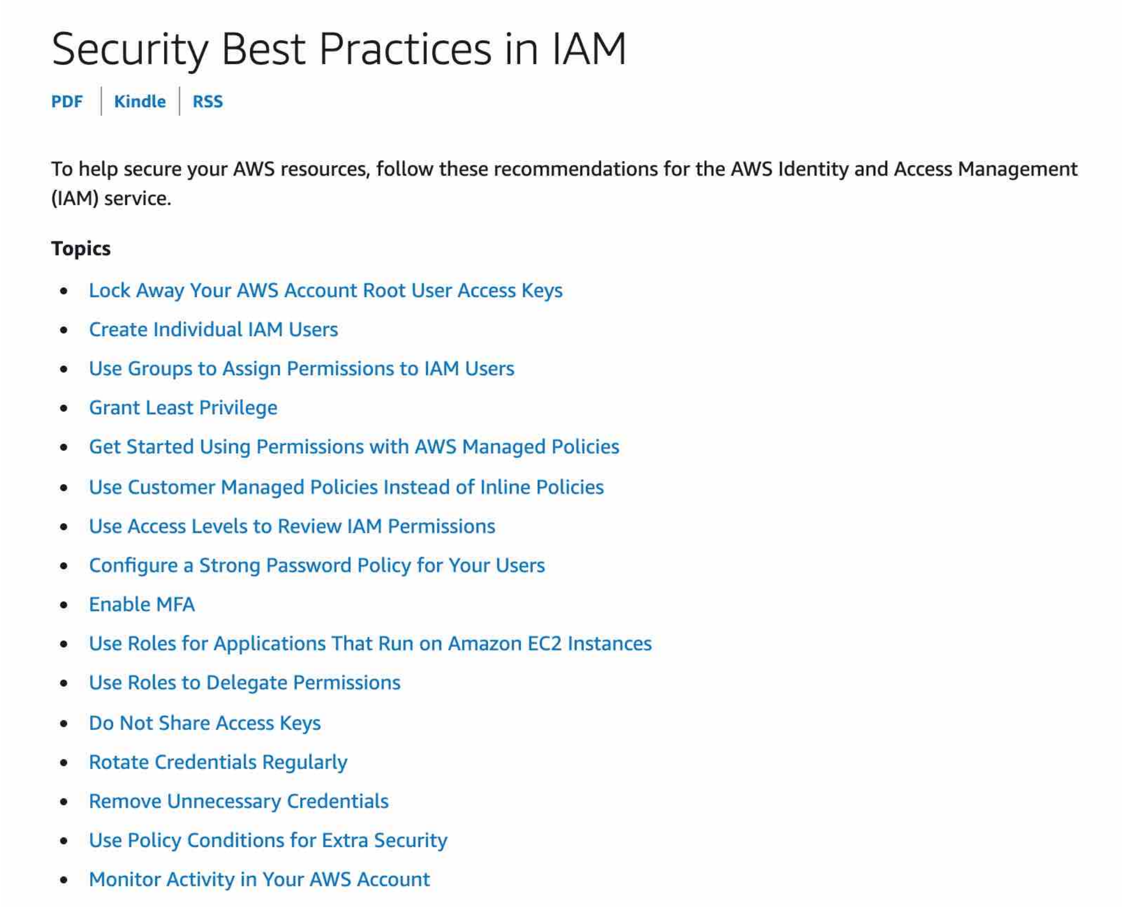
General Notes

◴ Created | @December 2, 2024 6:27 PM

▼ Cloud Concepts

- **Free AWS services** - AWS AutoScaling, AWS IAM, AWS Elastic Beanstalk
- **Global Services** - AWS IAM, Amazon CloudFront, AWS WAF, Amazon WorkSpaces
- IAM - Implementation of security resources
- **AWS IAM access advisor - review permissions granted to an IAM user**
- **AWS IAM Identity Center - simplify access management to multiple AWS accounts as well as facilitate AWS Single Sign-On (AWS SSO) access to its AWS accounts.**
- **Container service**- AWS Fargate, Amazon S3,
- Region = Minimum of 3 AZs, AZs = One or more discrete data centers in same location
- **CloudFront + S3 - static website hosting**
- S3 allows lifecycle configuration (transition action & expiration action)
- **DMS - DB to DB, Application Migration Service - DB to instance**
- **Best Practice for application architecture on AWS Cloud - Build loosely coupled components**
- **CloudWatch + SNS - Send alerts**
- **Best Practices for IAM**



Security Best Practices in IAM

PDF | Kindle | RSS

To help secure your AWS resources, follow these recommendations for the AWS Identity and Access Management (IAM) service.

Topics

- Lock Away Your AWS Account Root User Access Keys
- Create Individual IAM Users
- Use Groups to Assign Permissions to IAM Users
- Grant Least Privilege
- Get Started Using Permissions with AWS Managed Policies
- Use Customer Managed Policies Instead of Inline Policies
- Use Access Levels to Review IAM Permissions
- Configure a Strong Password Policy for Your Users
- Enable MFA
- Use Roles for Applications That Run on Amazon EC2 Instances
- Use Roles to Delegate Permissions
- Do Not Share Access Keys
- Rotate Credentials Regularly
- Remove Unnecessary Credentials
- Use Policy Conditions for Extra Security
- Monitor Activity in Your AWS Account

- AWS services that have data encryption automatically enabled are **Amazon Simple Storage Service (Amazon S3), AWS CloudTrail Logs & AWS Storage Gateway** while **Amazon Elastic Block Store (Amazon EBS), Amazon Redshift & Amazon EFS** don´t have data encryption automatically enabled.

