WHIZLABS

AWS DevOps Professional Certification

Cheat Sheet

Quick Bytes for you before the exam!

*The information provided in the cheat sheet is for educational purposes only. It was created in our efforts to help aspirants prepare for the **AWS DevOps Professional certification exam**. Though references have been taken from **AWS documentation**, they are not intended to be substitutes for the official documents. The document can be reused, reproduced, and printed in any form; ensure that appropriate sources are credited and required permissions are received.*

Are you Ready for

"AWS DevOps Professional" Certification?

Self-assess yourself with

Whizlabs FREE TEST

800+ Hands-on-Labs and Cloud Sandbox

Hands-on Labs **Cloud Sandbox environments**

Index

—-Back to Index—

—-Back to Index—

Compute & Containers

Amazon Elastic Kubernetes Service (Amazon EKS)

What is EKS?

Amazon Elastic Kubernetes Service (Amazon EKS) is a managed service to run and manage Kubernetes applications on AWS or on-premises without altering code for standard Kubernetes applications.

Key Components

1. **Control Plane**
    - Dedicated Kubernetes infrastructure for high availability and security.
    - Automated upgrades, patching, and instance replacement.
2. **Nodes**
    - EC2 instances or AWS Fargate for running workloads.

Cluster Creation Methods

1. **eksctl**: CLI tool for managing Kubernetes clusters.
2. **AWS Console/CLI**: GUI or command-line for setup and management.

Node Scheduling Options

1. **Self-Managed Nodes**: EC2 instances in Auto Scaling groups.
2. **Managed Node Groups**: Automated provisioning and scaling of EC2 nodes.
3. **AWS Fargate**: Serverless pods without infrastructure management.

AWS Integrations

- **Images**: Amazon ECR for container storage.
- **Load Balancing**: AWS ELB for traffic distribution.
- **Authentication**: AWS IAM for secure access.
- **Networking**: Amazon VPC for isolation.

Benefits

- Scalability with Kubernetes and AWS.
- High availability through multi-AZ control planes.
- Flexible infrastructure options (EC2, managed nodes, Fargate).
- Deep AWS service integration for security and performance.

Amazon Elastic Container Service (Amazon ECS)

Amazon ECS is a regional service for container orchestration, enabling you to run, manage, and stop containers within a cluster.

Core Features

Containers:

- Packages code, dependencies, and libraries into a portable unit.
- Created from Dockerfiles and stored in registries for deployment.

Task Definitions

- Defines container configurations in JSON format.
- Enables running single or multiple tasks within services.

ECS Clusters

- Groups of tasks or services running on EC2 instances or AWS Fargate.
- Automatically creates a default cluster upon initial use.

Container Agent

- Operates on instances within the cluster, monitoring tasks and resources.
- Communicates with ECS to start or stop tasks as required.

Task Scheduler: Assigns tasks to cluster resources based on task definitions.

Application Load Balancer Capabilities

- Supports dynamic host port mapping for running multiple tasks on one instance.
- Enables path-based routing and priority rules, allowing multiple services to share a listener port.

AWS Service Integrations

- **IAM**: Secures access and authentication.
- **EC2 Auto Scaling**: Automatically adjusts resources.
- **Elastic Load Balancing**: Distributes traffic efficiently.
- **ECR**: Manages container image storage.
- **CloudFormation**: Automates infrastructure management.
- **App Mesh**: Adds observability, traffic control, and enhanced security.

Use Cases

1. **Microservices**
   - Breaks down complex applications into smaller, manageable components.
2. **Batch Jobs**
   - Ideal for short-lived workloads packaged as Docker containers.

Pricing Options

1. **Fargate Launch Type**
   - Charges are based on vCPU and memory usage.
2. **EC2 Launch Type**
   - Charges based on resources provisioned for application workloads.

Amazon Elastic Container Registry (ECR)

What is Amazon ECR?

Amazon Elastic Container Registry (ECR) is a fully managed service for storing, managing, sharing, and deploying container images and artifacts. It integrates seamlessly with Amazon ECS, EKS, Lambda, and Fargate to streamline workflows.

Features

- **Image Storage:** Stores created containers and container software from AWS Marketplace.
- **Service Integration:** Works with ECS, EKS, Lambda, and Fargate for simplified deployments.
- **Access Control:** Uses AWS IAM for resource-level access control per repository.
- **Repository Types:** Supports public and private image repositories for flexible sharing options.
- **Public Access:** Provides a dedicated ECR Public Gallery for public repositories.
- **Durable Storage:** Utilizes Amazon S3 for 99.999999999% (11 9's) durability.
- **Replication:** Enables cross-region and cross-account data replication for high availability.
- **Encryption:** Secures images in transit via HTTPS and at rest using Amazon S3 encryption or AWS KMS keys.
- **CI/CD Integration:** Supports continuous integration and delivery workflows, including third-party tools.
- **Lifecycle Management:** Uses lifecycle policies to automate image retention.

Pricing Details

- **Free Tier:**
  - 500 MB/month of private storage for one year.
  - 50 GB/month of public storage for new customers.
- **Data Transfer:**
  - Without sign-up: 500 GB/month free from public repositories.
  - With an AWS account, 5 TB/month free from public repositories.

AWS Lambda

What is AWS Lambda?

- Serverless service: Executes code without the need for server management
- Auto-scaling: Adjusts automatically based on incoming requests
- Manages backend: Handles applications and services without infrastructure management
- Event-driven: Triggers on events like S3 modifications, DynamoDB updates, or API Gateway HTTP requests **Pay-per-use:** Charges apply solely when the code is executed

What is Serverless Computing?

- Backend services are provided on a pay-per-use basis.
- No need to manage servers; the cloud vendor handles infrastructure.
- Charges are based on resource usage.

When to Use AWS Lambda

- Focus only on writing and deploying code.
- AWS manages memory, CPU, and networking resources.
- No server access or OS customization is allowed.
- For compute management, consider services like EC2 or Elastic Beanstalk.

How AWS Lambda Works

Lambda Functions

- Code blocks are uploaded as single or multiple functions.
- Deployed as zip files or directly from S3. Monitors function metrics via Amazon CloudWatch.

Lambda Layers

- Archives for additional code, libraries, or runtimes. Up to five layers per function.
- Immutable layers; new versions are created for updates.
- Layers are private by default but can be shared or made public.

Lambda Events

- Entities that trigger Lambda functions (e.g., DynamoDB, SQS, SNS, API Gateway).
- Supports synchronous invocations.

Supported Languages

- NodeJS, Go, Java, Python, Ruby.

Lambda@Edge

- CloudFront feature to run code closer to users for reduced latency.
- Infrastructure is managed globally. Triggers from CDN events.

Pricing

- Based on the number of requests and duration (per 100 ms).
- **Free tier:**
  - 1 million requests/month.
  - 400,000 GB-seconds compute time/month.

EC2 Image Builder

Overview

- **Purpose**: Simplifies the creation, testing, and deployment of VM and container images for AWS or on-premises environments.
- **Why It's Useful**: Automates the process of keeping images up-to-date and secure, reducing manual effort and the need for custom automation pipelines.

Benefits

Improved Productivity

- Simplifies image maintenance with a graphical interface and built-in automation.
- Eliminates the need for custom automation, saving time and IT resources.

Enhanced Security

- Create minimal, secure images to reduce vulnerability exposure.
- Automatic patching for security updates.
- Apply AWS or custom security policies (e.g., encryption, password policies) for compliance.

Consistent Image Creation

- One unified workflow for building, securing, and testing VM and container images.

Built-in Validation

- Ensure images meet functionality, compatibility, and security standards before deployment.
- Reduce errors by running tests before production use.

Centralized Policy Enforcement

- Version control for image management and revision tracking.
- Share automation scripts and images across AWS accounts with AWS Resource Access Manager and Amazon ECR.
- Enforce security and compliance policies for image usage.

Cost

- Free service, except for the AWS resources used for image creation, storage, and sharing.

AWS Fargate

What is AWS Fargate?

AWS Fargate is a serverless compute service for containers used with Amazon ECS and EKS. It simplifies running containers by eliminating the need to manage virtual machines like EC2.

Key Features	Description
Serverless Containers	Runs containers by specifying CPU, memory, and IAM policies.
Isolation	Fargate tasks have dedicated kernels, memory, CPU, and ENI, ensuring task isolation.
Task Limitations	Supports only specific ECS task definition parameters with some restrictions.
Kubernetes Integration	Schedules Kubernetes pods on Fargate using controllers. Security groups for EKS pods are unsupported.
Storage Support	- Amazon EFS for persistent storage. - Ephemeral storage for nonpersistent needs.

