**EC2 instance types**

1. **General purpose instance** provides **balance of compute , memory and networking** resources . **use case** is **application servers, gaming or small and medium data base .** basically where you do not need to optimise in any single resource .
2. **Compute optimized instances**  basically for applications **requires high computing power** . **used case** for **high-performance web servers**, compute-intensive applications servers, and **dedicated gaming servers.**
3. **memory optimized instances** are good for **memory-intensive tasks**. Its designed to deliver  **fast performance on large datasets** in memory. **Use case** when workload requires to **preload application before running** and requires perform **real-time processing large unstructured data.**
4. **Accelerated computing instances** use **hardware accelerators, or coprocessors perform** functions very efficiently in running software. Basically **hardwear speeds up data processing**. **Use case graphics applications, game streaming, and application streaming.**
5. **Storage optimized instances** are designed for workloads that **require high, sequential read and write** access to large datasets on **local storage**. It can perform tens of thousands **low latency** random **input/output operations per second (IOPS).** **Use case** file distribution system , **data warehousing applications**, and **high-frequency online transaction processing** (OLTP) systems. Basically where low latency IOPS demand is high .

**EC2 instance pricing**

1. **On-Demand Instances** are ideal for **short-term, irregular workloads** that **cannot be interrupted**. **No upfront costs** or minimum contracts apply. The instances run continuously until you stop them, and **you pay for only the compute time you use.** **Use case** testing applications , or for unpredictable usage patterns. Definitely not for long term use .
2. **Amazon EC2 Savings Plans** can get Up to **72% discount** If you commit to **1 or 3years term commitment.** **Use case** basically when demand is predictable. when you know how much you going to use.
3. **Reserved Instances** Cheaper than on-demand instance. offer you up to a **75% discount versus On-Demand pricing.**  can purchase **standard and convertible reserved** instances for **1 or 3 year term**. You get **more discount** if you **pay all upfront** And get least amount of Discount when you don't pay anything upfront. **Use case** when demand is predictable.
4. **Spot on instance** Offers **highest amount of discounts** . **Discounts up to 90%.** AWS allows you to request **spare capacity instance** basically when the availability Zone have spear Computing capacity. but the catch is AWS can **terminate instance Any time** . **use case** For workloads that tolerate interruptions.
5. **Dedicated Hosts** These are basically **physical host .** When **the whole physical server is dedicated to your needs.** It is the **most expensive** option. **Use case** to comply with **regulatory requirements** of the company. For example Healthcare data, Financial transactions And sensitive information.

**Auto scaling vs. elastic load balancing**

**Auto-scaling i**s **adding or terminating EC2** instances Based on the demand.

**Elastic Load Balancing** is the AWS service that automatically **distributes incoming application traffic** across multiple resources, such as Amazon EC2 instances.

**How do they work together?**

Elastic load balancer distribute traffic all across instances. Based on their computing power means if the instance is running at near maximum capacity(computing power) The auto scale will add instances . Works the same way when instances runs at low capacity, it terminate EC2 instances . Elastic Load Balancing and Amazon EC2 Auto Scaling are separate services, they work together to help ensure that applications running in Amazon EC2 can provide high performance and availability**.**

**simple notification service (SNS)vs Service Queue service (SQS)**

SNS service Publishers **messages to subscribers** of the applications. For example when a company sends the coupons to customers .

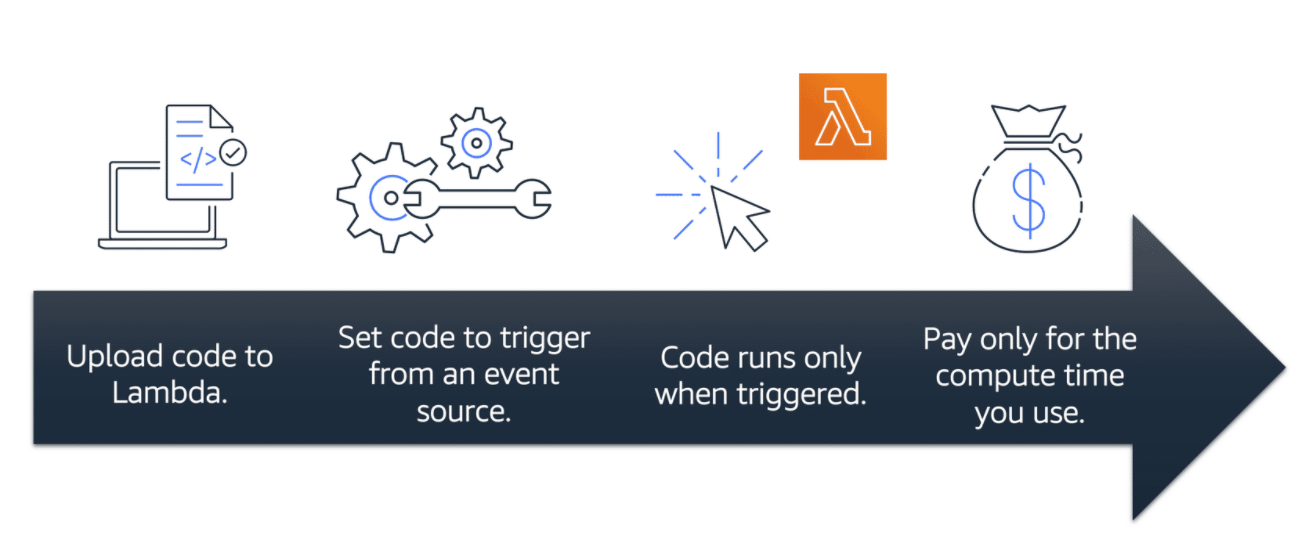
SQS service **Helps application A communicate with application B**.It can send, store and receive data or message from one application to another. For example when cashier at coffee shop post orders on screen for Coffee maker to see the orders in back kitchen . (This kind of setting also called Loosely coupled service.) If applications communicating without SQS Service With one another it'll called Tightly coupled service. (By the way Loosely couple Services good There is no communication message is lost if one application goes down)

**Serverless computing**

The term **“serverless”** means that your code runs on servers, but you do not need to provision or manage these servers. With serverless computing, you can focus more on innovating new products and features instead of maintaining servers.

**Types of Serverless computing**

* **AWS Lambda** is a service that lets you **run code without needing to provision or manage servers.** Lambda's a service that allows you to **upload your code** into what's called **a Lambda function.** 1 or 1000 requests AWS will scale to meet demands. Designed to **run code under 15 mins** .



## **This is background for AWS ECS and EKS**

* [**Containers**](https://www.youtube.com/watch?v=-LeV_c1zG-s&t=231s) provide you with a standard way to package your application's code and dependencies into a single object. You can also use containers for processes and workflows in which there are essential requirements for security, reliability, and scalability. **In simple language a container is a package for your code where you package up your application, its dependencies as well as any configurations that it needs to run.**
* **AWS Elastic Container service (ECS)**is a highly scalable, high-performance **container management system** that enables you to run and scale containerized applications on AWS. **supports Docker containers.** Its open source. You can built and test application. AWS **supports open-source Docker Community Edition and subscription-based Docker Enterprise Edition.**
* **Amazon Elastic Kubernetes Service (Amazon EKS)** is a fully managed service that you can use to run Kubernetes on AWS. **Kubernetes** is open-**source software** that enables you to deploy and manage containerized applications at scale.
* [**AWS Fargate**](https://aws.amazon.com/fargate/)is a **serverless compute engine for containers**. **It works with both Amazon ECS and Amazon EKS.Although you can run both( ECS and EKS** **) applications on ec2 instances but you can use AWS fargate to fully manage ECS or EKS** . **AWS Fargate managers servers for you.** You can focus more on innovating and developing your applications, and **you pay only for the resources that are required to run your containers.**

# **AWS global infrastructure**

**AWS Region**

**How to determine what is the right region for you?**

**F**irst check the compliance for the **data governance and legal requirements**. Secondly check but **distance to your customer.** Third step is to **check available services** in that region because not all services are available in all regions. At last check **pricing.**

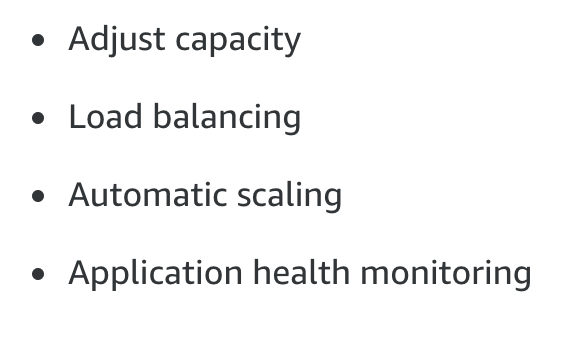
**Availability Zones**

Each region have **multiple availability zones** at **least three.**There are tens of miles apart but still close enough to have single-digit millisecond latency.The best practice is run your application into at least two availability zones.