> ### CloudTrail Logs can be used on EC2 instances & on-premises servers

- **AWS CloudTrail - L**og, monitor and retain account activity related to actions across your AWS infrastructure. Ensure that its AWS account activity meets the governance, compliance and auditing norms.
- **Serverless Services** - AWS Lambda, Amazon EventBridge, AWS Fargate, Amazon S3, Amazon DynamoDB, Amazon Aurora, Amazon API Getaway,

Amazon SNS & SQS, AWS AppSync, AWS StepFunction, Amazon Kinesis, Amazon Athena,

- **Advantages of Cloud** - Trade capital expenses for variable expenses, Benefit from massive economies of scale (**due to PAYG model**), Stop guessing capacity, Increase speed & **agility (ability to innovate faster and rapidly develop, test and launch software applications)**, Stop spending money running & maintaining data centers, AND Go global in minutes

> **A Security Group is stateful (allows return traffic) can have allow rules only.**

> **A Network Address Translation gateway (NAT gateway) is managed by AWS**

> **NACL contains a numbered list of rules and evaluates these rules in the increasing order while deciding whether to allow the traffic**

- **AWS Architecture Center - provides reference architecture diagrams, vetted architecture solutions, Well-Architected best practices, patterns, icons, etc.**
- **VPC Endpoint** - A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. There are two types of VPC endpoints: interface endpoints and gateway endpoints. **VPC Endpoint only supports Amazon S3 (also supports VPC Interface Endpoint) & Amazon DynamoDB**

> **only Amazon S3 and Amazon DynamoDB support VPC gateway endpoint.** All other services that support VPC Endpoints use a VPC interface endpoint (note that Amazon S3 supports the VPC interface endpoint as well).

> ### Connect VPC TO Amazon SQS = VPC Interface Endpoint

- **AWS Site-to-Site VPN** - AWS Site-to-Site VPN creates a secure connection between your data center or branch office and your AWS cloud resources. **Components are Customer gateway & Virtual private gateway (VGW).**
- **VPC peering connection -** A VPC peering connection is a networking connection between **two VPCs** that enables you to route traffic between them privately.
- **AWS Direct Connect** - AWS Direct Connect is a cloud service that links your network directly to AWS, bypassing the internet (**i.e., doesn´t need internet**) to deliver more consistent, lower-latency performance.
- **AWS Transit Gateway -** AWS Transit Gateway connects Amazon Virtual Private Clouds (Amazon VPC) and on-premises networks through a central hub. Works for multiple VPCs

> ### AWS Direct Connect & AWS Transit Gateway can be used to connect multiple VPCs & on-premises data center with the different VPC

> ### AWS Direct Connect & IGW can be used to connect your on-premises network with AWS Cloud

- **AWS Trusted Advisor** - AWS Trusted Advisor is an online tool that provides you real-time guidance to help you provision your resources following AWS best practices on **cost optimization, security, fault tolerance, service limits and performance improvement.**

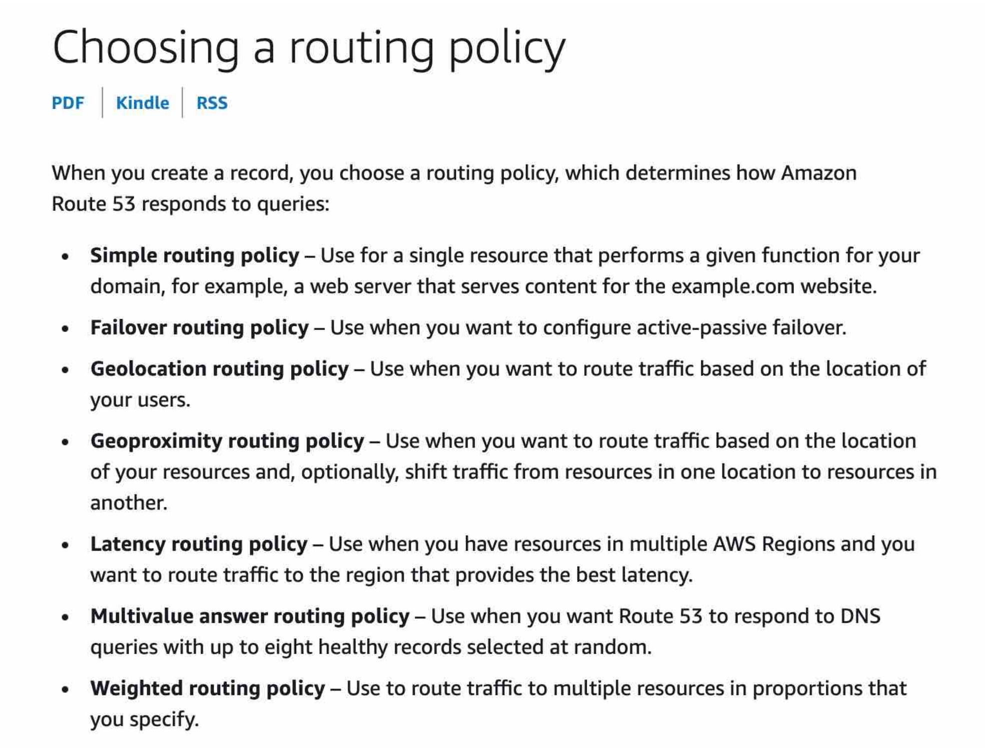
> ### AWS Trusted Advisor Provide alerts When you don't turn on user activity logging (AWS CloudTrail) & When you allow public access to Amazon S3 buckets

> **AWS Trusted Advisor can identify unattached or underutilized Amazon EBS Elastic Volumes**

- **AWS Systems Manager - operational insights of resources to quickly identify any issues that might impact applications using those resources.**
- **AWS Cost Explorer** - AWS Cost Explorer has an easy-to-use interface that lets you **visualize, understand, forecast, and manage your AWS costs and usage over time**.

> **AWS Cost Explorer** & **AWS Trusted Advisor can be used identify all Amazon Elastic Compute Cloud (Amazon EC2) instances that are under-utilized without needing any manual configurations.**

- **Route 53 - DNS & Health checks and monitoring. Route 53 routing policy** - Highly available and scalable cloud Domain Name System (DNS) web service.