Benefits of AWS Fargate:

- **Focus on Application Development**: Fargate enables users to focus on building and operating applications rather than managing servers, security, scaling, and patching.
- **Automatic Scaling**: It automatically adjusts the compute environment to meet the container's resource requirements.
- **Built-in Integrations**: Fargate integrates seamlessly with other AWS services, including Amazon CloudWatch Container Insights for monitoring.

Pricing Details:

- **Cost Based on vCPU and Memory Usage**: Charges are incurred based on the amount of vCPU and memory consumed by the containerized applications.
- **Savings Plans**: Fargate's Savings Plans offer up to 50% savings in exchange for a one- or three-year long-term commitment.
- **Additional Charges**: Extra charges may apply if containers are used in conjunction with other AWS services.

Application Integration

Amazon Elastic Beanstalk

What is Amazon Elastic Beanstalk?

- Compute service for deploying and scaling applications in multiple languages
- Focus on coding; no need to manage infrastructure
- Fastest and simplest deployment method
- Provides a dashboard for application monitoring
- Flexibility to choose AWS resources like EC2 and pricing options

Supported Environments

Web Tier Environment

- Handles HTTP/HTTPS requests
- Auto assigns resources to run the app
- Uses Elastic Load Balancer (ELB) to distribute traffic to EC2 instances
- Auto Scaling adjusts EC2 instances based on load
- Host Manager handles logs, monitoring, and events

Worker Environment

- Processes background tasks (e.g., database cleanup, report generation)
- Daemon on EC2 instances pulls tasks from the SQS queue
- Task execution and retry mechanism upon failure

Supported Platforms

- .Net (Linux/Windows), Docker, GlassFish, Go, Java, Node.js, Python, Ruby, Tomcat

Deployment Models

- **All at Once:** All instances are updated simultaneously, causing brief downtime
- **Rolling:** Deploy in batches with no full downtime
- **Rolling with Additional Batch:** The new version deployed with extra instances for no downtime
- **Immutable:** New version on separate instances with no changes to old ones
- **Traffic Splitting:** Split traffic between old and new instances

Pricing

- No charge for the Elastic Beanstalk service
- Pay for underlying resources (EC2, ELB, Auto Scaling) used for hosting the app

AWS Control Tower

What is the AWS Control Tower?

- Extends AWS Organizations to provide additional controls
- Helps create a well-architected multi-account baseline (Landing Zone) based on AWS best practices
- Automatically creates an AWS Organization if one does not exist

Features

- **Sets up Organizational Units (OUs):** Security, Sandbox, and Production
- Security OU includes Audit & Log Archive accounts
- Sandbox & Production OUs allow adding Development and Production accounts
- Integrates with AWS Identity Center for SSO using AWS Identity Center directories, SAML IDps, or Microsoft AD
- Root users in Management Accounts can bypass Guardrails (similar to AWS Organizations SCPs)
- Centralized Dashboard for oversight of accounts, OUs, Guardrails, and policies
- Account Factory for provisioning new accounts with standardized configurations

Use Cases

- Launch AWS Control Tower in a new or existing AWS Organization
- **Guardrails for Governance & Compliance:**
    - **Preventive Guardrails:** Based on SCPs to restrict API actions
    - **Detective Guardrails:** Use AWS Config and Lambda functions to monitor and enforce compliance

AWS Resource Access Manager (RAM)

What is AWS Resource Access Manager (RAM)?

- AWS RAM allows the sharing of resources across AWS accounts or within an AWS Organization.

Resources Integrated with AWS RAM

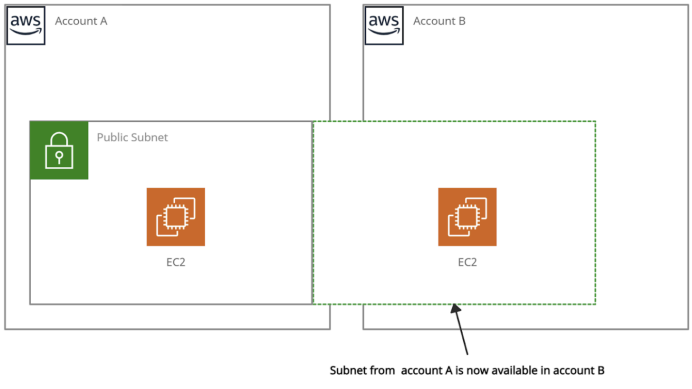
- **AWS App Mesh**
- **Amazon Aurora**
- **AWS Certificate Manager Private Certificate Authority**
- **AWS CodeBuild**
- **EC2 Image Builder**
- **AWS Glue**
- **AWS License Manager**
- **AWS Network Firewall**
- **AWS Outposts**
- **AWS Resource Groups**

Benefits

- Reduces the need to create duplicate resources across multiple accounts
- Controls shared resource consumption with existing policies and permissions
- Integrates with Amazon CloudWatch and AWS CloudTrail for detailed visibility
- Security and governance controls via AWS IAM and Service Control Policies in AWS Organizations

Pricing

- No charges for creating resource shares or sharing resources across accounts
- Charges depend on the resource type



AWS Resource Access Manager

Source: AWS Documentation

AWS Service Catalog

What is the AWS Service Catalog?

Service Catalog allows the creation, sharing, organization, and governance of curated Infrastructure-as-Code (IaC) templates.

Benefits

- Fast Deployment: Quickly provision cloud resources
- Stay Agile: Enable rapid resource deployment with minimal overhead
- Streamline Workflows: Simplify cloud resource management and governance
- Stay Up to Date: Keep resources aligned with the latest standards and updates

Why Service Catalog?

- Create and manage a curated catalog of approved AWS resources
- Share resources at the permissions level for secure and compliant access
- Enable quick provisioning of resources without direct access to AWS services

Use Cases

- Automate Access to ML Notebooks: Simplify access management for machine learning environments
- Apply Access Controls: Enforce resource access policies and governance
- Provision Resources for AWS Accounts: Streamline provisioning across multiple accounts
- Accelerate CI/CD Pipeline Provisioning: Speed up the setup of continuous integration and deployment pipelines

Amazon EventBridge

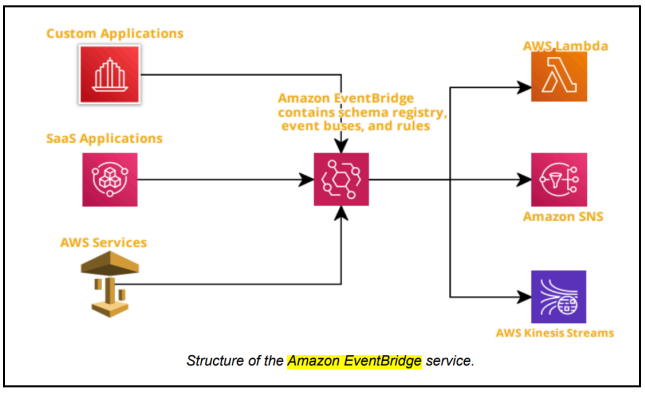
What is Amazon EventBridge?

Amazon EventBridge is a serverless event bus service that integrates SaaS applications with AWS services, delivering real-time data to multiple targets like AWS Lambda or SNS. It handles event ingestion, delivery, security, and infrastructure management. Previously known as Amazon CloudWatch Events, it uses the same API.

Key Concept	Description
Event Buses	Receives and processes events based on routing rules. Includes a default event bus for AWS services and supports custom event buses.
Events	Represents changes in the environment, such as from AWS services, SaaS applications, or custom apps. Rules trigger actions based on these events.
Schema Registry	Stores schemas for events across AWS services. Allows creation, updates, or automatic inference of schemas. Supports multiple schema versions.
Rules	Defines how incoming events are matched and routed to processing targets. A rule can route events to multiple targets for parallel processing.
Targets	Handles events in JSON format. Targets must be in the same region as the associated rule.

Features

- Fully Managed: No infrastructure management is required.
- Pay-As-You-Go: Charges based on events published.
- Native SaaS Integration: Supports 90+ AWS services as event sources.
- Multiple Target Locations: Events can be routed to multiple destinations.
- Easy Scaling: Automatically scales to handle event traffic.
- Cost: $1 per million events ingested into the bus. No additional charge for event delivery.



Structure of the Amazon EventBridge service.