# **Edge locations**

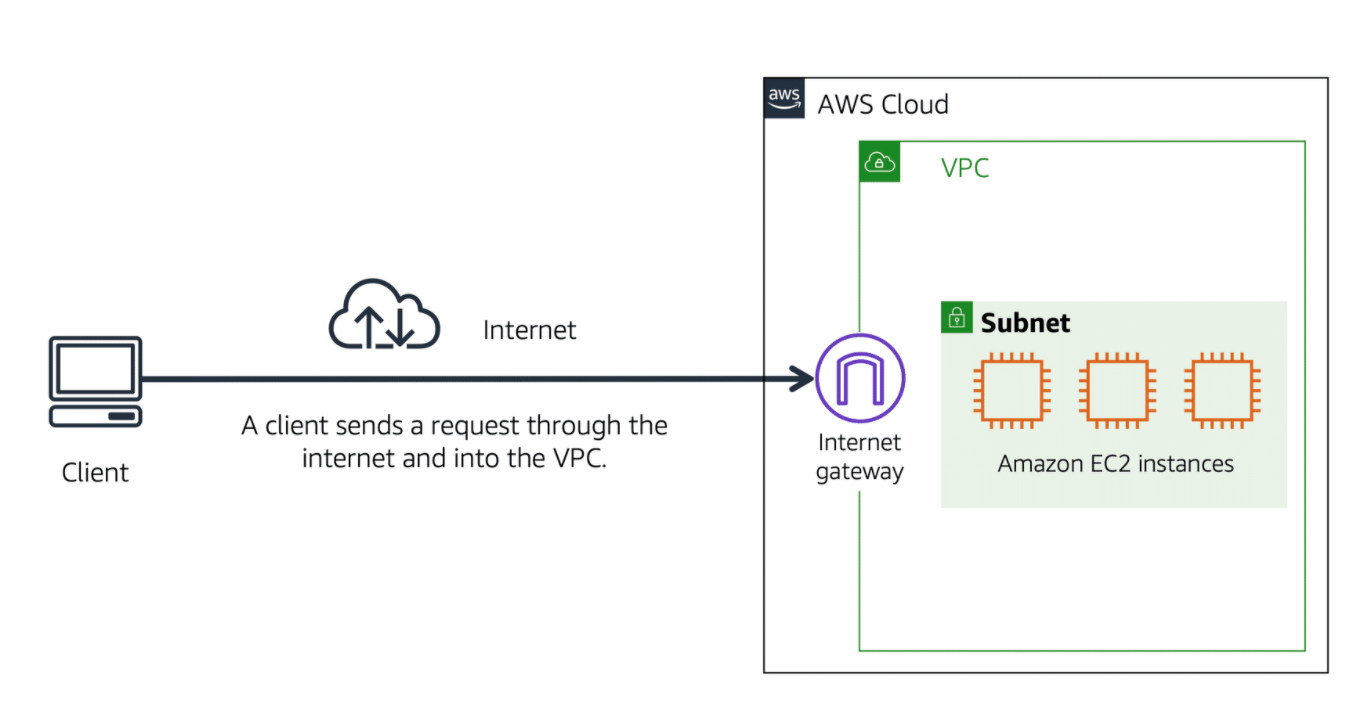
An **edge location** is a site that **Amazon CloudFront** uses to **store cached** copies of your content closer to your customers for faster delivery.

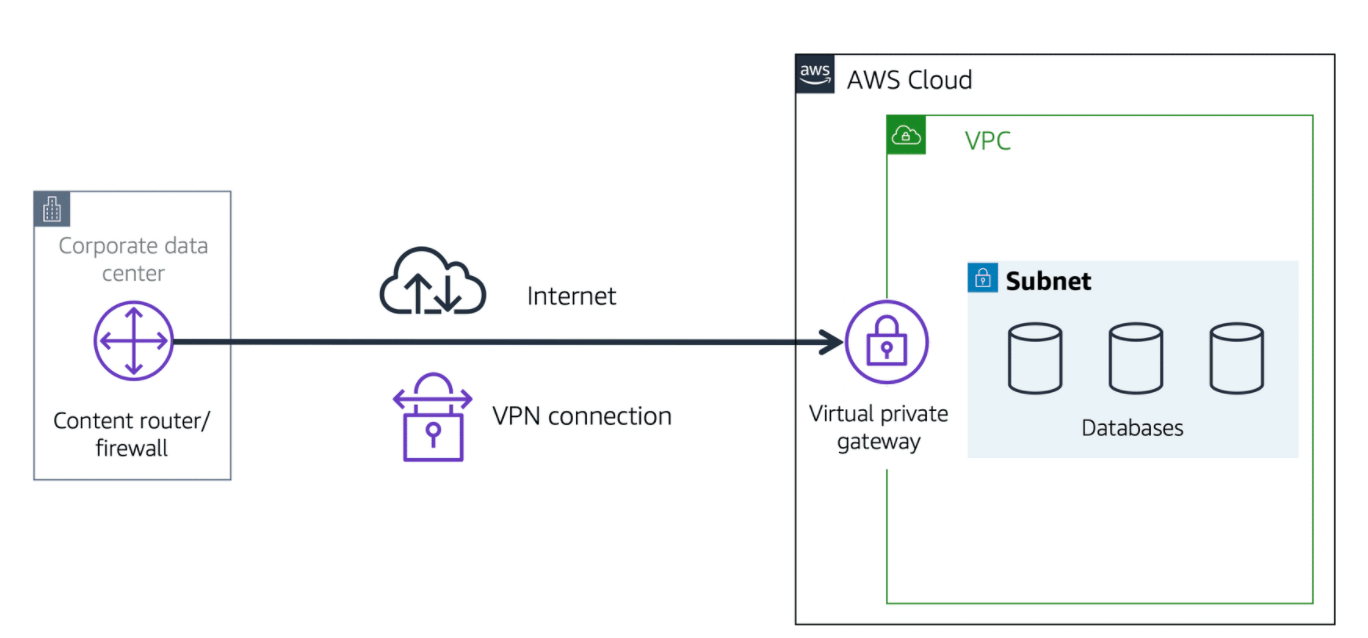
**Ways to interact with AWS services**

* The **AWS Management Console** is a **web-based interface** for accessing and managing AWS services. The console includes **wizards and automated workflows** that can simplify the process of completing tasks.
* **AWS Command Line Interface (AWS CLI)** enables you to **control multiple AWS services directly** from the command line within one tool. AWS CLI is available for users on **Windows, macOS, and Linux. AWS CLI Helps you to automate** action that your service and applications performed through Scripts.For example, you can use commands to launch an Amazon EC2 instance, connect an Amazon EC2 instance to a specific Auto Scaling group, and more.
* **software development kits (SDKs)** enable you to use AWS services with your existing applications or create entirely new applications that will run on AWS**.** To help you get started with using SDKs, AWS provides documentation and **sample code for each supported programming language**. Supported **programming languages include C++, Java, .NET, and more.**
* **AWS Elastic Beanstalk is a managed service.** you **provide code and configuration settings,** and Elastic Beanstalk deploys the resources necessary to perform the following tasks:
* **AWS CloudFormation** treat your **infrastructure as code**. AWS cloud formations help you **built environment by writing lines of code** Instead of using AWS Management console to individually provision resources. AWS CloudFormation provisions your resources in a safe, repeatable manner, enabling you to frequently build your infrastructure and applications without having to perform manual actions or write custom scripts.

# 

# **Connectivity to AWS**

* [**Amazon Virtual Private Cloud (Amazon VPC)**](https://aws.amazon.com/vpc/) Is a service that allows you to **create a boundary around your AWS resources**. Amazon VPC enables you to provision **an isolated section of the AWS Cloud**. In VPC you can launch resources Which you Define and also Organize them into **subnets**. **A subnet is a section of a VPC that can contain resources such as Amazon EC2 instances.**
* **internet gateway** Allows public traffic from internet to access VPC. An internet gateway is a connection between a VPC and the internet.
* To access private resources in a VPC, you can use a **virtual private gateway**. The virtual private gateway is the component that allows protected internet traffic to enter into the VPC. **A virtual private gateway enables you to establish a virtual private network (VPN) connection between your VPC and a private network,** such as an on-premises data center or internal corporate network.