Choosing a routing policy

PDF | Kindle | RSS

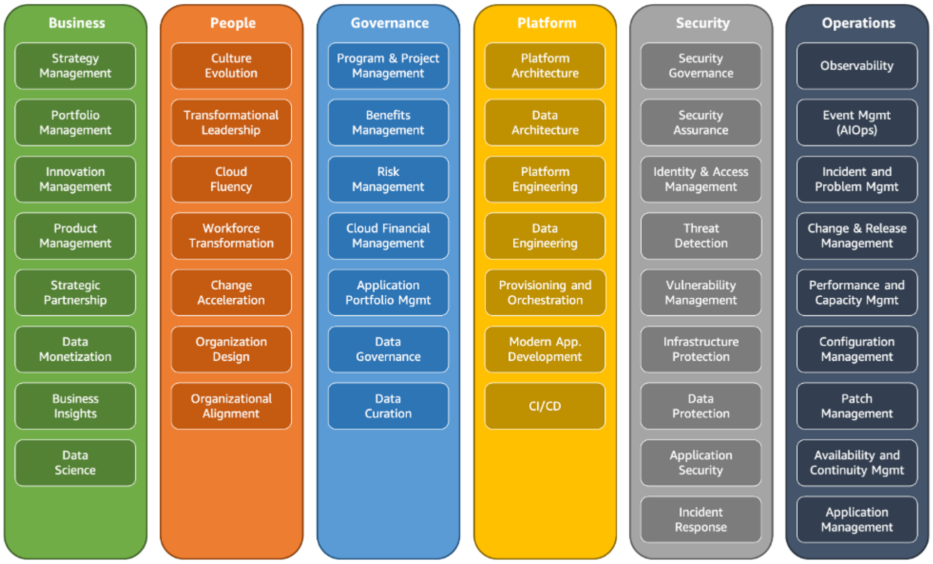
When you create a record, you choose a routing policy, which determines how Amazon Route 53 responds to queries:

- **Simple routing policy** – Use for a single resource that performs a given function for your domain, for example, a web server that serves content for the example.com website.
- **Failover routing policy** – Use when you want to configure active-passive failover.
- **Geolocation routing policy** – Use when you want to route traffic based on the location of your users.
- **Geoproximity routing policy** – Use when you want to route traffic based on the location of your resources and, optionally, shift traffic from resources in one location to resources in another.
- **Latency routing policy** – Use when you have resources in multiple AWS Regions and you want to route traffic to the region that provides the best latency.
- **Multivalue answer routing policy** – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
- **Weighted routing policy** – Use to route traffic to multiple resources in proportions that you specify.

- The AWS Partner Network (APN) is the global partner program for technology and consulting businesses that leverage Amazon Web Services to build solutions and services for customers and it is divided into:

1. **APN Consulting Partner -** Professional services firms that help customers of all types and sizes design, architect, build, migrate, and manage their workloads and applications on AWS, accelerating their migration to AWS cloud.
2. **APN Technology Partner** - APN Technology Partners provide hardware, connectivity services, or software solutions that are either hosted on or integrated with, the AWS Cloud.

- **AWS Partner Solutions** are automated reference deployments built by Amazon Web Services (AWS) solutions architects and AWS Partners.
- **Common stakeholder role** for the AWS WAF **Platform** perspective - **Chief Technology Officer (CTO), technology leaders, architects, and engineers.**



Business	People	Governance	Platform	Security	Operations
Strategy Management	Culture Evolution	Program & Project Management	Platform Architecture	Security Governance	Observability
Portfolio Management	Transformational Leadership	Benefits Management	Data Architecture	Security Assurance	Event Mgmt (AIOps)
Innovation Management	Cloud Fluency	Risk Management	Platform Engineering	Identity & Access Management	Incident and Problem Mgmt
Product Management	Workforce Transformation	Cloud Financial Management	Data Engineering	Threat Detection	Change & Release Management
Strategic Partnership	Change Acceleration	Application Portfolio Mgmt	Provisioning and Orchestration	Vulnerability Management	Performance and Capacity Mgmt
Data Monetization	Organization Design	Data Governance	Modern App. Development	Infrastructure Protection	Configuration Management
Business Insights	Organizational Alignment	Data Curation	CI/CD	Data Protection	Patch Management
Data Science				Application Security	Availability and Continuity Mgmt
				Incident Response	Application Management

- **Cloud Transformation Phases Of CAF:**

Envision - The Envision phase of the AWS Cloud Adoption Framework (AWS CAF) focuses on demonstrating how the cloud will help **accelerate your business outcomes.**

Align - The Align phase of the AWS Cloud Adoption Framework (AWS CAF) focuses on identifying capability gaps across the six AWS CAF perspectives, **identifying cross-organizational dependencies, and surfacing stakeholder concerns and challenges.**

Launch - The Launch phase of the AWS Cloud Adoption Framework (AWS CAF) focuses on **delivering pilot initiatives in production and on demonstrating incremental business value**.

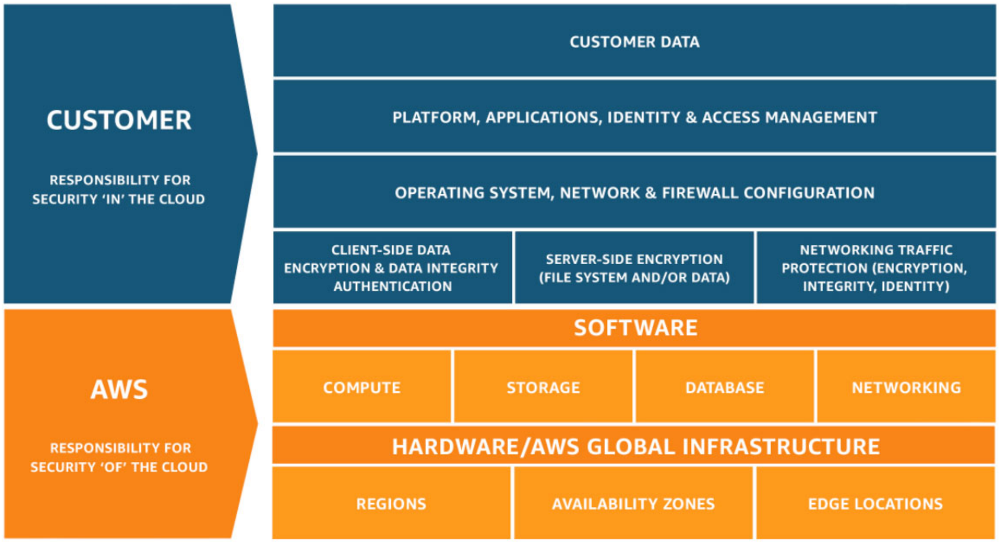
Scale - The Scale phase of the AWS Cloud Adoption Framework (AWS CAF) focuses on **expanding production pilots and business value to desired scale and ensuring that the business benefits associated with your cloud investments are realized and sustained.**