Pricing

- Custom Events: $1.00 per million requests.
- Third-Party Events (SaaS): $1.00 per million requests. Cross-Account Events: $1.00 per million requests. No extra charges for rules or event delivery.

—-Back to Index—

AWS Step Functions

What are Step Functions?

AWS Step Functions is a fully managed service that allows the coordination and orchestration of microservices and distributed applications by executing workflows across various AWS services. It complex workflows by defining them as "state machines"—a series of steps (states) that control the execution of tasks, handling failures, retries, and enabling parallel processing.

Types of Step Functions:

1. **Standard Workflow**
    - Used for long-running, durable, and auditable workflows.
2. **Express Workflow**
    - Designed for high-volume, event processing workloads.

Features:

- Create workflows with fixed or dynamic sequences.
- Built-in **Retry** and error handling functionality.
- Integrates with AWS services like Lambda, SNS, ECS, and AWS Fargate.
- GUI for auditing workflows, input/output, and error detection.
- High availability, scalability, and low cost.
- Manages application states during workflow execution.
- Based on **tasks** and **state machines**:
    - Tasks: Defined by activities or AWS Lambda functions.
    - State machines: Represent algorithms with relations, inputs, and outputs.

Best Practices:

- **Set Timeouts**: Define timeouts in state machine definitions to handle task response delays. **Example:** "TimeoutSeconds": 900, "HeartbeatSeconds": 40
- **Use S3 for Large Payloads**: Use Amazon S3 ARN for input to Lambda instead of large payloads. **Example:** { "Data": "arn:aws:s3:::MyBucket/data.json" }
- **Handle Errors in State Machines**: Implement retry logic when invoking Lambda functions. **Example:** "Retry": [{"ErrorEquals": ["Lambda.CreditServiceException"], "IntervalSeconds": 2, "MaxAttempts": 3, "BackoffRate": 2}]
- **Execution History Limit**: Avoid the 25K execution history limit by using Lambda for long-running executions.

Supported AWS Services:

- Lambda, AWS Batch, DynamoDB, ECS/Fargate, SNS, SQS, SageMaker, EMR

Pricing:

- **Standard Workflows**: $0.025 per 1,000 state transitions.
- **Express Workflows**: $1.00 per 1M requests.

AWS Serverless Application Model (SAM)

What is the AWS Serverless Application Model (SAM)?

- An open-source developer tool designed to simplify the building and running of serverless applications on AWS.
- Improves the experience for developers by streamlining the process of defining, developing, and deploying serverless applications.

Benefits of AWS SAM:

1. **Streamlines Development Cycle**: Speeds up the process of building, testing, and deploying serverless applications.
2. **Simplifies Infrastructure Management**: Defines and manages your infrastructure as code.
3. **Real-Time Debugging and Testing**: Allows for on-the-fly debugging and testing of serverless applications.
4. **Easy Deployment**: Automates the deployment of applications to AWS.

Feature	Description
AWS SAM Templates	The simplified syntax for defining Infrastructure as Code (IaC) for serverless applications, an extension of AWS CloudFormation for easier deployment of serverless resources.
AWS SAM CLI	A command-line tool that enables fast creation, development, and deployment of serverless applications. Integrates with tools like AWS Cloud Development Kit (AWS CDK) and Terraform.
AWS SAM Accelerate	Speeds up local development and cloud testing, significantly reducing development time.
Integrations with Other Tools	Extends functionality by integrating with AWS CDK, Terraform, and other CI/CD systems.

Use Cases:

- **Build and Deploy Serverless Applications**: Streamline the process of creating and managing serverless architectures.
- **Quick Sync for Development and Testing**: Sync your application to the cloud quickly for real-time development and testing.
- **CI/CD Pipeline Integration**: Automate the deployment process through supported CI/CD systems.
- **Integration with Terraform**: Use AWS SAM CLI with Terraform for infrastructure management.

Management & Governance

AWS CloudTrail

What is AWS CloudTrail?

- A global service for operational and risk auditing of AWS accounts.
- Allows users to view, search, download, and respond to account activity across AWS services.
- Records events from users, roles, and AWS services via the AWS Management Console, CLI, and APIs.

Integrations

- Amazon S3: Stores log files.
- Amazon SNS: Notifies about log file delivery.
- Amazon CloudWatch & IAM: For monitoring and security.

Event Types

1. Management Events: Control plane operations (e.g., EC2 CreateSubnet, CreateDefaultVpc).
2. Data Events: Data plane operations (e.g., S3 GetObject, DeleteObject, PutObject).
3. CloudTrail Insights Events: Identifies unusual activity (e.g., S3 deleteBucket, EC2 AuthorizeSecurityGroupIngress).

Example of CloudTrail Log

- IAM Log File Example:
    - User "Rohit" adds "Nayan" to the "admin" group.

Pricing

- Charges are based on Amazon S3 usage.
- The first copy of management events within a region is free; additional copies cost $2 per 100,000 events.
- Data events cost $0.10 per 100,000 events.
- CloudTrail Insights events cost $0.35 per 100,000 write events analyzed.

Amazon CloudWatch

What is Amazon CloudWatch?

- A service for monitoring and managing AWS applications and infrastructure.
- Provides actionable insights and data for resources like Amazon RDS, EC2, DynamoDB, and log files from applications.

Access Methods

- CloudWatch Console, AWS CLI, CloudWatch API, AWS SDKs

Integration with Other AWS Services

- **Amazon SNS:** For notifications.
- **Amazon EC2 Auto Scaling:** For resource scaling.
- **AWS CloudTrail:** For tracking AWS service activity.
- **AWS IAM:** For managing access and security.

Feature	Description
Data Monitoring	Gathers logs, metrics, and events from both AWS and on-premises resources.
Custom Dashboards	Allows users to build personalized dashboards to visualize metrics.
CloudWatch Alarms	Enables the creation of alarms to monitor metrics and trigger actions when thresholds are exceeded.
Cross-Account Access	Offers cross-account visibility without needing to sign in and out, particularly useful in AWS Organizations.

Insights Features

- **Container Insights:** Collects and summarizes metrics and logs from containerized applications (Amazon ECS, EKS, and Kubernetes on EC2).
- **Lambda Insights:** Collects system-level metrics for serverless applications running on AWS Lambda.

CloudWatch Agent

- **System-Level Metrics:** Collects metrics from EC2 instances and on-premises servers across operating systems.
- **Custom Metrics:** Collects custom application metrics using StatsD and collected protocols.
    - StatsD: Supported on Linux and Windows servers.
    - collectd: Supported only on Linux servers.
- **Storage:** Metrics from the CloudWatch agent are stored in CloudWatch with the default namespace "CWAgent," which can be customized.

AWS Config

What is AWS Config?

Monitoring & Evaluation:

- Continuously monitors and evaluates AWS resource configurations.
- Tracks configuration changes over time via AWS Config Console or CLI.

Snapshots & Notifications:

- Captures resource configuration snapshots for a complete inventory.
- Retrieves past configurations and sends notifications for resource creation, modification, or deletion.

Config Rules:

- Evaluate resource configurations and check rule violations.
- Supports up to **150 rules per region**:
  - **Managed Rules**
  - **Custom Rules**

Integration:

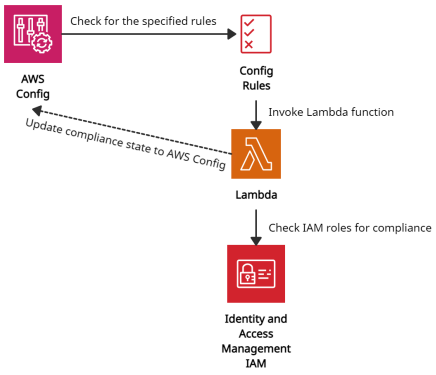
- Works with AWS IAM for permission policies, S3 for snapshots, and SNS for notifications.
- Integrated with CloudTrail to log API calls as events in AWS Config.

AWS Config provides an aggregator (a resource) to collect AWS Config configuration and compliance data from:

- Multiple accounts and multiple regions.
- Single account and multiple regions.
- An organization in AWS Organizations
- The Accounts in the organization that have AWS Config enabled.

Use Cases:

- **Custom Rules:**
  - Define custom resource configuration rules using AWS Lambda.
  - Automate resource configuration assessments for compliance and self-governance.
- **Security Monitoring:**
  - Continuously monitor configurations for security weaknesses.
  - Review configuration history after alerts to assess risk factors.