****

* [**AWS Direct Connect**](https://aws.amazon.com/directconnect/) **is a service that enables you to establish a dedicated private connection between your data center and a VPC.**

# **Subnets and network access control lists**

**Types of subnet**

* **Public subnets** contain resources that need to be accessible by the public, such as an online store’s website.
* **Private subnets** contain resources that should be accessible only through your private network, such as a database that contains customers’ personal information and order histories.

## **Network traffic in a VPC**

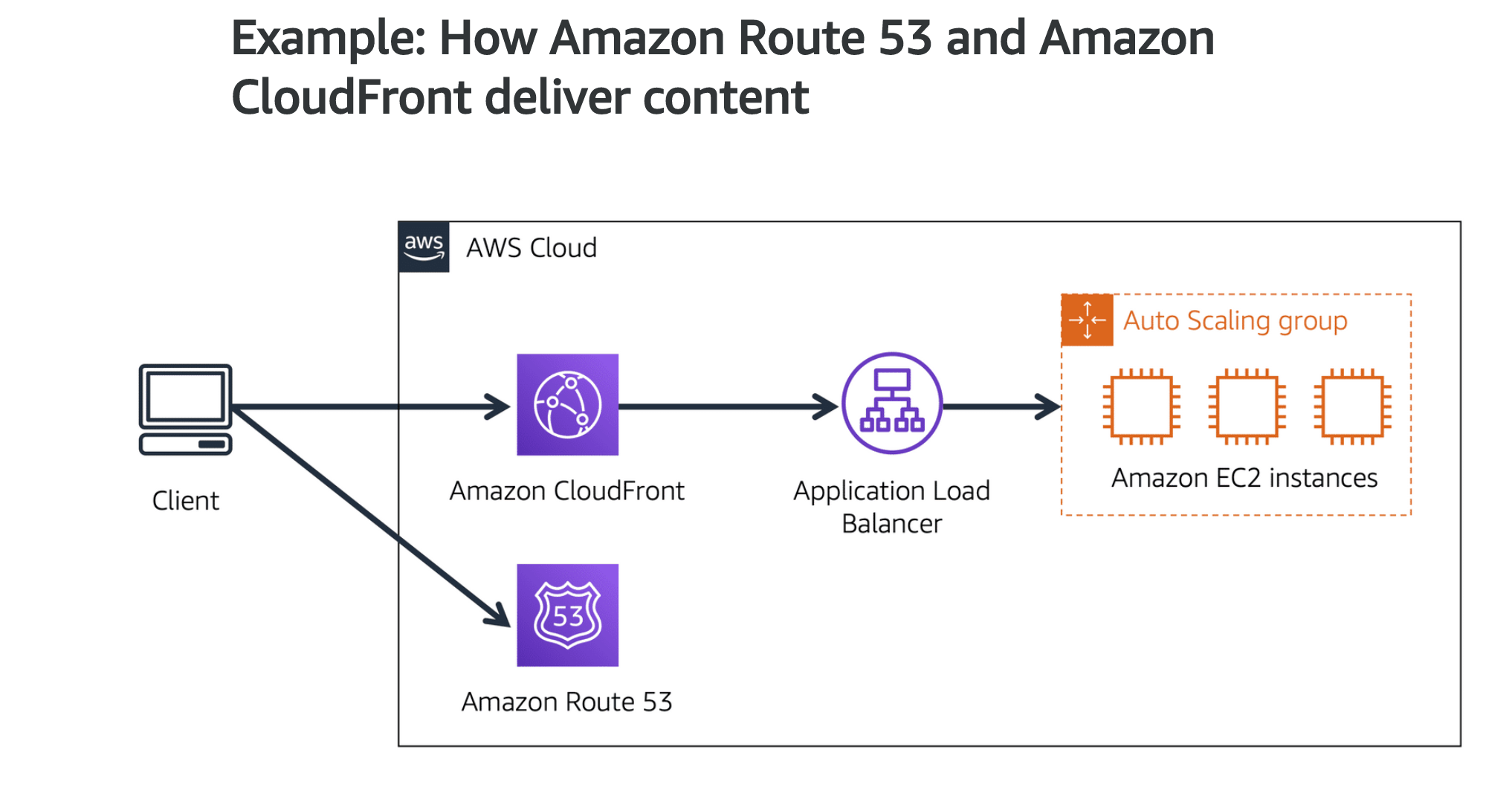
When a customer requests data from an application hosted in the AWS Cloud, this request is sent **as a packet**. A **packet** is a unit of data sent over the internet or a network.

* **A network access control list (ACL)** is a virtual **firewall that controls** **inbound and outbound traffic** at the **subnet level.** Network ACLs perform **stateless** packet filtering. They remember nothing and check packets that cross the subnet border each way: inbound and outbound. **Each AWS account includes a default network ACL. When configuring your VPC, you can use your account’s default network ACL or create custom network ACLs.**
* **A security group** is a virtual firewall that controls **inbound and outbound** traffic for an Amazon EC2 instance. Security groups perform **stateful** packet filtering. They remember previous decisions made for incoming packets.

# **Global networking**

**Amazon Route 53**  is a DNS web service. It gives developers and businesses a reliable way to route end users to internet applications hosted in AWS. Amazon Route 53 connects user requests to infrastructure running in AWS (such as Amazon EC2 instances and load balancers). **It can route users to infrastructure outside of AWS.**

Another feature of Route 53 is the **ability to manage the DNS records for domain names**. **You can register new domain names directly in Route 53.** You can also transfer DNS records for existing domain names managed by other domain registrars. This enables you to manage all of your domain names within a single location.



**Instance stores and Amazon Elastic Block Store (Amazon EBS)**

* **An** [**instance store**](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html)provides **temporary block-level storage** for an Amazon EC2 instance. If **ec2 instance is terminated the instance storage is lost.**
* [**Amazon Elastic Block Store (Amazon EBS)**](https://aws.amazon.com/ebs)is a service that **provides block-level storage volumes that you can use with Amazon EC2 instances. I**f **you stop or terminate an Amazon EC2 instance, all the data on the attached EBS volume remains available**.To create an EBS volume, you define the configuration (such as volume size and type) and provision it. After you create an EBS volume, it can attach to an Amazon EC2 instance.
* **An** [**EBS snapshot**](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html)is an **incremental backup.** This means that the first backup taken of a volume copies all the data. For subsequent backups, only the blocks of data that have changed since the most recent snapshot are saved.

# **Amazon Simple Storage Service (Amazon S3)**

* [**Amazon Simple Storage Service (Amazon S3)**](https://aws.amazon.com/s3/) is a service that provides **object-level storage**. Amazon S3 stores data as objects in bucket. You can upload any type of data. **The maximum file size is 5TB**. When you upload a file to Amazon S3, you can set permissions to control visibility and access to it. You can also use the Amazon S3 versioning feature to track changes to your objects over time.

**Amazon S3 storage classes**

1. **S3 standard Design for frequent data access.** Highly reliable **stores data in minimum of three availability zones.** This makes the data Highly available . **The most expensive choice.** Use case websites , contact distribution And data analytics.
2. **S3 Standard-Infrequent Access (S3 Standard-IA)** I**t is ideal for low frequent access** . low Storage price but High retrieval price. **Saves data into at least two availability zone**s Just like standard S3.
3. **S3 One Zone-Infrequent Access (S3 One Zone-IA)** I**t is cheaper than both S3 standard and s3 IA . I**t stores data into one available zone . It is good for saving cost.
4. **S3 Intelligent-Tiering** It is smart way to store data. **if you do not access data for specific time it automatically saves your data into S3 IA .** if you access data s3 IA it moves back to S3 standard.a small monthly monitoring and automation fee per object **.Ideal for data with unknown or changing access pattern.**
5. **S3 Glacier** Low-cost data saving service. Ideal for data archiving.
6. **S3 Glacier Deep Archive** The cheapest option out there. In S3 Glacier you retrieve **data from few minutes to a few hours.** In this data storage **class it takes 12 hours.**

* [**Amazon Elastic File System (Amazon EFS)**](https://aws.amazon.com/efs/) is a s**calable file system used with AWS Cloud s**ervices and on-premises resources. As you add and remove files, **Amazon EFS grows and shrinks automatically. It can scale on demand to petabytes without disrupting applications.**