- **AWS Command Line Interface (CLI)** - The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services.
- **AWS Marketplace**: Sell SaaS, Software bundled into custom AMIs by sellers.
- SaaS - All is managed by service provider, PaaS - All except applications & data is managed by service provider e.g., AWS, IaaS - service provider manages server & network (infrastructure)

Category	**AWS Services**
IaaS	Amazon EC2, Amazon S3, Amazon EBS, Amazon Glacier, Amazon VPC, AWS Direct Connect, Elastic Load Balancing, Route 53, AWS Snow Family
PaaS	AWS Elastic Beanstalk, AWS Amplify, Amazon RDS, Amazon DynamoDB, Amazon Redshift, Amazon SageMaker, AWS Glue, Amazon EMR, AWS Step Functions, Amazon MQ, Amazon ECS, Amazon EKS, AWS Lambda, Amazon API Gateway

SaaS	Amazon Chime, Amazon WorkSpaces, Amazon WorkDocs, Amazon Connect, AWS Trusted Advisor, AWS Shield, AWS WAF, Amazon CloudFront

- **Client-side encryption** - Encrypting data before sending it to Amazon S3. This can be done using AWS SDK
- AWS Shared Responsibilty


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Billing & Pricing

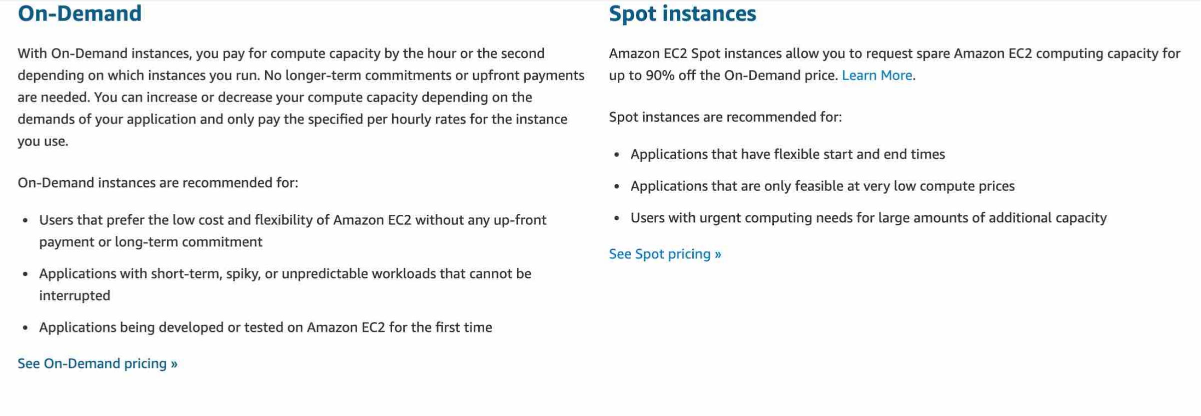
- **AWS Budgets** - AWS Budgets gives the ability to set custom budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount. **Usage, Reservation, Savings Plan & Cost Budget are budgets that can be created**.
- **AWS Pricing Calculator -** AWS Pricing Calculator lets you explore AWS services and create an estimate for the cost of your use cases on AWS.
- **EC2 Spot instances** are cheapest with up to 90% discount but can be gone in an instant while **EC2 RI** is next cheapest option with up to 75% discount compared to On-demand instances & Dedicated hosts. **On-demand instances** are billed per seconds and has 1 minute (60 secs) minimum

charge but it is the most cost-effective and flexible with no requirement for a **long term resource commitment.**

On-demand < RI

RI (only for predictable usage) < On-demand

Partial-upfront 3 years RI < All-upfront 1 yr RI



On-Demand

With On-Demand instances, you pay for compute capacity by the hour or the second depending on which instances you run. No longer-term commitments or upfront payments are needed. You can increase or decrease your compute capacity depending on the demands of your application and only pay the specified per hourly rates for the instance you use.

On-Demand instances are recommended for:

- Users that prefer the low cost and flexibility of Amazon EC2 without any up-front payment or long-term commitment
- Applications with short-term, spiky, or unpredictable workloads that cannot be interrupted
- Applications being developed or tested on Amazon EC2 for the first time

See On-Demand pricing »

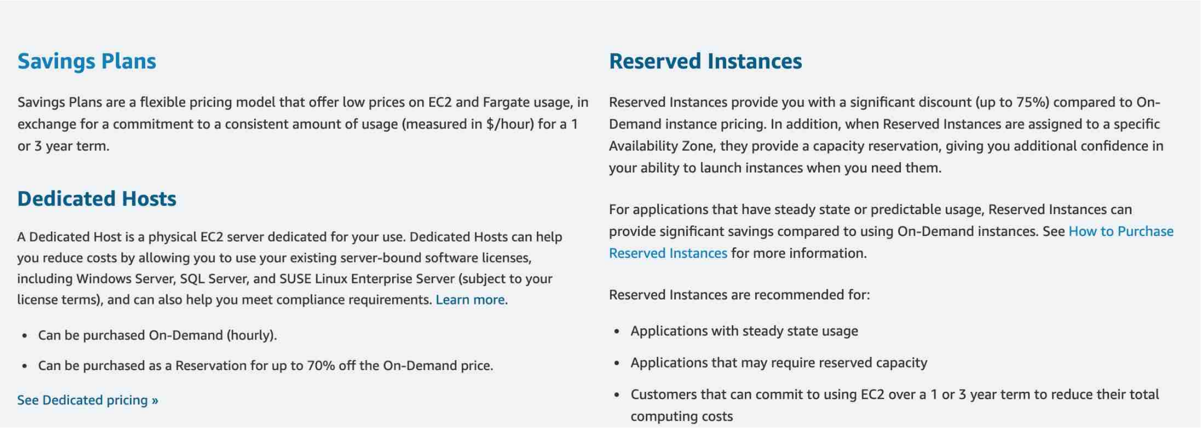
Spot instances

Amazon EC2 Spot instances allow you to request spare Amazon EC2 computing capacity for up to 90% off the On-Demand price. Learn More.