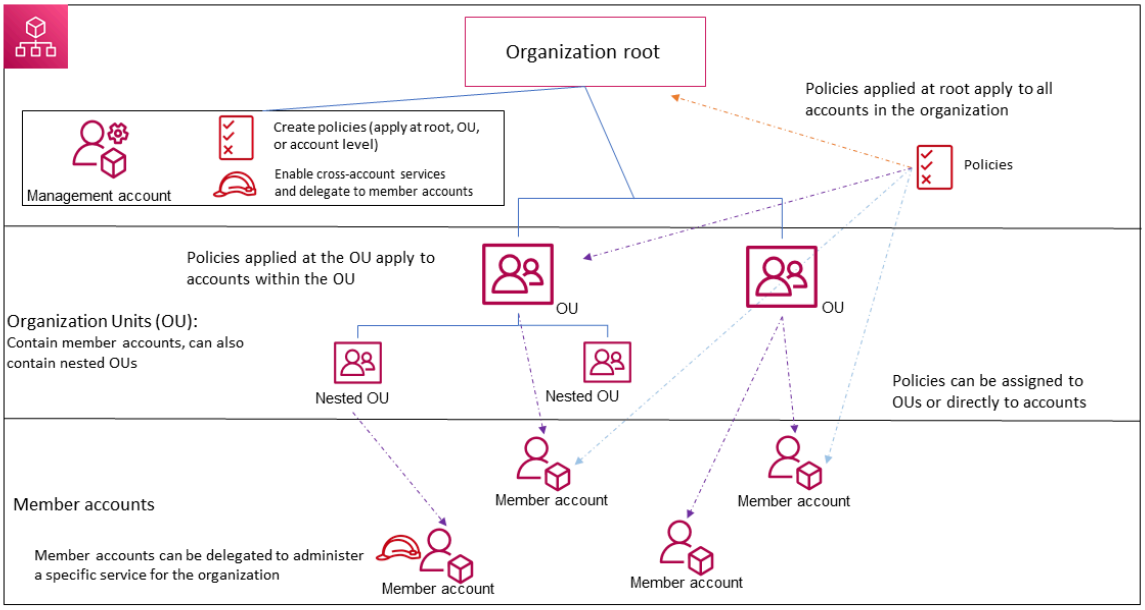
AWS Config in action

AWS Organizations

What are AWS Organizations?

AWS Organizations is a global service that enables users to consolidate and manage multiple AWS accounts into an organization.
It includes account management and combined billing capabilities that help to meet the budgetary, and security needs of the business better.

- The main account is the management account – it cannot be changed.
- Other accounts are member accounts that can only be part of a single organization.



Access Methods

- AWS Management Console
- AWS Command Line Tools and CLI
- AWS Tools for Windows PowerShell
- AWS SDKs
- AWS Organizations HTTPS Query API

Features

- **Security and Resource Sharing:**
  - Enforces security boundaries with multiple member accounts.
  - Shares critical resources across accounts.
- **Account Organization:**
  - Groups accounts into **Organizational Units (OUs)** for specific applications.
  - Enforces governance using **Service Control Policies (SCPs)** to meet security requirements.
- **Cost Management:**
  - Uses cost allocation tags for tracking costs by category.
  - Provides consolidated billing for all member accounts with volume discounts.

- **Integrations:**
    - **AWS CloudTrail:** Auditing and event logging.
    - **AWS Backup:** Backup monitoring.
    - **AWS Control Tower:** Cross-account security audits and policy management.
    - **Amazon GuardDuty:** Threat detection and security services.
    - **AWS RAM:** Shares resources to reduce duplication.

Member Account Migration

1. Remove the member account from the old organization.
2. Invite the member account to the new organization.
3. Accept the invitation in the member account.

Pricing

- AWS Organizations is free. Charges apply to other AWS services used.
- The management account pays for all resources used within the organization.

AWS Systems Manager

What is AWS Systems manager?

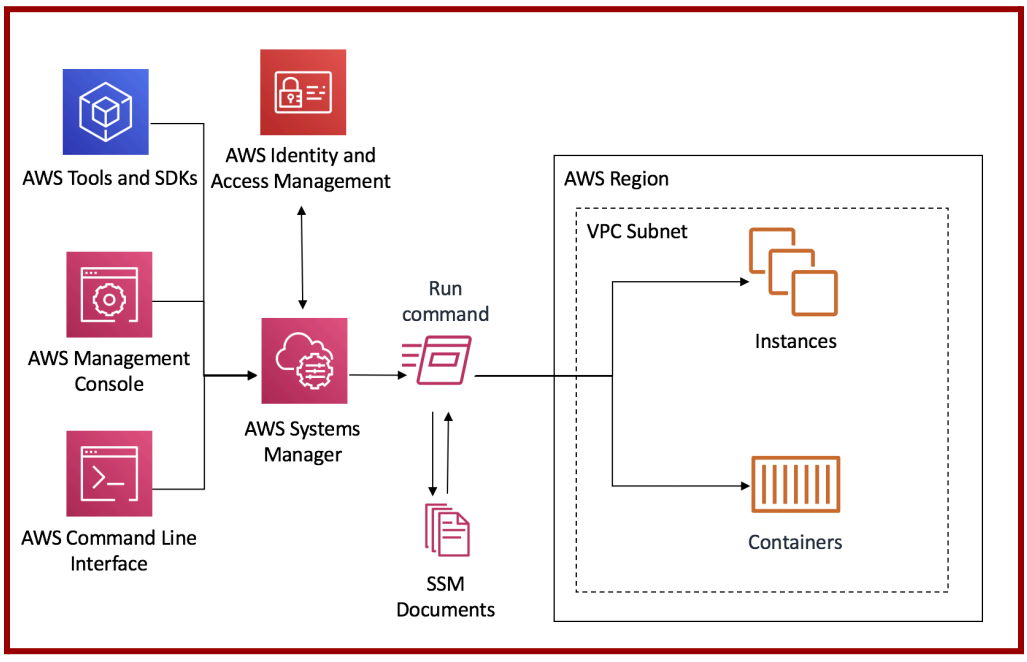
AWS Systems Manager helps manage EC2 and on-premises systems at scale, providing infrastructure insights, problem detection, and automated patching for compliance. It supports both Windows and Linux operating systems.

Key Features

- **Integration:** Works with AWS Config and CloudWatch metrics/dashboards.
- **Compliance Management:**
  - Automates patching and ensures compliance with desired states.
  - Audits installed software and detects discrepancies.
- **Resource Grouping:** Organizes over 100 resource types into applications, business units, or environments.
- **Instance Insights:**
  - Provides information on OS patch levels and installed software.
  - Distributes multiple software versions securely.
- **Security and Automation:**
  - Runs commands/scripts to increase security.
  - Automates workflows to reduce errors using configurable parameters.

How AWS Systems Manager Works

1. **SSM Agent:** Install the SSM agent on systems to enable management.
2. **IAM Role:** Ensure EC2 instances have proper IAM roles for SSM actions.
3. **Troubleshooting:** If management fails, verify the SSM agent installation and role configuration.



Source: AWS Documentation

AWS CloudFormation

- **What is AWS CloudFormation?**
  - A service for managing AWS and third-party resources by launching them together as a stack.
  - Allows creation, update, and deletion of an entire stack using a template, managing resources as a unit.
- **Key Features**
  - **Template:** JSON or YAML formatted file used to build AWS resources.
  - Stack: A collection of resources created as a unit.
  - **Change Sets:** Preview and manage changes before applying them to resources.
  - **StackSets:** Provision, update, or delete stacks across multiple accounts or regions.
  - **Nested Stacks:** Stack within another stack to reuse resources, reducing duplication.
  - **AWS CloudFormation Registry:** Integrates third-party resources with AWS resources (e.g., incident management, and version control tools).
- **Integration with Other AWS Services**
  - Can be integrated with IAM for security and CloudTrail to capture API calls as events.
- **Stack Updates**
  - **Direct Update:** Quick deployment of changes.
  - **Creating and Executing Change Sets:** Preview changes in JSON files before applying.
- **Pricing**
  - No charge for using CloudFormation itself; charges apply for the AWS resources it provisions.
  - **Free Tier:** 1,000 handler operations per month per account.
  - **Handler Operations:** $0.0009 per operation beyond the free tier.
  - **Namespaces Supported:** AWS::, *Alexa::*, and Custom::*. Charges apply for other namespaces.

Analytics

Amazon Athena:

Serverless interactive SQL query service for analyzing data stored in S3.

- **Key Features:**
  - Runs ANSI SQL queries on various formats (CSV, JSON, ORC, Avro, Parquet).
  - Integrates with Amazon QuickSight.
- **Pricing:** Billed per data scanned; DDL commands are free; costs reduced via compression, partitioning, and columnar formats.