## **Amazon Relational Database Service**

* [**Amazon Relational Database Service (Amazon RDS)**](https://aws.amazon.com/rds/) is a service that enables you to **run relational databases in the AWS Cloud.**Amazon RDS provides a number of different security options. **Many Amazon RDS database engines offer encryption at rest (protecting data while it is stored) and encryption in transit (protecting data while it is being sent and received).**

Amazon RDS is available on six database engines, which optimize for memory, performance, or input/output (I/O). Supported database engines include:

* Amazon Aurora
* PostgreSQL
* MySQL
* MariaDB
* Oracle Database
* Microsoft SQL Server
* [**Amazon Aurora**](https://aws.amazon.com/rds/aurora/) is an **enterprise-class relational database**. It is **compatible with MySQL and PostgreSQL** relational databases. It is up to **five times faster than standard MySQL** databases and up to **three times faster than standard PostgreSQL** databases**.It replicates six copies of your data across three Availability Zones and continuously backs up your data to Amazon S3.**

**Nonrelational databases**

## 

* [**Amazon DynamoDB**](https://aws.amazon.com/dynamodb/) **is a key-value database service. It delivers single-digit millisecond performance at any scale.**

## 

## 

## **Amazon Redshift**

[**Amazon Redshift**](https://aws.amazon.com/redshift) **is a data warehousing service that you can use for big data analytics.** It offers the **ability to collect data from many sources** and **helps you to understand relationships and trends across your data.**

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

[**AWS Database Migration Service (AWS DMS)**](https://aws.amazon.com/dms/) **enables you to migrate relational databases, nonrelational databases, and other types of data stores . With AWS DMS, you move data between a source database and a target database.** [**The source and target databases**](https://aws.amazon.com/dms/resources) **can be of the same type or different types. During the migration, your source database remains operational, reducing downtime for any applications that rely on the database.**

# 

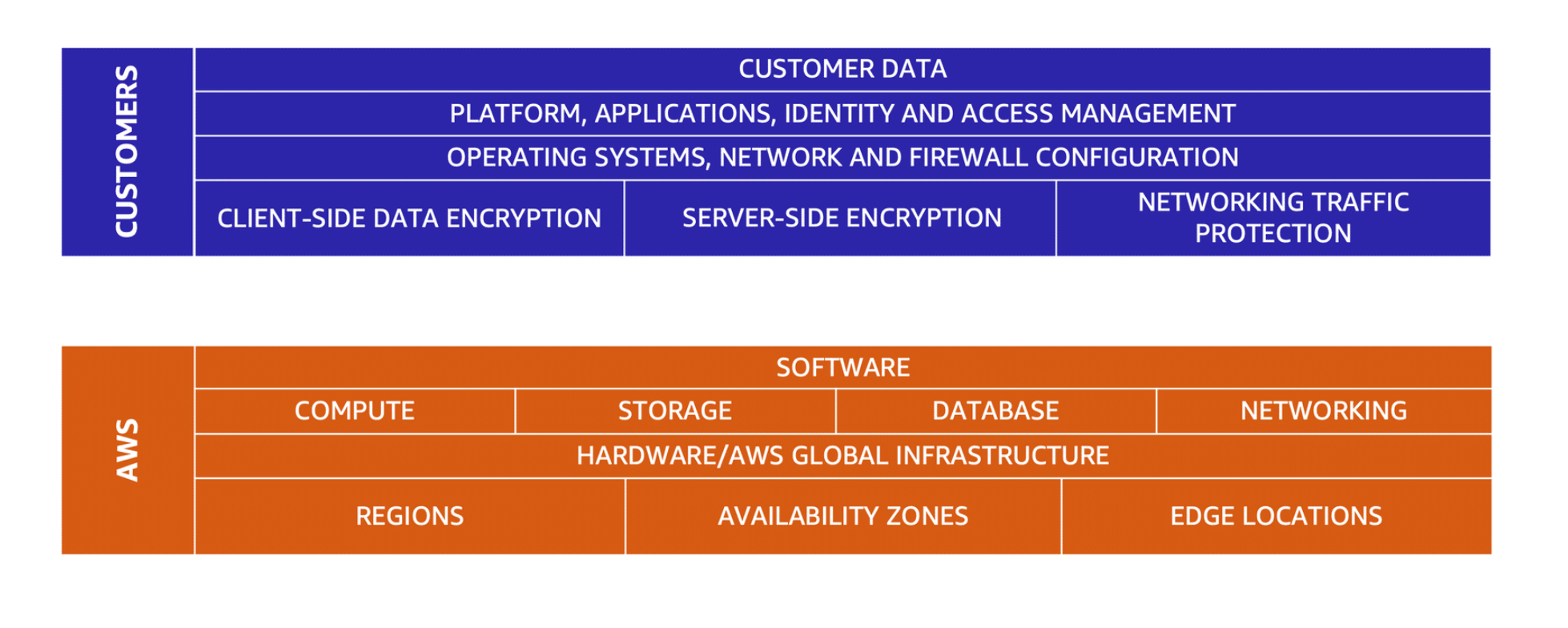
# 

# **Additional database services**

* [**Amazon DocumentDB**](https://aws.amazon.com/documentdb) is a **document database** service that supports MongoDB workloads. (MongoDB is a document database program.)
* [**Amazon Neptune**](https://aws.amazon.com/neptune) is a **graph database service.** You can use Amazon Neptune to build and run applications that work with highly connected datasets, such as recommendation **engines, fraud detection, and knowledge graphs.**
* [**Amazon Quantum Ledger Database (Amazon QLDB)**](https://aws.amazon.com/qldb) is a ledger database service. You can use Amazon QLDB to review a complete history of all the changes that have been made to your application data.
* [**Amazon Managed Blockchain**](https://aws.amazon.com/managed-blockchain) is a service that you can use to create and **manage blockchain networks with open-source frameworks. Amazon Managed Blockchain** is a service that you can use to create and manage blockchain networks with open-source frameworks. Blockchain is a distributed ledger system that lets multiple parties run transactions and share data without a central authority.
* [**Amazon ElastiCache**](https://aws.amazon.com/elasticache) is a service that **adds caching layers o**n top of your databases to help improve the read times of common requests. It supports two types of data stores: Redis and Memcached.
* [**Amazon DynamoDB Accelerator (DAX)**](https://aws.amazon.com/dynamodb/dax/) is an **in-memory cache for DynamoDB.**

It helps improve response times from single-digit milliseconds to microseconds.

**Shared responsibility model**

****

**The shared responsibility model divides into customer responsibilities (commonly referred to as “security in the cloud”) and AWS responsibilities (commonly referred to as “security of the cloud”).**