Spot instances are recommended for:

- Applications that have flexible start and end times
- Applications that are only feasible at very low compute prices
- Users with urgent computing needs for large amounts of additional capacity

See Spot pricing »



Savings Plans

Savings Plans are a flexible pricing model that offer low prices on EC2 and Fargate usage, in exchange for a commitment to a consistent amount of usage (measured in $/hour) for a 1 or 3 year term.

Dedicated Hosts

A Dedicated Host is a physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses, including Windows Server, SQL Server, and SUSE Linux Enterprise Server (subject to your license terms), and can also help you meet compliance requirements. Learn more.

- Can be purchased On-Demand (hourly).
- Can be purchased as a Reservation for up to 70% off the On-Demand price.

See Dedicated pricing »

Reserved Instances

Reserved Instances provide you with a significant discount (up to 75%) compared to On-Demand instance pricing. In addition, when Reserved Instances are assigned to a specific Availability Zone, they provide a capacity reservation, giving you additional confidence in your ability to launch instances when you need them.

For applications that have steady state or predictable usage, Reserved Instances can provide significant savings compared to using On-Demand instances. See How to Purchase Reserved Instances for more information.

Reserved Instances are recommended for:

- Applications with steady state usage
- Applications that may require reserved capacity
- Customers that can commit to using EC2 over a 1 or 3 year term to reduce their total computing costs

> ## Cost Benefit on RI applies only when RI from the two accounts are launched in the same AZ

- Amazon CloudWatch billing metric data is stored in **US East (N. Virginia) - us-east-1**
- **Concierge Support Team** - The Concierge Support Team are AWS billing and account experts that specialize in working with enterprise accounts.
- **AWS Organizations** helps you to centrally manage billing; control access, compliance, and security; and share resources such as r**eserved Amazon**

EC2 instances & Volume discounts for Amazon EC2 and Amazon S3 across your AWS accounts.

- Other S3 storage classes store data in a minimum of 3 AZs while Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA) stores data in a single Availability Zone (AZ) while offering the same high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval fee and costs 20% less than Amazon S3 Standard-Infrequent Access (S3 Standard-IA).

> S3 pricing components– storage pricing; request and data retrieval pricing; data transfer and transfer acceleration pricing; and data management features pricing

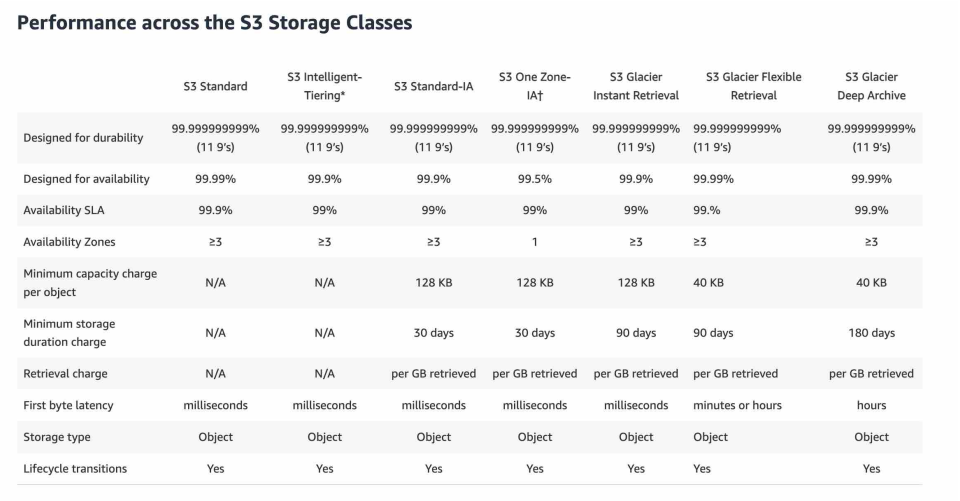
> **Free S3 services - Data transferred in from the internet & Data transferred out to an Amazon EC2 instance, when the instance is in the same AWS Region as the S3 bucket**

> S3 stores objects and not a DB service

1. **Glacier Flexible Retrieval** is a secure, durable, and low-cost storage class for **data archiving**. Amazon S3 Glacier Flexible Retrieval is cheaper than Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).
2. **Amazon S3 Standard** offers high durability, availability, and performance object storage for frequently accessed data. **Do not charge any data retrieval fee**
3. **Amazon S3 Standard-Infrequent Access (S3 Standard-IA)** storage class is for **data that is accessed less frequently** but requires rapid access when needed.
4. **Amazon S3 Glacier Deep Archive** is Amazon S3's lowest-cost storage class and supports **long-term retention and digital preservation** for data that may be accessed once or twice in a year. Also, it takes the most time to retrieve data (also known as first byte latency)

5. **Amazon S3 Intelligent-Tiering do not charge any data retrieval fee and lowest cost.**

> ### Amazon EC2, DynamoDB & RDS supports reservations to optimize costs



Performance across the S3 Storage Classes

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128 KB	128 KB	128 KB	40 KB	40 KB
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Storage type	Object	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes	Yes

- **AWS Migration Evaluator -** AWS Migration Evaluator (Formerly TSO Logic) is a complimentary service to create data-driven business cases for AWS Cloud planning and migration.
- AWS Lambda pricing is **based on compute time (the time it takes for the Lambda function to execute) & The number of requests for the AWS Lambda function**
- **Power/Cooling & Server administration is included in the Total Cost of Ownership (TCO) estimate**
- **CloudEndure Disaster Recovery -** continuously replicates server-hosted applications and server-hosted databases from any source into AWS using block-level replication of the underlying server (physical, virtual, and cloud-based).
- Amazon API Gateway **can call an AWS Lambda function to create the front door of a serverless application, support API result caching & can be configured to send data directly to Amazon Kinesis Data Stream**

▼ Technology

> **Onboarding (from on-premises to cloud) - AWS Service Catalog, AWS Partner Network**

> **EBS Snapshots are stored in Amazon S3**

> **Lambda + EventBridge = serverless solution to run a log backup process**

> **AWS DMS & Snowball - data migration from on-premises to AWS Cloud**

- **AWS Elastic Beanstalk** - AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services. PaaS.