Amazon EMR:

Managed cluster service for processing and analyzing big data with frameworks like Hadoop, Spark, Hive, and Flink.

- **Key Features:**
  - Scalable clusters on EC2; decouples compute (clusters) from storage (S3).
  - Supports machine learning, clickstream analysis, and real-time streaming.
- **Access:** EMR Console, CLI, SDK, and API.

AWS Glue:

Serverless ETL service for extracting, transforming, and loading data.

- **Key Features:**
  - Automates data cataloging and code generation (Python/Scala).
  - Processes semi-structured data using dynamic frames.
- **Use Cases:** Data migration, integration, and preparation for analytics.

Amazon Data Firehose:

Serverless service for capturing, transforming, and delivering streaming data.

- **Key Features:**
  - Synchronously replicates data across AZs.
  - Supports transformation, compression, and encryption.
  - Delivers data to S3, Redshift, Elasticsearch, and Splunk.
- **Latency:** Minimum 60 seconds or when 32 MB of data is collected.

Amazon Kinesis Data Streams:

Real-time data streaming service to collect, process, and analyze streaming data.

- **Key Features:**
  - Scalable shards (default retention 1 day, extendable to 7 days).
  - Captures data from sources like websites, events, and social media.
  - Each shard offers 1MB/sec input and 2MB/sec output capacity.

Comparison of Amazon Data Firehose & Amazon Kinesis Data Streams

Category	Amazon Data Firehose	Amazon Kinesis Data Streams
Purpose	Ingests, transforms, and delivers data to AWS destinations.	Collects and processes streaming data for custom applications.
Management	Fully managed; auto-buffers and delivers data.	Requires manual management of shards and consumers.
Latency	Near real-time (min 60 sec or on size threshold).	Low latency; processes data immediately.
Use Cases	Simple ingestion and loading into S3, Redshift, etc.	Real-time analytics and custom stream processing.
Data Retention	Temporary buffering only.	Configurable retention (24 hours to 7 days).
Integration	Directly integrates with AWS storage/analytics services.	Integrates with custom consumers via APIs and Kinesis Client Library.
Overhead	Minimal operational overhead.	Higher operational management required.

Amazon OpenSearch Service:

Managed service to deploy, operate, and scale Elasticsearch/OpenSearch clusters.

- **Key Features:**
  - Direct access to Elasticsearch APIs.
  - Integrated with Kibana (visualization) and Logstash (log ingestion).
  - Auto-scales and auto-replaces failed nodes.
- **Pricing:** Billed per EC2 instance hour and attached storage; free data transfer within AZs.

Amazon QuickSight:

Scalable, cloud-based business intelligence (BI) service for interactive dashboards.

- **Key Features:**
  - Connects to diverse data sources.
  - Offers auto-forecasting, anomaly detection, and natural language query (Amazon Q).
  - Provides enterprise-grade security (SSO, row-level security, encryption).
- **Pricing:** Flexible per-user or capacity-based models; reader fees start at ~$3/month; no upfront licensing costs.

Database

AWS Database Migration Service (DMS)

AWS Database Migration Service (AWS DMS) is a cloud-based solution designed to facilitate the migration of various types of data stores, including relational databases, data warehouses, and NoSQL databases. With AWS DMS, you can transfer your data seamlessly to the AWS Cloud or between different environments, such as cloud and on-premises configurations.

Benefits

- **Comprehensive Migration Workflow:** Discover, assess, convert, and migrate databases and analytics workloads to AWS using automated tools.
- **Minimal Downtime:** Ensure high availability with Multi-AZ support and continuous data replication during migration.
- **Flexible Database Support:** Perform migrations between similar (homogeneous) or different (heterogeneous) database types, including Oracle, SQL Server, PostgreSQL, MySQL, MongoDB, and MariaDB.
- **Cost-Effective Migration:** Migrate large databases (up to terabytes) by paying only for the compute resources and log storage used.

Use Cases

- **Transition to Managed Databases:** Simplify operations, eliminate licensing fees, and boost business growth.
- **Ongoing Data Replication:** Facilitate seamless integration with data lakes and other analytics systems.

Amazon RDS

Amazon RDS simplifies operating, managing, and scaling relational databases in the cloud. It offers cost-efficient pricing, automates administrative tasks, and supports multiple database engines.

Supported Database Engines

1. **MySQL:** Popular open-source database. Focus on application development without managing infrastructure.
2. **MS SQL:** Developed by Microsoft. Supports provisioned IOPS or standard storage.
3. **MariaDB:** Open-source, created by MySQL developers. Infrastructure management is automated.
4. **PostgreSQL:** Preferred open-source relational database for enterprises.
5. **Oracle:** Fully managed commercial database engine. Licensing models: "License Included" or "Bring Your Own License (BYOL)."
6. **Amazon Aurora**
    - AWS-developed relational database engine.
    - MySQL and PostgreSQL-compatible.
    - Faster and more cost-efficient than traditional MySQL/PostgreSQL.
    - Supports up to 15 read replicas.

Key Features

Multi-AZ Deployment

- Creates a synchronous standby replica in another availability zone.
- Ensures disaster recovery (not for performance).

Read Replicas

- Creates read-only copies for performance enhancement.
- Can be used across regions for disaster recovery.

Storage Types

- **General Purpose (SSD):** 3 IOPS/GiB, bursts up to 3,000 IOPS.
- **Provisioned IOPS (SSD):** 1,000–30,000 IOPS for I/O-intensive workloads.

Monitoring

- Enhanced monitoring is optional and incurs additional costs.
- Metrics include IOPS, latency, throughput, and queue depth.

Backups & Restore

- Automatic backup retention: 1–35 days (default: 7 days via console).
- Up to 100 manual snapshots per region.

Pricing Factors

- Active RDS instances. Storage and requests.Backup and enhanced monitoring. Cross-region replication and data transfer.

Amazon DynamoDB

Amazon DynamoDB is a fully managed, NoSQL, serverless database designed for applications requiring single-digit millisecond latency. It scales automatically, requires no maintenance, and offers strong security and compliance features.

Why Choose DynamoDB?

1. **Serverless Simplicity**
   - Pay only for usage.
   - Automatic scaling, no cold starts, version upgrades, or downtime.
2. **Global Availability**
   - Supports multi-Region, multi-active global tables.
   - Provides a 99.999% SLA for high availability and resilience.
3. **Event-Driven Architecture**
   - DynamoDB Streams enable the building of serverless, event-driven applications.
4. **Data Reliability**
   - Managed backups and point-in-time recovery for data protection.

Benefits of DynamoDB

High Performance: Offers consistent low latency and supports virtually unlimited throughput and storage.

Global Scalability: Multi-region global tables ensure fast, local read/write performance.

Cost Optimization: Fully serverless design that scales to zero when not in use, reducing costs.

AWS Ecosystem Integration: Seamless integration with AWS tools for analytics, insights, and additional features.

Concepts

1. **Data Model**
   - **Tables**: Collections of items; no predefined schema required, only a primary key.
   - **Items and Attributes**: Items can have various attributes (name-value pairs) with a maximum item size of 400 KB.
   - **Data Types**:
     - Scalar: Number, String, Binary, Boolean, Null.
     - Multi-valued: Sets (e.g., String Set, Number Set).
     - Document: List and Map.
2. **Primary Key Types**
   - **Hash Key**: Single attribute key.
   - **Hash and Range Key**: Composite key for finer granularity.
3. **Indexes**
   - **Local Secondary Index (LSI)**: Shares the hash key with the table but uses a different range key.
   - **Global Secondary Index (GSI)**: Independent hash and range keys; allows up to 5 LSIs and 5 GSIs per table.
4. **Operations**
   - **Query**: Retrieves data using the primary key and optional conditions on range keys.
   - **Scan**: Reads all items in a table or index; supports filters to limit returned attributes.

Amazon ElastiCache

Amazon ElastiCache is a fully managed in-memory caching service that boosts application performance and reduces latency. It supports Redis and Memcached engines, offering significantly faster data retrieval compared to traditional disk-based databases.

Key Features

- **High Availability**: Maintains access even during data center outages.
- **Key-Value Data Retrieval**: Retrieves data in a key-value pair format.
- **Node-Based Storage**: Data is stored in network-attached RAM nodes, with automatic replacement for failed nodes.