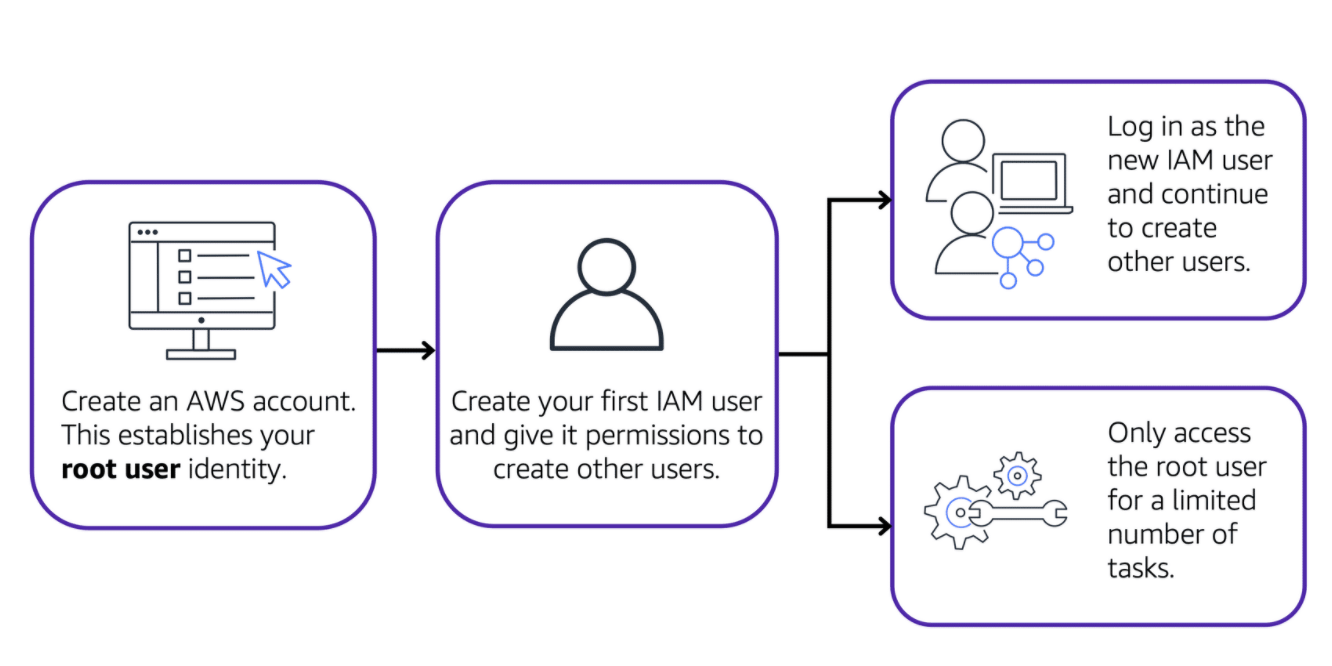
**Customers: Security in the cloud**

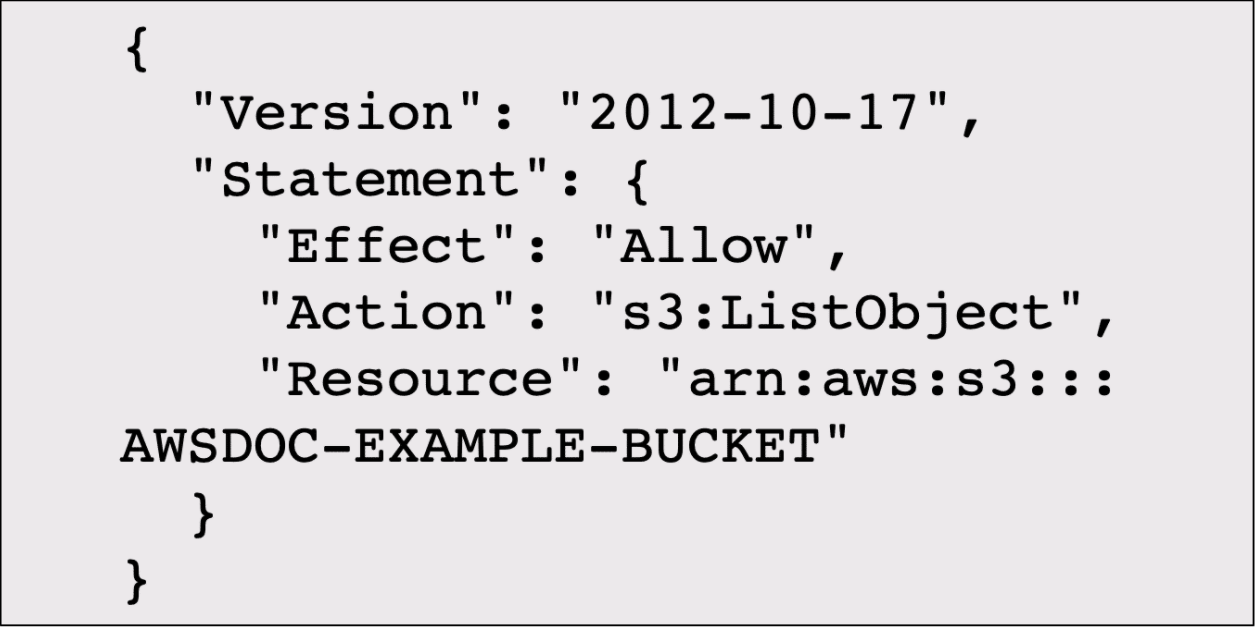
You are responsible for managing security requirements for your content, including which content you choose to store on AWS, which AWS services **you use, and who has access to that content. You also control how access rights are granted, managed, and revoked.**

**AWS: Security of the cloud**

AWS is responsible for **security *of* the cloud**.**Physical security of data centers,Hardware and software infrastructure,Network infrastructure, Virtualization infrastructure.** AWS is responsible for **protecting the global infrastructure t**hat runs all of the services offered in the AWS Cloud**.**

# **User permissions and access**

* [**AWS Identity and Access Management (IAM)**](https://aws.amazon.com/iam/)enables you to **manage access to AWS services and resources securely**. IAM gives you **the flexibility to configure access based on your company’s specific operational and security needs**. You do this by using a combination of IAM features, which are explored in detail in this lesson:
* **IAM users, groups, and roles**
* **IAM policies**
* **Multi-factor authentication**
* **AWS account root user** is accessed by **signing in with the email address and password that you used to create your** AWS account. Best practice **Do not use the root user for everyday tasks.** Instead, use the root user to create your first IAM user and assign it permissions to create other users.
* **IAM user** is an identity that you create in AWS. It **represents the person or application that interacts with AWS services and resources**. It consists of a name and credentials.**By default, when you create a new IAM user in AWS, it has no permissions associated with it. you must grant the IAM user the necessary permissions.** to perform specific actions in AWS, such as launching an Amazon EC2 instance or creating an Amazon S3 bucket**. Best practice** We recommend that **you create individual IAM users for each person who needs to access AWS.** Even if you have multiple employees who require the same level of access, you should create individual IAM users for each of them. **This provides additional security by allowing each IAM user to have a unique set of security credentials.**
* **IAM policy** is a **document that allows or denies permissions to AWS services and resources. I**AM policies enable you to **customize users’ levels of access to resources. Best practice** Follow the security principle of **least privilege when granting permissions.** This prevent users or rolls having more permissions than needed to perform their tasks.For example, if an employee needs access to only a specific bucket, specify the bucket in the IAM policy. Do this instead of granting the employee access to all of the buckets in your AWS account.



In this example, the IAM policy is allowing a specific action within Amazon S3: ListObject. The policy also mentions a specific bucket ID: AWSDOC-EXAMPLE-BUCKET.

* **IAM group** is a collection of IAM users. When you assign an IAM policy to a group, all users in the group are granted permissions specified by the policy.Assigning IAM policies a**t the group level also makes it easier to adjust permissions when an employee transfers to a different job.**
* **An IAM role** is an **identity that you can assume to gain temporary access to permissions.** When **someone assumes an IAM role, they abandon all previous permissions that they had under a previous role a**nd assume the permissions of the new role. **Best prAprilactice The best use case is when service resource need to be granted temporary and start of long-term.**
* [**multi-factor authentication**](https://aws.amazon.com/iam/features/mfa/)Automated generated number by a security app such as Google MFA. multi-factor authentication (MFA) provides an **extra layer of security for your AWS account.**

**AWS Organizations**

**AWS organizations to consolidate and manage multiple accounts the organisation from a central location**.centrally control permissions for the accounts in your organization by using [**service control policies (SCPs)**](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html). **SCPs enable** you to **place restrictions on the AWS services, resources, and individual API actions that users and roles in each account can access.**

## 

## 

## 

## **Organizational units**

## 

**AWS Organizations,** you can group accounts into **organizational units (OUs) to make it easier to manage accounts with similar business or security requirements.** apply a **policy to an OU, all the accounts in the OU automatically inherit the permissions specified in the policy.**

# **Compliance**

[**AWS Artifact**](https://aws.amazon.com/artifact)is a service that **provides on-demand access to AWS security and compliance reports and select online agreements.** AWS Artifact consists of two main sections: AWS Artifact Agreements and AWS Artifact Reports.

* **AWS Artifact Agreements** allows you to  **review, accept, and manage agreements for an individual account and for all your accounts in AWS Organizations.**Different types of agreements are offered to address the needs of customers who are subject to specific regulations
* **AWS Artifact Reports** provide c**ompliance reports from third-party auditors. T**hese auditors have tested and verified that AWS is compliant with a variety of global, regional, and industry-specific security standards and regulations. A**WS Artifact Reports remains up to date with the latest reports released.** You can provide the AWS audit artifacts to your auditors or regulators as evidence of AWS security controls.
* **The** [**Customer Compliance Center**](https://aws.amazon.com/compliance/customer-center/)contains resources to help you learn more about AWS compliance. It provides **customer compliance stories to discover how companies in regulated industries have solved various compliance, governance, and audit challenges.** the Customer Compliance Center includes an auditor learning path. This learning path is designed for individuals in auditing, compliance, and legal roles who want to learn more about how their internal operations can demonstrate compliance using the AWS Cloud.

