO Queue	- Handles up to 300 messages per second (or 3000 messages per second with batching). - Supports batches of 10 messages per operation. - Guarantees exactly-once message consumption in order.
Delay Queue	- Allows postponement of message delivery by a specified duration. - Messages can be delayed from 0 seconds (default) up to a maximum of 15 minutes.
Dead-Letter Queue	- Captures messages that fail to be consumed successfully. - Helps manage and troubleshoot message processing failures.
Visibility Timeout	- Determines the time period during which a message is hidden from other consumers once retrieved. - Default: 30 seconds; Minimum: 0 seconds; Maximum: 12 hours.

General SQS Characteristics:

- Serves as a temporary repository between producers and consumers.
- Scales to manage between 1 to 10,000 messages per second.
- Default message retention is 4 days, extendable up to 14 days.
- Automatically deletes messages once consumed.
- Each message can be up to 256KB in size.



Source: AWS Documentation

Developer Tools

Developer tools overview

Feature	Details
Benefits	Faster releases, seamless AWS integration, simplified development, ML-based security & code quality.
Services	CI/CD, Infrastructure as Code, SDKs & CLI, IDEs, collaboration tools.
Use Cases	Automate deployments, streamline CI/CD, boost productivity, monitor performance.

AWS CodeBuild

Feature	Details
Description	Fully managed CI service for efficient builds & tests.
Benefits	No build queue waiting, auto-scaling, pay-as-you-go pricing.
Features	Easy setup, integrates with Jenkins/Git, automated builds.
Pricing	First 100 minutes free, charges based on usage.

AWS CodeDeploy

Feature	Details
Description	Automates deployments to EC2, Lambda, on-premises, ECS.
Deployment	Code, Lambda, web files, executables, scripts.
How It Works	Define revision ⟶ Configure YAML ⟶ Deploy.
Features	Rapid releases, zero-downtime deployment, status tracking.
Pricing	Free for EC2/Lambda, $0.02 per on-prem deployment.

AWS X-Ray

Feature	Details
Description	Debugs & analyzes distributed applications.
Components	Daemon, Segments, Traces, Sampling, Service Graph.
Features	Supports multiple languages, AWS integrations, performance insights.
Pricing	$0.50 per 1M requests (beyond free tier).

—-Back to Index—

Billing & Cost Management

AWS Cost Explorer

- **What It Is:** A UI tool for analyzing AWS cost and usage via graphs and reports.
- **Reports:** Cost & Usage and Reserved Instance (RI) utilization/coverage.
- **Data:** Up to 12 months of historical data, current month, and 12-month forecasts.
- **Access:** Billing & Cost Management console and API ($0.01 per API request).

AWS Cost & Usage Report (CUR)

- **What It Is:** Detailed report of AWS cost, usage, and resource metadata.
- **Delivery:** Report files sent to S3 up to three times per day.
- **Usage:** Analyze using Athena, Redshift, or QuickSight.
- **Access:** CUR API for creation, retrieval, and deletion.

AWS Management Console

- **What It Is:** A web-based interface for managing AWS services.
- **Features:** Access to all AWS service consoles, recent services, region selection, and a search function.
- **Availability:** Also available as a mobile app for Android and iOS.