Memcached Features

- **Volatile Data**: Data is not retained after a restart.
- **Simple Data Types**: Supports basic data types only.
- **Multi-Threading**: Utilizes multiple threads for operations.
- **Scalability**: Add/remove nodes; nodes can span across AZs.
- **No Multi-AZ Failover**: Lacks cross-AZ failover support.

Redis Features

- **Non-Volatile Data**: Retains data on restart.
- **Complex Data Types**: Supports strings, hashes, and geospatial indexes.
- **Single Threaded**: Operates on a single thread.
- **Sharding for Scaling**: Scales by adding shards (collections of primary nodes and replicas).
- **Multi-AZ Failover**: Supports read replicas in other AZs for failover.

Best Practices

- **Web Sessions**: Use Redis to store sessions for load-balanced web applications.
- **Database Caching**: Use Memcached for repetitive query results to enhance RDS performance.
- **Polling & Gaming Dashboards**: Use Memcached for quick access to frequently used data.
- **Hybrid Architecture**: Combine RDS and ElastiCache for backend optimization.

Pricing Highlights

- **Node-Based Charges**: Costs are per node hour (partial hours are rounded up).
- **On-Demand & Reserved Nodes**: Pricing options available.
- **No Intra-AZ Charges**: Free data exchange between ElastiCache and EC2 within the same AZ.

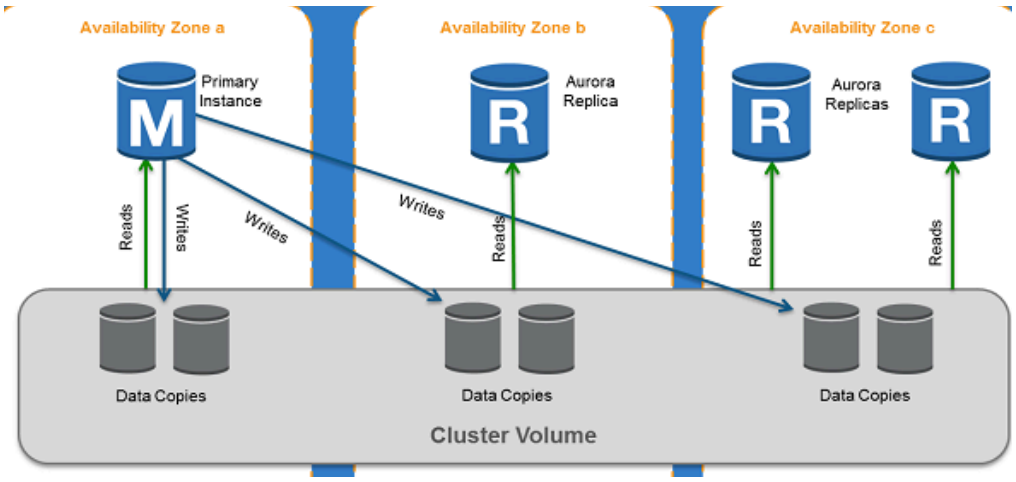
Amazon Aurora

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.

—-Back to Index—

Amazon DocumentDB

What is Amazon DocumentDB?

DocumentDB is a fully managed document database service by AWS which supports MongoDB workloads. It is highly recommended for storing, querying, and indexing JSON Data.

Features:

- It is compatible with MongoDB versions 3.6 and 4.0.
- All on-premise MongoDB or EC2 hosted MongoDB databases can be migrated to DocumentDB by using DMS (Database Migration Service).
- All database patching is automated in a stipulated time interval.
- DocumentDB storage scales automatically in increments of 10GB and maximum up to 64TB.
- Provides up to **15 Read replicas** with single-digit millisecond latency.
- All database instances are highly secure as they reside in VPCs which only allow a given set of users to access through security group permissions.
- It supports **role-based access control (RBAC).**
- Minimum **6 read copies of data is created in 3 availability zones making it fault-tolerant**.
- **Self-healing** – Data blocks and disks are continuously scanned and repaired automatically.
- All cluster snapshots are user-initiated and stored in S3 till explicitly deleted.

Best Practices:

- It reserves 1/3rd RAM for its services, so choose your instance type with enough RAM so that performance and throughput are not impacted.
- Setup Cloudwatch alerts to notify users when the database is reaching its maximum capacity.

Use Case:

- Highly beneficial for workloads that have flexible schemas.
- It removes the overhead of keeping two databases for operation and reporting. Store the operational data and send them parallel to BI systems for reporting without having two environments.

Pricing:

- Pricing is based on the instance hours, I/O requests, and backup storage.

Developer Tools

AWS CodeBuild

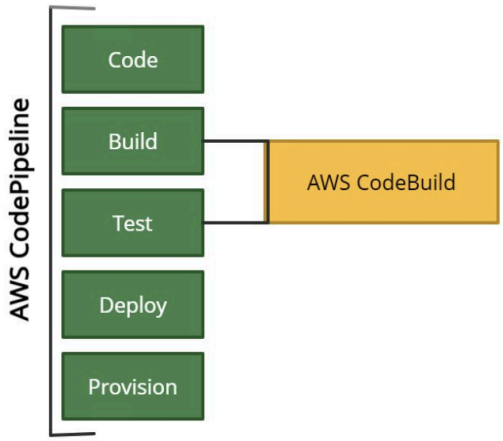
AWS CodeBuild is a fully managed continuous integration (CI) service that compiles source code, runs tests, and builds packages for deployment.

Features

- **Complete CI/CD Integration**: Part of AWS Code Services (CodeBuild, CodeCommit, CodeDeploy, CodePipeline) for end-to-end automation of CI/CD pipelines.
- **Prepackaged & Custom Build Environments**: Supports many programming languages and tools with both preconfigured and customizable build environments.
- **Auto-Scaling**: Scales automatically to process multiple builds concurrently.
- **Pipeline Integration**: This can be used as the build or test stage in an AWS CodePipeline workflow.
- **VPC Access**: Requires VPC settings (ID, subnet IDs, security group IDs) to access resources within a VPC during build or test processes.
- **Pricing**: Charges based on the time taken to complete the build.

Use Cases

- **Deployment to AWS Services**: Works with AWS Lambda, Amazon S3, Amazon ECR, and AWS CodeArtifact for easy deployment of applications.
- **Build Performance Optimization**: Automatically provisions and scales build resources based on workload demands.
- **Pre-configured Environments**: Offers ready-to-use build environments for various programming languages, runtime versions, and build tools.



AWS CodeBuild

AWS CodeDeploy

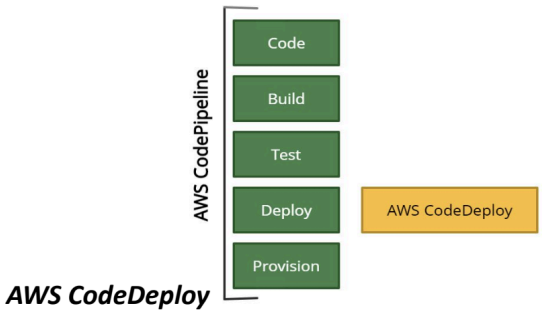
AWS CodeDeploy automates application deployments to various compute services like Amazon EC2, AWS Fargate, AWS ECS, and on-premises instances.

Features

- **Hybrid Kubernetes Management:** Manage Kubernetes clusters and applications across hybrid environments using Amazon EKS without modifying the code.
- **Flexible Deployment Sources:** Fetch deployment content from Amazon S3 buckets, Bitbucket, or GitHub repositories.
- **Versatile Content Support:** Deploy various application types, including code, Lambda functions, configuration files, scripts, and multimedia files.
- **Scalable Deployment:** Scales with infrastructure to deploy across multiple instances in development, test, and production environments.
- **Integration with CI/CD:** Seamlessly integrates with AWS CodePipeline, GitHub, Jenkins, and other delivery workflows.

Use Cases

1. **In-Place Deployment**
   - Stops all instances in the deployment group, updates with the new revision, and restarts them after completion.
   - Best suited for EC2 or on-premises computing platforms.
2. **Blue/Green Deployment**
   - Replace original environment instances with new instances from the replacement environment.
   - Traffic is rerouted using Elastic Load Balancer, and original instances are terminated post-deployment.
   - Suitable for EC2, on-premises, AWS Lambda, and Amazon ECS compute platforms.



AWS CodeArtifact

AWS CodeArtifact is a fully managed software artifact repository service designed to help organizations store, manage, and share software artifacts like libraries, packages, and dependencies. It streamlines development and deployment workflows, especially for teams using multiple programming languages.

Features

1. **Centralized Artifact Repository**

- Provides a centralized location for storing and managing software artifacts.