**Denial-of-service attacks**

**A denial-of-service (DoS) attack is a deliberate attempt to make a website or application unavailable to users.**For example, an attacker might flood a website or application with excessive network traffic until the targeted website or application becomes overloaded and is no longer able to respond. If the website or application becomes unavailable, this denies service to users who are trying to make legitimate requests.

## 

## 

## 

## **Distributed denial-of-service attacks**

## 

In a distributed **denial-of-service (DDoS) attack,** **multiple sources are used to start an attack** that aims to make a website or application unavailable

## **AWS Shield**

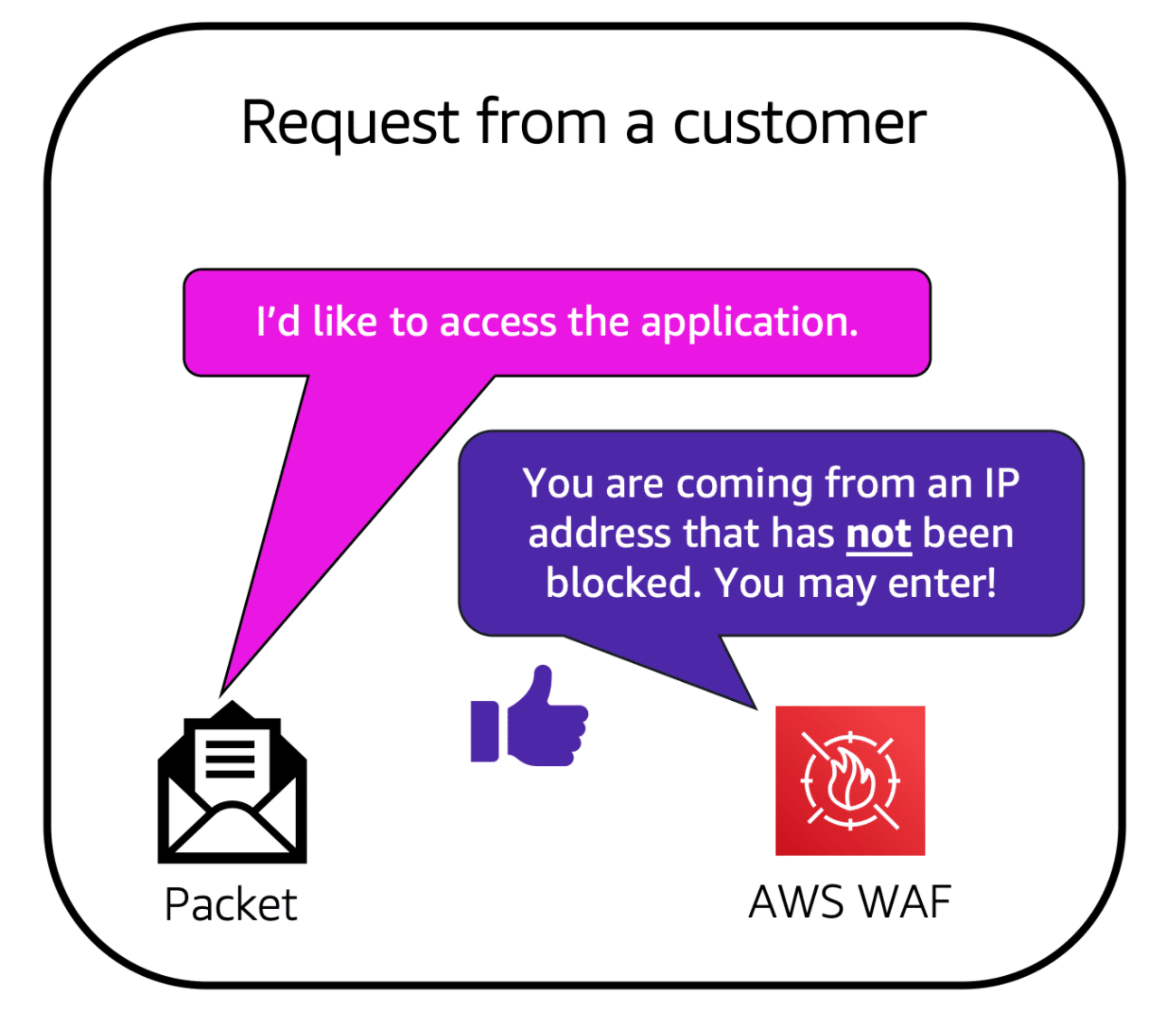
## 

**AWS Shield** is a service tha**t protects applications against DDoS attacks.AWS Shield provides two levels of protection: Standard and Advanced.**

* **AWS Shield Standard automatically protects all AWS customers at no cost. I**t protects your AWS resources from the most common, **frequently occurring types of DDoS attacks.** AWS Shield Standard uses a variety of analysis techniques to detect malicious traffic in real time and automatically mitigates i**t.**
* **AWS Shield Advanced** is a **paid service** that provides detailed attack diagnostics and the **ability to detect and mitigate sophisticated DDoS attacks.** It also **integrates with other services** such as A**mazon CloudFront, Amazon Route 53, and Elastic Load Balancing.** integrate **AWS Shield with AWS WAF** by **writing custom rules to mitigate complex DDoS attacks.**

# **Additional security services**

* [**AWS Key Management Service (AWS KMS)**](https://aws.amazon.com/kms)enables you to perform encryption operations through the use of **cryptographic keys**. **A cryptographic key is a random string of digits used for locking (encrypting) and unlocking (decrypting) data.** in any AWS service data is encrypted at rest and as well as transfers .
* [**AWS WAF**](https://aws.amazon.com/waf) is a **web application firewall** that lets you **monitor network requests that come into your web applications.** **AWS WAF works together with Amazon CloudFront and an Application Load Balancer. It the ip address of the incoming package and if it is on the list .**

****

* [**Amazon Inspector**](https://aws.amazon.com/inspector/)**.** helps to **improve the security and compliance of applications by running automated security assessments.** It checks applications for **security vulnerabilities and deviations from security best practices,** such as open access to Amazon EC2 instances and installations of vulnerable software versions. it provides you with a **list of security findings.** The list prioritizes by severity level, including a detailed description of each security issue and a **recommendation for how to fix it. AWS does not guarantee t**hat following the provided recommendations **resolves every potential security issue.**
* [**Amazon GuardDuty**](https://aws.amazon.com/guardduty) is a service that **provides intelligent threat detection for your AWS infrastructure and resources**.It identifies threats by continuously **monitoring the network activity and account behavior within your AWS environment**.it continuously **analyzes data from multiple AWS sources, including VPC Flow Logs and DNS logs.** If it finds threats it recommends next steps. You can a**lso attach lambda functions to automate response.**

# **Amazon CloudWatch**

[**Amazon CloudWatch**](https://aws.amazon.com/cloudwatch/) **i**s a web service that enables you to **monitor and manage various metrics and configure alarm actions based on data from those metrics.** CloudWatch then uses these **metrics to create graphs automatically that show how performance has changed over time.**

* **CloudWatch alarms** you can create[**alarms**](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html) **that automatically perform actions** if the value of your metric has **gone above or below a predefined threshold.**
* **CloudWatch** [**dashboard**](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html)feature enables you to access **all the metrics for your resources from a single location**. CloudWatch dashboard to **monitor the CPU utilization of an Amazon EC2 instance, the total number of requests made to an Amazon S3 bucket, and more.**

# **AWS CloudTrail**

[**AWS CloudTrail**](https://aws.amazon.com/cloudtrail/) **records** API calls for your account. CloudTrail, you can view a c**omplete history of user activity and API calls** for your applications and resources. The recorded **information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, and more.** typically **updated in CloudTrail within 15 minutes** after an API call. [**CloudTrail Insights**](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-insights-events-with-cloudtrail.html) **optional feature allows CloudTrail to automatically detect unusual API activities in your AWS account.**

# **AWS Trusted Advisor**

[**AWS Trusted Advisor**](https://aws.amazon.com/premiumsupport/technology/trusted-advisor/)is a web service that **inspects your AWS environment and provides real-time recommendations** in accordance with **AWS best practices.**findings to AW**S best practices in five categories**: **cost optimization, performance, security, fault tolerance, and service limits.**

****

**AWS Free Tier**

**The** [**AWS Free Tier**](https://aws.amazon.com/free/) **enables** you to begin using **certain services without having to worry about incurring costs for the specified period.**

* **Always Free** These offers do not expire and are available to all AWS customers. For example, **AWS Lambda allows 1 million free requests and up to 3.2 million seconds of compute time per month. Amazon DynamoDB allows 25 GB of free storage per month.**
* **12 month Free** These offers are **free for 12 months** following your initial sign-up date to AWS.Examples include specific **amounts of Amazon S3 Standard Storage, thresholds for monthly hours of Amazon EC2 compute time, and amounts of Amazon CloudFront data transfer out.**
* **TriaLs Short-term free trial offers** start from the date you activate a particular service.For example, **Amazon Inspector offers a 90-day free trial**. Amazon Lightsail (a service that enables you to run virtual private servers) offers 750 free hours of usage over a 30-day period.