> **AWS Elastic Beanstalk Health & Monitoring: With basic health reporting, the AWS Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch AND The AWS Elastic Beanstalk health monitoring can determine that the environment's Auto Scaling group is available and has a minimum of at least one instance**

> **With AWS Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications AND There is no additional charge for AWS Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes**

- **Amazon CloudWatch - resource utilization, application performance, and operational health**
- **Amazon SageMaker** - Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train,

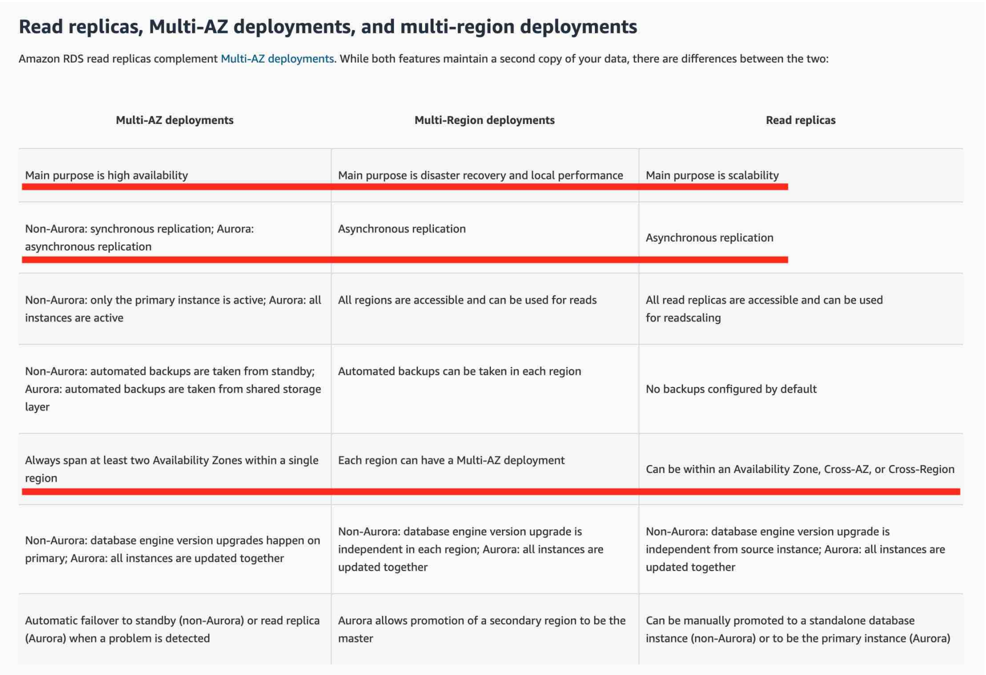
and deploy machine learning (ML) models quickly.

- AWS Compute Optimizer delivers recommendations for **Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon EC2 Auto Scaling groups, Amazon Elastic Block Store (Amazon EBS), AWS Lambda functions**
- **AWS X-Ray -** You can use AWS X-Ray to analyze and debug serverless and distributed applications such as those built using a microservices architecture. With X-Ray, you can understand how your application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors.

> ## X-Ray - debug serverless applications

- **Amazon Pinpoint** - Amazon Pinpoint allows marketers and developers to deliver customer-centric engagement experiences by capturing customer usage data to draw real-time insights. Pinpoint cannot be used to debug performance issues for this serverless application built using a microservices architecture.
- **AWS CloudFormation** - AWS CloudFormation allows you to use programming languages or a simple text file to model and provision, in an automated and secure manner, all the resources needed for your applications across all Regions and accounts. Think infrastructure as code; think CloudFormation. CloudFormation cannot be used to debug performance issues for this serverless application built using a microservices architecture.
- **AWS Storage Gateway** is a **hybrid cloud storage service** that connects your existing on-premises environments with the AWS Cloud. **Gateway types** supported by AWS Storage Gateway are: **Tape, File & Volume Gateway**
- **AWS Local Zones** - latency, **AWS Wavelength** - 5G,
- **AWS Edge Locations** - An AWS Edge location is a site that CloudFront uses to cache copies of the content for faster delivery to users at any location.

- **AWS Lambda** - AWS Lambda lets you run code without provisioning or managing servers. You pay for compute time.
- **Amazon RedShift** - Online analytical Processing
- **Amazon EventBridge** - Amazon EventBridge is a service that provides real-time access to changes in data in AWS services, your own applications, and software as a service (SaaS) applications without writing code.
- **AWS Glue** - AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics.
- **Amazon RDS RR** primarily enhances DB scalability, **RDS RR multi-AZ** enhances DB high availability, **RDS RR multi-region** enhances disaster recovery & local performance. **RR** generally increases DB costs



Read replicas, Multi-AZ deployments, and multi-region deployments

Amazon RDS read replicas complement Multi-AZ deployments. While both features maintain a second copy of your data, there are differences between the two:

Multi-AZ deployments	Multi-Region deployments	Read replicas
Main purpose is high availability	Main purpose is disaster recovery and local performance	Main purpose is scalability
Non-Aurora: synchronous replication; Aurora: asynchronous replication	Asynchronous replication	Asynchronous replication
Non-Aurora: only the primary instance is active; Aurora: all instances are active	All regions are accessible and can be used for reads	All read replicas are accessible and can be used for readscaling
Non-Aurora: automated backups are taken from standby; Aurora: automated backups are taken from shared storage layer	Automated backups can be taken in each region	No backups configured by default
Always span at least two Availability Zones within a single region	Each region can have a Multi-AZ deployment	Can be within an Availability Zone, Cross-AZ, or Cross-Region
Non-Aurora: database engine version upgrades happen on primary; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent in each region; Aurora: all instances are updated together	Non-Aurora: database engine version upgrade is independent from source instance; Aurora: all instances are updated together
Automatic failover to standby (non-Aurora) or read replica (Aurora) when a problem is detected	Aurora allows promotion of a secondary region to be the master	Can be manually promoted to a standalone database instance (non-Aurora) or to be the primary instance (Aurora)

- **DynamoDB** - NoSQL, Schemaless/flexible schema DB and least operational overhead, its non-relational. **RedShift, RDS, & Aurora** are schema-based DB. **Amazon RDS** is **less operationally efficient** than **Amazon DynamoDB** while building a highly scalable solution.

> **DynamoDB & Amazon S3 support VPC Endpoint Gateway for a private connection from a VPC**

> **DynamoDB global tables replicate data automatically across your choice of AWS Regions and automatically scale capacity to accommodate your workloads** while **DynamoDB Accelerator (DAX) is an in-memory cache that delivers fast read performance for your tables at scale by enabling you to use a fully managed in-memory cache.**

> **In a multi-master cluster, all DB instances have read/write capability.**

> **RDS is a NoSQL DB. Performance of AWS managed RDS instance is better than a customer-managed database instance**

SQL DB	NoSQL DB
Amazon RDS	Amazon DocumentDB
Amazon Aurora	Amazon Neptune

- **Amazon Elastic File System (Amazon EFS) -** Amazon EFS is a **file storage service** for use with Amazon EC2. Amazon EFS provides a file system interface, file system access semantics, and **concurrently-accessible storage for up to thousands of Amazon EC2 instances.** Amazon EFS uses the Network File System protocol. **You will pay a fee each time you read from or write data stored on the Amazon Elastic File System (Amazon EFS) - Infrequent Access storage class. EFS can be used directly with on-premises system.**

> ## DynamoDB & EFS supports high availability by default due to multi-AZ deployment

- **Amazon Elastic Block Store (Amazon EBS)** - Amazon Elastic Block Store (EBS) is an easy to use, high-performance **block storage service** designed **for use with Amazon Elastic Compute Cloud (EC2) & on-premises servers** for both throughput and transaction-intensive workloads at any scale. **EBS volumes cannot be accessed simultaneously by multiple EC2 instances but are bound to several AZs. Amazon EBS Snapshots are stored incrementally, which means you are billed only for the changed blocks stored**
- **Instance Store** - An instance store provides **temporary block-level storage** for your instance. This storage is located on disks that are physically attached to the host computer. **Instance Store volumes cannot be accessed simultaneously by multiple EC2 instances and it is available as hardware disks.**

> ## Instance Store is the only block-level storage capable of caching information .

- **Amazon Elastic Container Service (Amazon ECS) -** Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster. It is of two types: **EC2 Launch type (Not serverless) & Fargate Launch type (Serverless)**.
- **AWS Fargate** - AWS Fargate is a serverless compute engine for containers. It works with both Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS)
- **Amazon Elastic Container Registry (Amazon ECR)** - Amazon Elastic Container Registry (Amazon ECR) can be used to store, manage, and deploy Docker container images.
- **AWS DataSync -** AWS DataSync is a secure online data transfer service that simplifies, automates, and accelerates copying terabytes of data to

and from AWS storage services.

- **AWS CodeArtifact - r**epository service that helps in maintaining application dependencies via integration with commonly used package managers and build tools
- **AWS CodeDeploy -** AWS CodeDeploy is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises.
- **AWS CodeCommit** - AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories.
- **AWS CodePipeline** - AWS CodePipeline is a continuous delivery service that enables you to model, visualize, and automate the steps required to release your software.
- **AWS Elastic Load Balancing (ELB)** automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses; **its benefits include high availability, fault tolerance**; its types are **Classic Load Balancer, Network Load Balancer & Application Load Balancer** which distributes traffic and does not scale resources while **Amazon EC2 Auto Scaling** helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application (scaling) automatically & it is cost-effective.
- **Horizontal scaling (elasticity)** operation refers to an increase in capacity by adding more computers to the system e.g. ELB (Auto Scaling Group) & Amazon RDS RR while **vertical scaling** operation implies adding more resources (like CPU, RAM) to a single node or machine e.g. Resizing an instance of EC2.
- **Amazon FSx -** for Windows File Server provides fully managed, highly reliable, and scalable file storage that is accessible over the industry-standard Service Message Block (SMB) protocol and built on Windows Server WHILE **Amazon FSx for Lustre** - For compute-intensive and fast processing workloads, like high-performance computing (HPC), machine learning, EDA, and media processing, it provides a file system that’s optimized for performance, with input and output stored on Amazon S3. Amazon FSx for Lustre is only compatible with Linux.

- **Amazon Transcribe**: Convert speech to text
- **Amazon Polly**: Convey text results via speech
- **Amazon Macie: Identify sensitive data**
- **Amazon Kendra** - Patents
- **AWS Batch** - AWS Batch enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS.
- **AWS OpsWorks -** AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet.
- **AWS Software Development Kit (SDK) -** You can also access via AWS SDK that provides **language-specific abstracted APIs** for AWS services.
- **Amazon MQ -** Amazon MQ is a managed message broker service for Apache ActiveMQ and RabbitMQ that makes it easy to set up and operate message brokers on AWS. M**essage broker service for moving on-premises application to AWS Cloud.**
- **Amazon Simple Queue Service (Amazon SQS)** - Amazon Simple Queue Service (Amazon SQS) offers a reliable, highly scalable hosted queue for storing messages as they travel between computers.
- **Amazon Simple Notification Service (Amazon SNS)** - Amazon Simple Notification Service (Amazon SNS) is a fully managed messaging service for both application-to-application (A2A) and application-to-person (A2P) communication. Can also be used to decouple microservices, distributed systems, and serverless applications.