2. **Support for Multiple Package Formats**

- Supports popular package formats like:
  - **npm** (Node.js)
  - **Maven** (Java)
  - **PyPI** (Python)

3. **Security and Access Control**

- Integrates with **AWS Identity and Access Management (IAM)** for controlling access and publishing rights to artifacts.

4. **Dependency Resolution**

- Resolves project dependencies efficiently, ensuring compatibility and smooth builds.

5. **Integration with Popular Tools**

- Seamlessly integrates with build and deployment tools such as:
  - AWS CodePipeline
  - AWS CodeBuild
  - AWS CodeDeploy

AWS CodePipeline

AWS CodePipeline is a Continuous Integration (CI) and Continuous Delivery (CD) service that automates the build, test, and deployment phases of your software release process.

Features

1. **Pipeline Stages**
   - **Source Stage**: Specifies the source code repository (e.g., CodeCommit, GitHub) and triggers the pipeline when changes are detected.
   - **Build Stage**: Uses tools like AWS CodeBuild to compile code, run tests, and create deployable artifacts.
   - **Test Stage**: Integrates testing tools to validate that the application meets quality standards.
   - **Deployment Stage**: Deploys the application to environments like AWS Elastic Beanstalk, Lambda, or ECS.
   - **Approval Actions**: Manual approval steps before promoting changes to production.
   - **Notifications**: Sends alerts via Amazon SNS or other channels about pipeline events.
2. **AWS Integration**
   - Seamless integration with AWS services like CodeBuild, CodeDeploy, CodeCommit, Elastic Beanstalk, and Lambda.

Concepts

- **Pipeline**: Defines the workflow for your release process, detailing how a new code change progresses through various stages like build, test, and deploy.
- **Stages**: Logical divisions of the pipeline, including actions like building code or deploying to test environments. Each pipeline must have at least two stages: a source stage and a build or deployment stage.
- **Actions**: Tasks performed within each stage (e.g., build, test, or deploy). These actions occur in a specified order, either serially or in parallel.
- **Revisions**: Changes made to the source code or other items in the pipeline. A pipeline can handle multiple revisions simultaneously.
- **Transition**: Defines whether actions can proceed between stages. Transitions can be enabled or disabled.
- **Approval Action**: A step that halts the pipeline until manually approved, often used for code reviews before deployment.

Use Cases

- **Web Application Deployment**: Automate deployment for web apps hosted on AWS.
- **Serverless Application Deployment**: Automate deployment for serverless apps with Lambda and API Gateway.
- **CI/CD for Containerized Applications**: Automate the pipeline for containerized applications on ECS or EKS.

- **Graphical User Interface**: Allows easy creation, configuration, and management of pipelines.
- **Automatic Triggers**: Pipelines can start automatically when changes are detected or when manually initiated.
- **Parallel Execution**: Actions like build, test, and deployment can be modeled to run in parallel, enhancing workflow speed.
- **Integration with AWS Services**: CodePipeline integrates with AWS CodeCommit, GitHub, Amazon S3, and more for source code, and AWS CodeBuild, CodeDeploy, Elastic Beanstalk, ECS, and others for deployment.
- **Webhooks**: Creates webhooks for automatic triggering based on events from tools like GitHub.
- **Jenkins Integration**: Supports Jenkins as a custom action provider, allowing the use of existing Jenkins servers for build or test actions.
- **Amazon VPC Endpoints**: Supports private connectivity through AWS PrivateLink to keep traffic within your VPC.
-

Pricing

- **Cost**: $1.00 per active pipeline/month.
- **Free Tier**: First 30 days free, one active pipeline free monthly (across regions).
- Additional charges apply for storing artifacts in S3 and third-party integrations.
- **Limitations:**
- **Number of Pipelines**: Up to 300 pipelines per AWS account per region.
- **Number of Stages**: A pipeline can have a minimum of 2 and a maximum of 10 stages.

AWS CodeStar

Feature	Details
Project Templates	Offers pre-configured templates for various languages and application types to jumpstart development projects.
Integrated Development Tools	Integrates with AWS Cloud9, Visual Studio Code, and others, providing a unified development environment.
CI/CD Automation	Automates build, test, and deployment processes via integration with CodePipeline, CodeBuild, and CodeDeploy.
Centralized Management	Provides a dashboard to manage projects, monitor progress, and facilitate team collaboration.
Limitations	Customization may be limited compared to more flexible, self-managed setups, and it relies heavily on other AWS services like CodeCommit, CodeBuild, and CodeDeploy.

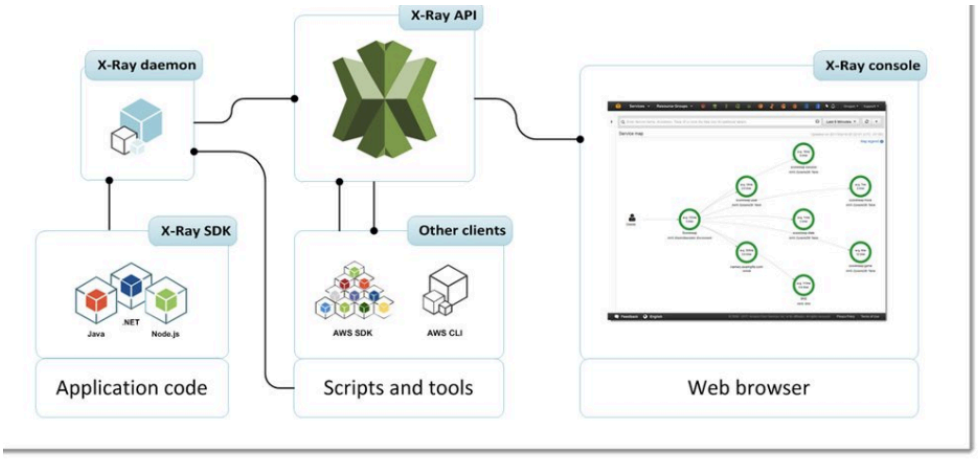
AWS X-Ray

AWS X-Ray is a service that provides visual analysis and tracing for microservices-based applications. It helps developers understand the application's behaviour and identify performance bottlenecks.

Features

1. **End-to-End Request Tracing**
   - Tracks requests and responses as they travel through the application's underlying components.
   - Includes calls to other AWS resources for a comprehensive view of interactions.
2. **Service Graph Creation**
   - Builds a service graph using trace data from AWS resources.
   - Displays details about front-end and back-end service calls.
3. **Troubleshooting and Performance Optimization**
   - Provides insights into application performance and operational issues.
   - Helps identify bottlenecks and improve overall application efficiency.

The X-Ray SDKs are available for the following languages:
Go, Java, Node.js, Python, Ruby



Security, Identity & Compliance

AWS IAM Identity Center

Purpose:

AWS IAM Identity Center simplifies workforce access to AWS applications by connecting existing identity sources and providing a centralized management solution.

Key Features:

- Seamlessly integrates with existing identity systems.
- Provides a unified user experience across AWS applications.
- Works alongside current AWS account access configurations.

Benefits

- **Streamlined Access:** Connect your identity source to simplify workforce access to AWS applications.
- **Centralized Management:** Manage user access efficiently across AWS applications.
- **Enhanced Control:** Gain improved visibility and control over user access to application data.
- **Multi-Account Support:** Centrally manage access across multiple AWS accounts.

Why Choose IAM Identity Center?

- **Scalable Access Management:** Securely manage access across AWS accounts and applications.
- **Support for Tools like Amazon Q Developer:** Facilitate productivity in IDEs and the command line.

Use Cases

- **Unified User Experience:** Offer consistent and seamless access for workforce users across AWS applications.
- **Application Access Management:** Control access to AWS applications effectively.
- **Audit and Configure Access:** Manage user and group permissions for application data.
- **Single Sign-On (SSO):** Enable SSO for Amazon EC2 Windows instances.
- **Multi-Account Environments:** Simplify access control for users across multiple AWS accounts.

AWS WAF

What is AWS WAF?

- **AWS WAF** (Web Application Firewall) is a managed service that helps protect web applications from common exploits like SQL injection, cross-site scripting (XSS), and DDoS attacks.
- It provides an **additional security layer** to safeguard application availability, security, and resource consumption.