**How AWS pricing w**orks

* **Pay for what you use.** you **pay for exactly the amount of resources** that you actually use, without requiring long-term contracts or complex licensing.
* **Pay less when you reserve .** Some services offer reservation options that provide a significant discount compared to On-Demand Instance pricing.
* **Pay less with volume-based discounts when you use more.** Some services offer tiered pricing, so **the per-unit cost is incrementally lower with increased usa**ge.

**AWS Pricing Calculator**

[**AWS Pricing Calculator**](https://calculator.aws/#/) **l**ets you **explore AWS services and create an estimate** for the cost of your use cases on AWS. You can **organize your AWS estimates by groups** that you define. A group can reflect how your company is organized, such as providing estimates by cost center.

## **AWS pricing examples**

## 

* **AWS Lambda** allows **1 million free requests** and up to **3.2 million seconds of compute time per month.** You can **save on AWS Lambda** costs by **signing up for a Compute Savings Plan.** A **Compute Savings Plan** offers lower compute costs in exchange for **committing to a consistent amount of usage over a 1-year or 3-year term. T**his is an example **of paying less when you reserve. You can see pricing by region**
* **Amazon EC2** pay for **only the compute time that you use while your instances are running**. some workloads, you ca**n significantly reduce Amazon EC2 costs by using Spot Instances**
* **Amazon S3 pricing, consider the following cost components:**
  + **Storage -** You **pay for only the storage that you use.** You are c**harged the rate to store objects** in your Amazon S3 buckets based on your **objects’ sizes, storage classes, and duration.**
  + **Requests and data retrievals** - You pay for requests made to your Amazon S3 objects and buckets.
  + **Data transfer** There is **no cost to transfer data between different Amazon S3 buckets or from Amazon S3 to other services within the same AWS Region. you pay for data that you transfer into and out of Amazon S3, . There is no cost for data transferred into Amazon S3 from the internet or out to Amazon CloudFront. There is also no cost for data transferred out to an** Amazon EC2 instance in the same AWS Region as the Amazon S3 bucket.
  + **Management and replication** pay for the **storage management features .** features include Amazon S3 **inventory, analytics, and object tagging.**

[**AWS Billing & Cost Management dashboard**](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html)

* **Compare your current month-to-date balance with the previous month, and get a forecast of the next month based on current usage.**
* **View month-to-date spend by service.**
* **View Free Tier usage by service.**
* **Access Cost Explorer and create budgets.**
* **Purchase and manage Savings Plans.**
* **Publish** [**AWS Cost and Usage Reports**](https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html)**.**

**Consolidated billing**

**AWS Organizations**, a service that enables you to manage multiple AWS accounts from a central location. AWS Organizations also provides the option for [**consolidated billing**](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/consolidated-billing.html)**. The consolidated billing feature of AWS Organizations enables you to receive a single bill for all AWS accounts in your organization.** The benefit of consolidated billing is the ability to s**hare bulk discount pricing, Savings Plans, and Reserved Instances across the accounts in your organization.**

**AWS Budgets**

**In** [**AWS Budgets**](https://aws.amazon.com/aws-cost-management/aws-budgets)**,** you can create budgets to plan your service usage, service costs, and instance reservations.The information in AWS Budgets updates three times a day. This helps you to accurately determine how close your usage is to your budgeted amounts or to the AWS Free Tier limits.

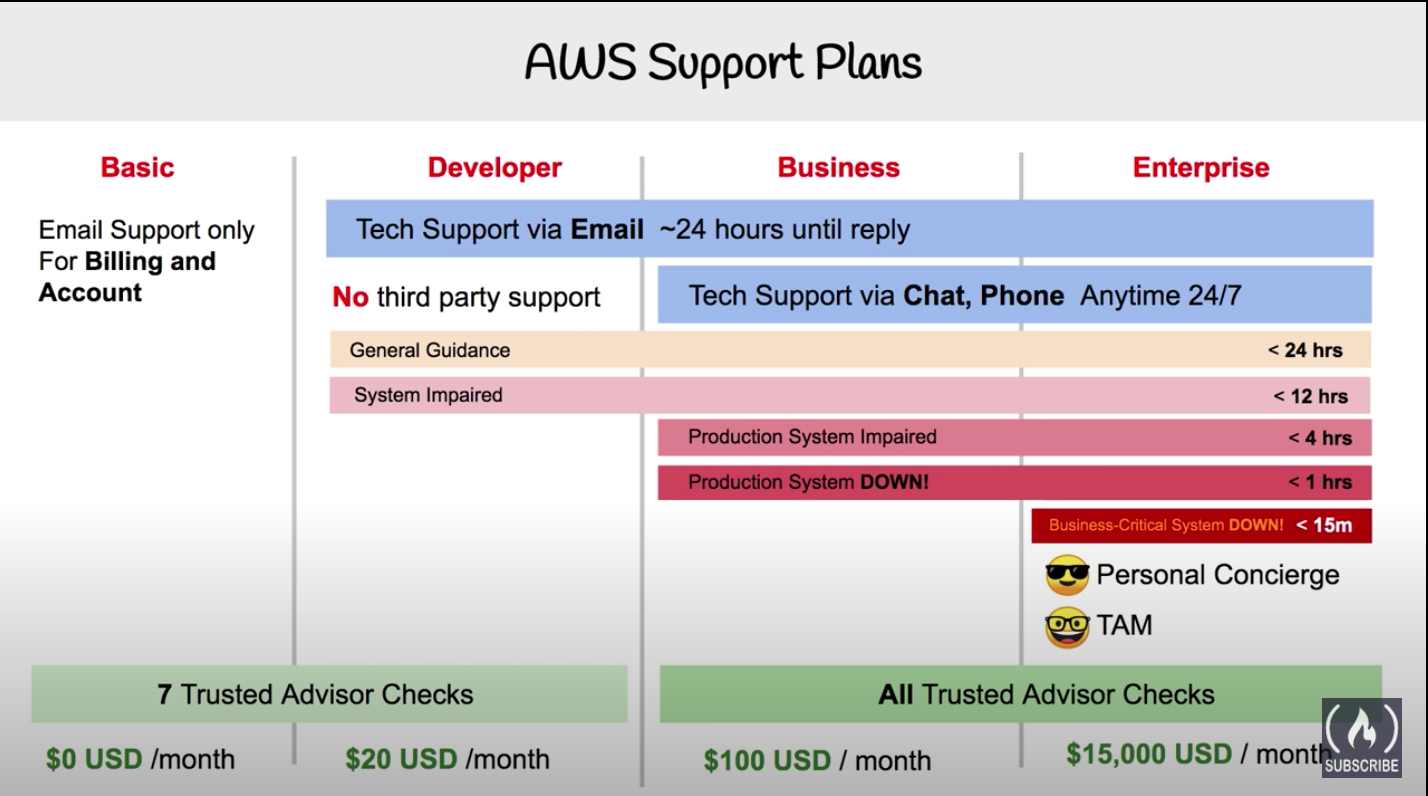
**AWS Cost Explorer**

[**AWS Cost Explorer**](https://aws.amazon.com/aws-cost-management/aws-cost-explorer/) is a tool that enables you to visualize, understand, and manage your AWS costs and usage over time .AWS Cost Explorer includes a default report of the costs and usage for your top five cost-accruing AWS services. You can apply custom filters and groups to analyze your data. For example, you can view resource usage at the hourly level.