> **SQS & SNS can be used to decouple components of a micro services based application on AWS cloud.**

- **Amazon Kinesis Data Streams** - Amazon Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs.

- **AWS Step Function** - AWS Step Function lets you coordinate multiple AWS services into serverless workflows. It doesn´t provision resources.
- **AWS Batch** - Runs batch computing workloads by provisioning the compute resources.
- **AWS Global Accelerator provides static IP addresses that act as a fixed entry point to your applications & is a good fit for non-HTTP use cases**
- **Amazon Quicksight -** Amazon QuickSight is a scalable, serverless, embeddable, machine learning-powered business intelligence (BI) service built for the cloud.
- **Amazon Elastic Transcoder -** Amazon Elastic Transcoder lets you convert media files that you have stored in Amazon Simple Storage Service (Amazon S3) into media files in the formats required by consumer playback devices.
- AWS CodeStar is a cloud-based development service (IDE) that provides the tools you need to quickly develop, build, and deploy applications on AWS.
- **Each AWS CodeStar project includes development tools, including AWS CodePipeline, AWS CodeCommit, AWS CodeBuild, and AWS CodeDeploy, that can be used on their own and with existing AWS applications**
- **AWS CodePipeline uses Amazon CloudWatch Events to detect changes in CodeCommit repositories used as a source for a pipeline**
- **You can use AWS CodeStar and AWS Cloud9 to develop, build, and deploy a serverless web application**

▼ Security & Compliance

- **AWS Acceptable Use Policy -** The Acceptable Use Policy describes prohibited uses of the web services offered by Amazon Web Services, Inc. and its affiliates (the “Services”) and the website located at http://aws.amazon.com (the “AWS Site”). This policy is present at https://aws.amazon.com/aup/ and is updated on a need basis by AWS
- **AWS Health - Your Account Health Dashboard:** AWS Health - Your Account Health Dashboard provides alerts and remediation guidance when

AWS is experiencing events that may impact you.

- **AWS Health Dashboard - Service Health:** The AWS Health Dashboard – Service health is the single place to learn about the availability and operations of AWS services.
- **IAM access advisor review permissions granted to an IAM user**
- **AWS CloudTrail -** Monitor AWS account activity & event history meets the governance, compliance and auditing norms.

> Think account-specific activity and audit; think CloudTrail.

- **AWS Config** - AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.

> Think resource-specific change history, audit, and compliance; think Config.

- **Amazon CloudWatch** - Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. This is an excellent service for building Resilient systems. It can be used to centralize the server logs for its Amazon Elastic Compute Cloud (Amazon EC2) instances and on-premises servers.

> Think resource performance monitoring, events, and alerts; think CloudWatch.

- **AWS CloudTrail Insights - identify and respond to unusual activity associated with write API calls by continuously analyzing CloudTrail management events.**

- **Amazon Inspector** - Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on your Amazon EC2 instances.

Service	**Purpose**	**Keyword**
GuardDuty	Threat detection	**Security threats**
Inspector	Vulnerability management	**Vulnerabilities**
Systems Manager	Operational task automation	**Manage resources**
CloudWatch	Monitoring and observability	**Metrics & alarms**
CloudTrail	Activity logs and auditing	**Who did what?**
Trusted Advisor	Optimization recommendations	**Best practices**
X-Ray	Distributed application tracing	**Trace workflows**

- **AWS Systems Manager** gives you visibility and control of your infrastructure on AWS, also, operational insights of your resources to quickly identify any issues that might impact applications using those resources.
- **Security Group -** Firewall at **instance level, NACL -** Firewall at **subnet level**
- **CloudHSM** - Hardware keys, **AWS KMS** - Create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications.
- MFA devices:

1. **Virtual Multi-Factor Authentication (MFA) device -** A software app that runs on a phone or other device and emulates a physical device.
2. **U2F security key** - A device that you plug into a USB port on your computer.
3. **Hardware Multi-Factor Authentication (MFA) device** - A hardware device that generates a six-digit numeric code based upon a time-synchronized

one-time password algorithm.

- **Penetration Testing -** AWS customers can carry out security assessments or penetration tests against their AWS infrastructure without prior approval for few common AWS services.
- **Network Stress Testing** - AWS considers "network stress test" to be when a test sends a large volume of legitimate or test traffic to a specific intended target application. The endpoint and infrastructure are expected to be able to handle this traffic.
- **AWS Shield** - Automatically protects against DDoS. **AWS Shield Advanced is not automatically deployed & provides expanded DDoS attack protection (on Layer 3, 4,& 7) for web applications running on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, Amazon Route 53 & AWS Global Accelerator**

> **AWS Shield Standard is shared responsibility of AWS & customers**

- **AWS WAF** - a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor (count) web requests based on conditions that you define. Protects against **Layer 7 (application level), SQL injection and cross-site scripting** and DDoS using rate-based rules. It can be deployed on **Amazon CloudFront, Application Load Balancer, Amazon API Gateway, AWS AppSync**

> **Layer 3** - Network layer, **Layer 4** - Transport layer

- **AWS IAM Identity Center -** AWS Single Sign-On (AWS SSO). It is built on top of AWS Identity and Access Management (IAM) to simplify access management to multiple AWS accounts, AWS applications, and other SAML-enabled cloud applications.
- **AWS Cognito** - Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.

- **S3 Access Logs can be used audit requests made to an Amazon Simple Storage Service (Amazon S3) bucket**
- Amazon Detective sources are **AWS CloudTrail logs, Amazon VPC Flow Logs, and Amazon GuardDuty findings**
- Security group control the incoming traffic to an Amazon EC2 instance
- **NACL** acts as a firewall for controlling traffic in and out of one or more subnets.
- **Route Table** contains a set of rules, called routes, that are used to determine where network traffic from your VPC is directed.