Features:

- **Integration with AWS services**: Combine AWS WAF with services like **AWS Shield** (DDoS protection) and **Amazon CloudFront** (content delivery) for a **multi-layered security approach**.
- **Managed Rule Sets**: Keep **AWS Managed Rule Sets** up to date for protection against emerging threats.
- **Logging**: Enable logging to capture detailed information about web requests and potential threats. Use **Amazon CloudWatch** or SIEM solutions for monitoring and analysis.
- **Rate-limiting**: Implement **rate-limiting rules** to protect APIs from abuse and DDoS attacks by setting limits based on traffic patterns.
- **Web ACLs**: Customize **web access control lists (ACLs)** according to the specific needs of your application.
- **Regular rule reviews**: Periodically **review and adjust AWS WAF rules** based on changing requirements and evolving threats.

AWS Firewall Manager

Overview

- Simplifies administration and maintenance across multiple accounts and resources for various protections (AWS WAF, AWS Shield Advanced, VPC security groups, network ACLs, AWS Network Firewall, Route 53 Resolver DNS Firewall).
- Protects resources by applying security configurations across accounts and resources, even when new ones are added.

Key Benefits

- Cross-account Protection: Protects resources across multiple accounts.
- Resource-based Protection: Secures all resources of a specific type (e.g., CloudFront distributions).
- Tag-based Protection: Secures resources based on specific tags.
- Automatic Protection: Automatically adds protection to new resources as they are added to your account.
- Centralized Management for Shield Advanced: Subscribes all member accounts in an AWS Organizations organization to AWS Shield Advanced and automatically subscribes new accounts.
- Security Group Management: Allows applying security group rules to all or specific subsets of accounts in an AWS Organization, and auto-applies to new accounts.
- Custom and Managed Rules: Allows using custom rules or purchasing managed rules from AWS Marketplace.

Use Cases

- Ideal for organizations protecting multiple accounts and resources or frequently adding new resources.
- Provides centralized monitoring of DDoS attacks across the organization.

Amazon GuardDuty

Overview

- Managed threat detection service that monitors AWS accounts for security threats.
- Uses machine learning, threat intelligence feeds, and log analysis to detect suspicious activities.
- Analyzes AWS CloudTrail logs, VPC Flow Logs, and DNS logs for anomalies.
- Generates actionable findings and alerts for remediation.

Features

- Ensure complete detection coverage by enabling VPC Flow logs for all regions and necessary interfaces.
- GuardDuty is Region-specific; enable it for all regions for full visibility.
- Analyze GuardDuty findings with CloudTrail to detect tampering.
- Integrate GuardDuty with EventBridge and Lambda for automated risk mitigation.

Use Cases

- Assist security analysts with investigation using GuardDuty's findings, context, and impacted resource details.
- Detect malware in EBS files or suspicious behaviour on EC2 container workloads.
- Automatically enable log sources (VPC Flow logs, DNS logs) for GuardDuty—no need for manual configuration.
- Cannot add custom log sources, only the five supported by GuardDuty.

Amazon Detective

Amazon Detective is a security service that helps you analyze and investigate security findings, leveraging a security behaviour graph to visualize data and gain insights into potential threats.

Requirements for Enabling Amazon Detective

- **GuardDuty**: Must be enabled for at least 48 hours for Amazon Detective to function.
- **Data Flow**: The volume of data flowing into the security behaviour graph must be within allowed limits.
- **Regional Service**: Amazon Detective is a regional service and needs to be enabled for each region.

Features

- **Integration with GuardDuty & Security Hub**:
    - GuardDuty findings can be pivoted to Amazon Detective for detailed investigation.
    - The option to archive findings is available during the investigation.
- **Notification Updates**: To reduce update time, it is recommended to set CloudWatch notification frequency to 15 minutes instead of the default 6 hours.

Use Cases

- **Triage Security Findings/Alerts**: Helps determine if GuardDuty findings require further investigation.
- **Incident Investigation**: Allows for historical analysis (up to one year) to identify when a security issue started and its impact.
- **Threat Hunting**: Investigate interactions of IP addresses and users with the environment using the Security Behavior Graph.

AWS Trusted Advisor

What is AWS Trusted Advisor?

Trusted Advisor itself provides checks based on Best Practices in the Cost Optimization, Security, Fault Tolerance, and Performance improvement categories.

Category	Recommendations
Cost Optimization	Suggests terminating unused or idle resources and using Reserved capacity for continuous usage to save costs.
Security	Recommends restricting access using Security Groups (SG)/Network Access Control Lists (NACL), checking S3 bucket permissions, and enabling security features.
Fault Tolerance	Advises on increasing availability and redundancy by using Auto Scaling, performing health checks, configuring Multi-AZ environments, and taking backups.
Performance	Provides suggestions for improving performance by leveraging provisioned throughput and monitoring over-utilized instances.
Service Limits	Notifies when resource usage exceeds 80% of the allocated limits.

Use cases:

- **Optimization of cost & efficiency -** Trusted Advisor helps identify resources that are not used to capacity or idle resources and provides recommendations to lower costs.
- **Address Security Gaps -** Trusted Advisor performs Security checks of your AWS environment based on security best practices. It flags off errors or warnings depending on the severity of the security threat e.g. Open SG/NACL ports for unrestricted external user access, and open access permissions for S3 buckets in Accounts.
- **Performance Improvement -** Trusted Advisor checks for usage & configuration of your AWS resources and provides recommendations that can improve performance e.g. it can check for Provisioned IOPS EBS volumes on EC2 instances that are not EBS-optimized.

Storage

AWS EFS (Elastic File Storage)

What is AWS EFS?

- Scalable, fully managed file storage based on NFS, supporting petabyte-level storage.
- Shared by thousands of EC2 instances for high throughput and IOPS.
- Automatically replicated across multiple AZs for high availability and durability.

Types of EFS Storage Classes

- **Performance Modes:**
  - General Purpose: Low latency, lower throughput.
  - Max I/O: High throughput, higher latency.
- **Throughput Modes:**
  - Bursting: Scales throughput with the file system.
  - Provisioned: Fixed throughput capacity.

Features

- Fully managed, scalable, and POSIX-compliant distributed file system.
- High availability and low latency across multiple AZs and regions.
- Integrated with AWS DataSync, CloudWatch, CloudTrail, and AWS Backup.
- Encryption at rest (via KMS) and in transit (via TLS).
- Supports lifecycle management for cost optimization.

Use Cases

- Mission-critical applications, microservices, container storage, web content management, media file storage, database backups, and analytics.

Best Practices

- Monitor with CloudWatch, and track with CloudTrail.
- Use IAM for access control.
- Test before migrating critical workloads.
- Separate latency-sensitive workloads for optimal I/O.

Pricing

- Pay based on access mode, storage type, and backup storage.

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 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.

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 up to 10 GB of archive data per month for free.
- Data transfer out from S3 Glacier in the same region is free.

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.

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.

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.

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 PrivateLink

Category	Description
Overview	AWS PrivateLink enables secure, private connectivity between VPCs and AWS services (or endpoint services) without using the public internet.
Endpoints	**Interface Endpoints:** Create an ENI in a subnet with a private IP for AWS service access. **Gateway Endpoints:** Route traffic to S3 and DynamoDB via the route table.
Use Cases	Connects service consumers to providers across VPCs securely, and supports secure on-premises migration via AWS Direct Connect or VPN.
Security & Integration	Enhances security by isolating traffic from the public internet and integrates with AWS Marketplace services, reducing exposure to DDoS and brute-force attacks.
Pricing	Charged based on the usage of endpoints.

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 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:

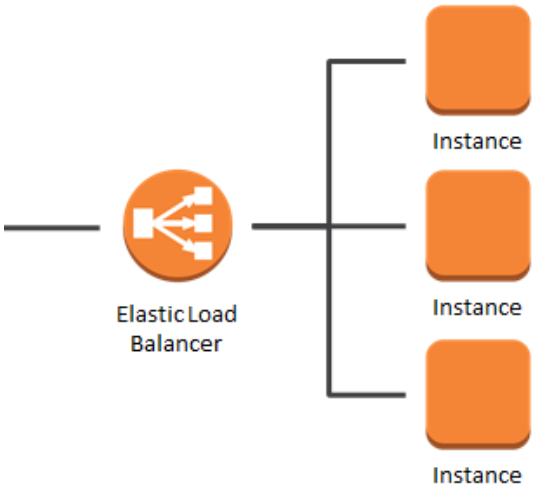
- **Application Load Balancer:** Ideal for web apps; routes traffic based on request content.
- **Network Load Balancer:** Suited for high-performance apps; supports TCP, UDP, and TLS protocols.
- **Gateway Load Balancer:** Designed for third-party appliances (e.g., security, analytics).
- **Classic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