**AWS Support**

**AWS offers four different** [**Support plans**](https://aws.amazon.com/premiumsupport/plans/) **to help you troubleshoot issues, lower costs, and efficiently use AWS services.**

* **Basic Support** is free for all AWS customers. Basic Support, you can also **contact AWS for billing questions and service limit increases.** access to a **limited selection of AWS Trusted Advisor checks. AWS Personal Health Dashboard,** a tool that provides alerts and remediation guidance when AWS is experiencing events that may affect you.
* **Developer Support** plan have access to features such as: **Best practice guidance, Client-side diagnostic tools , Building-block architecture support, which consists of guidance for how to use AWS offerings, features, and services together.** the building-block architecture support that is included with the Developer Support plan could help you to identify opportunities for combining specific services and features.
* **Business Support** plan have access to additional features, including: **Use-case guidance** to identify AWS offerings, features, and services that can best support your specific needs, **All AWS Trusted Advisor checks, Limited support for third-party software, such as common operating systems and application stack components**
* **Enterprise Support** plan have access to features such as:
  + Application **architecture guidance**, which is **a consultative relationship to support your company’s specific use cases and applications**
  + **Infrastructure event management:** A short-term engagement with AWS Support that helps your company gain a better understanding of your use cases. This also provides **your company with architectural and scaling guidance.**
  + A Technical Account Manager (TAM)



**AWS Marketplace**

[**AWS Marketplace**](https://aws.amazon.com/marketplace)is a **digital catalog** that includes **thousands of software listings from independent software vendors.** You can use **AWS Marketplace to find, test, and buy software that runs on AWS**.

# **AWS Cloud Adoption Framework (AWS CAF)**

[**AWS Cloud Adoption Framework (AWS CAF)**](https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf) organizes guidance into **six areas of focus**, called **Perspectives**. Each Perspective addresses distinct responsibilities.

* **Business Perspective** ensures **that IT aligns with business needs a**nd that **IT investments link to key business results. with business perspective we can make a strong case to move to Cloud and prioritize Cloud adoption initiatives . Common roles in the Business Perspective include:** 
  + **Business managers**
  + **Finance manager**
  + **Budget owner**
  + **Strategy stakeholde**
* **People Perspective s**upports **development of an organization-wide change management strategy for successful cloud adoption.** In this perspective we have to **evaluate organizational structures, rules, new skills , process requirements and Skill Gap.** Common roles in the People Perspective include:
  + Human resources
  + Staffing
  + **People managers**
* **Governance Perspective** focuses on the **skills and processes to align IT strategy with business strategy.** This ensures that you **maximize the business value and minimize risks.** Governance Perspective to understand how to **update the staff skills** and **processes necessary to ensure business governance in the cloud.** Manage and measure cloud investments to evaluate business outcomes. Common roles in the Governance Perspective include:
  + **Chief Information Officer (CIO)**
  + Program managers
  + Enterprise architects
  + Business analysts
  + Portfolio managers
* **Platform Perspective** includes **principles and patterns for implementing new solutions on the cloud, and migrating on-premises workloads to the cloud**.Use a **variety of architectural models to understand and communicate the structure of IT systems and their relationships.** Common roles in the Platform Perspective include:
  + Chief Technology Officer (CTO)
  + IT managers
  + Solutions architect
* **Security Perspective** ensures t**hat the organization meets security objectives for visibility, auditability, control, and agility. the** AWS CAF to structure the selection and implementation of security controls that meet the organization’s needs.Common roles in the Security Perspective include:
  + Chief Information Security Officer (CISO)
  + IT security managers
  + IT security analysts
* **Operations Perspective** helps you to **enable, run, use, operate, and recover IT workloads to the level agreed upon with your business stakeholders**. Define how **day-to-day, quarter-to-quarter, and year-to-year business is conducted. Align with and support the operations of the business.** The **AWS CAF helps these stakeholders define current operating procedures and identify the process changes and training needed to implement successful cloud adoption.Common roles in the Operations Perspective include:** 
  + **IT operations managers**
  + **IT support managers**

**6 strategies for migration**

* **Rehosting** also known as **“lift-and-shift” i**nvolves **moving applications without changes.**
* **Replatforming,** also known as **“lift, tinker, and shift,**” involves **making a few cloud optimizations to realize a tangible benefit.** Optimization is achieved without changing the core architecture of the application.
* **Refactoring (also known as re-architecting)** involves **reimagining how an application is architected and developed by using cloud-native features.** Refactoring is driven by a strong business need to add features, scale, or performance that would otherwise be difficult to achieve in the application’s existing environment.**writing new code to add features or performance that might not be possible on prem, but now are within your reach.**
* **Repurchasing involves** moving from a traditional license to a software-as-a-service model.
* **Retaining** consists of keeping applications that are critical for the business in the source environment. This might include applications that require major refactoring before they can be migrated, or, work that can be postponed until a later time.
* **Retiring is** the process of removing applications that are no longer needed.

**AWS Snow Family member**

**The** [**AWS Snow Family**](https://aws.amazon.com/snow)is a collection of physical devices that help to physically transport up to exabytes of data into and out of AWS.

* [**AWS Snowcone**](https://aws.amazon.com/snowcone)is **a small, rugged, and secure edge computing and data transfer device.** It features **2 CPUs, 4 GB of memory, and 8 TB** of usable storage.
* [**AWS Snowball**](https://aws.amazon.com/snowball/) offers two types of devices:
  + **Snowball Edge Storage Optimized suited for large-scale data migrations and recurring transfer workflows**, in addition to local computing with higher capacity needs. Storage**: 80 TB of hard disk drive (HDD) capacity** for block volumes and **Amazon S3 compatible object storage, and 1 TB of SATA** solid state drive (SSD) for block volumes.
  + **Snowball Edge Compute Optimize** provides **powerful computing resources for use cases such as machine learning, full motion video analysis, analytics, and local computing stacks. 42-TB usable HDD capacity** for **Amazon S3 compatible object storage** or Amazon EBS compatible block volumes and **7.68 TB of usable NVMe SSD capacity for Amazon EBS compatible block volumes. Compute: 52 vCPUs, 208 GiB of memory, and an optional NVIDIA Tesla V100 GPU.**
* [**AWS Snowmobile**](https://aws.amazon.com/snowmobile) **is an exabyte-scale data transfer service used to move large amounts of data to AWS.Y**ou can **transfer up to 100 petabytes** of data per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi trailer truck.

# **Innovation with AWS**

* **serverless** refers to applications that **don’t require you to provision, maintain, or administer servers.** You don’t need to worry about **fault tolerance or availability.** AWS handles these capabilities for you.
* AWS offers a variety of services powered by **artificial intelligence (AI)**. For example, you can perform the following tasks:
* Convert **speech to text** with **Amazon Transcribe.**
* Discover **patterns in text** with **Amazon Comprehend**.
* Identify potentially fraudulent online activities with Amazon Fraud Detector.
* Build voice and text chatbots with Amazon Lex.

l **machine learning (ML)** development is complex, expensive, time consuming, and error prone. **AWS offers Amazon SageMaker** to remove the difficult work from the process and empower you to build, train, and deploy ML models quickly.

**The AWS Well-Architected Framework**

**The** [**AWS Well-Architected Framework**](https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf) **helps you understand how to design and operate reliable, secure, efficient, and cost-effective systems in the AWS Cloud**

* **Operational excellence** is the ability to **run and monitor systems to deliver business value and to continually improve supporting processes and procedures. Design principles for operational excellence in the cloud include performing operations as code, annotating documentation, anticipating failure, and frequently making small, reversible changes.**
* **Security pillar** is the ability t**o protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.** When considering the security of your architecture, apply these best practices:
* **Automate security** best practices when possible.
* Apply **security at all layers.**
* **Protect data in transit and at rest**.
* **Reliability** is the ability of a system to do the following:
  + **Recover from infrastructure or service disruptions**
  + Dynamicall**y acquire computing resources to meet demand**
  + **Mitigate disruptions such as misconfigurations or transient network issue**s
  + Reliability includes testing **recovery procedures, scaling horizontally to increase aggregate system availability, and automatically recovering from failure.**
* **Cost optimization is the ability to run systems to deliver business value at the lowest price point.**
* **Performance efficiency** is the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.

**Advantages of cloud computing**

* **Trade upfront expense for variable expense.** Upfront expenses include data centers, physical servers, and other resources that you would need to invest in before using computing resources. Instead of investing heavily in data centers and servers before you know how you’re going to use them, you can pay only when you consume computing resources.
* **Benefit from massive economies of scale.**By using cloud computing, you can achieve a lower variable cost than you can get on your own.
* **Stop guessing capacity.** The flexibility of cloud computing makes it easier for you to develop and deploy applications.
* **Increase speed and agility.**
* **Stop spending money running and maintaining data centers. A benefit of cloud computing is the ability to focus less on these tasks and more on your applications and customers.**
* **Go global in minutes.**