# EC2 Elastic Compute Cloud

## Instance Types

* **On Demand** - **Fixed rate**, by the hour/sec with no commitment. When you want low cost and flexibility, best for short term and testing.
* **Reserved** - **1 to 3 years commitment** extreme discount. Different types that give you discounts up to 75%
  + Scheduled - enable you to purchase capacity reservations that recur on a daily/weekly/monthly basis. For stuff that runs on a schedule
  + Partial upfront and no upfront will result in you paying a discounted hourly rate throughout the duration of the term.
* **Spot** - server auto spins up and shuts off based on price, like stock market, applications that are only feasible at very low compute prices.  (bitcoin mining?) Ifrecover quickly from hardware failures spot is the best pricing
* **Dedicated Hosts** - Physical EC2 server dedicated for your use. For regulatory and licensing that require dedicated server, stupid oracle.

## Other EC2 Info

**There are no startup or termination fees associated with Amazon EC2.**

Convertible RIs provide a discount (up to 54% off On-Demand) and the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value. These attributes include instance family, instance type, platform, scope, and tenancy.

EC2 uses IaaS

**Highest level of control over the underlying virtual infrastructure.**

 Security Groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

EC2 instances will be billed on one second increments, with a minimum of one minute

EFS can connect to multiple EC2 instances EBS just one instance.

Customer Should regularly patch the Operating system (OS) and applications on your EC2 instances FOR SECURITY

EC2 and Lambda are compute services.

Security Groups (virtual firewall to control inbound and outbound traffic) & Network Access Control (acts as firewall to control traffic) list protect your EC2 instances from DDos attacks.

EC2 instance pricing varies depending on many variables:

- The buying option (On-demand, Reserved, Spot, Dedicated)

- Selected AMI

- Selected instance type

- Region

- Data Transfer in/out

- Storage capacity.

## AMI (Amazon Machine Image)

* **A template that contains a software configuration** (for example, an operating system, an application server, and applications). This pre-configured template save time and avoid errors when configuring settings to create new instances.
* Saves ec2 configurations

Infrastructure as a service (**Iaas**) - T**he basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Example (EC2)**

Platform as a service (Paas) - **removes the need for your organization to manage the underlying infrastructure (usually hardware and operating systems) and allows you to focus on the deployment and management of your applications. Example (Lambda)**

## Software as a Service (Saas) - provides you with a completed product that is run and managed by the service provider. **Example (Google Docs)**

**A screenshot of a cell phone

Description automatically generated**

# Amazon CloudFront

* a fast content delivery network (CDN) service that **securely delivers data, videos, applications, and APIs to customers globally**
* To **deliver content to global end users with lower latency, Amazon CloudFront uses a global network of Edge Locations and Regional Edge** Caches in multiple cities around the world.
* **ensures that end-user requests are served by the closest edge location**
* Uses edge locations to cache content
* The use cases of Amazon CloudFront include:

1- **Accelerate static website content delivery.**

2- **Live & on-demand video streaming.**

 3- **Security: CloudFront integrates seamlessly with AWS Shield for Layer 3/4 DDoS mitigation and AWS WAF for Layer 7 protection.**

* Cost estimated by the number of HTTP requests, data transfer out, the edge location where content is served.

# Dynamo DB

**DynamoDB** is serverless **managed service** with no servers to provision, patch, or manage and no software to install, maintain, or operate. DynamoDB automatically scales tables up and down to adjust for capacity and maintain performance. Availability and fault tolerance are built in, eliminating the need to architect your applications for these capabilities.

* Amazon DynamoDB is a fast and flexible **NoSQL database service**
* **Multi-AZ fault tolerance in mind**
* **Offers extremely low (single digit millisecond) latency.**
* **Automatically scales**
* **DAX – a fully managed, highly available, in-memory cache for DynamoDB that delivers performance improvements from milliseconds to microseconds**
* **Global Tables - a fully managed solution for deploying a multiregion, multi-master database, without having to build and maintain your own replication solution. With global tables you can specify the AWS Regions where you want the table to be available.**

# Relational Database Service (RDS)

Managed SQL database service.

Amazon Relational Database Service (Amazon RDS) **makes it easy to set up, operate, and scale a relational (SQL) database in the cloud**. It provides cost-efficient, resizable capacity while automating time-consuming administration tasks such as hardware provisioning, operating system maintenance, database setup, patching and backups. **It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.**

## Features that can be used to improve the availability of your database:

* Read replicas (provide enhanced performance and durability for database (DB) instances. This feature makes it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.)
* Multi-AZ deployment – provide enhanced availability and durability for RDS database (DB) instances, making them a natural fit for production database workloads.
* AWS sets up the database and manages the operating system

## Types of RDS DBs

* Aurora – THE ONLY **SERVERLESS** SQL DB. a **MySQL and PostgreSQL-compatible**[**relational database**](https://aws.amazon.com/relational-database/) built for the cloud. Amazon Aurora is designed to be compatible with MySQL and with PostgreSQL, so that existing applications and tools can run without requiring modification.
* Oracle
* MySQL
* MicrosoftSQLServer
* PostGres
* MariaDB

# Other DB Information

## AWS Database Migration Service

**Helps you migrate databases to AWS quickly and securely.** The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database. THIS WILL BE THE ANSWER IF NEEDING TO MIGRATE A DB THAT MUST STILL BE ACTIVE.

**Choose a database**

* Based on the number of reads and writes per second
* The nature of queries

**Amazon Athena**

* An interactive query service that makes it easy to **allows you to query S3 using SQL.**

**Aws Redshift**

* a fully managed, petabyte-scale data **warehouse service** in the cloud.
* allows you to run complex analytic queries against petabytes of structured data.

# AWS Simple Storage Service (S3)

Amazon S3 is **object** storage built to store and retrieve **any amount of data** from anywhere.It is designed to **deliver 99.999999999% durability**, and stores data for millions of applications used by market leaders in every industry.

Tiers/Storage Classes - **S3 classes are rated by Availability & Durability**

* **S3 Standard** – General purpose storage
* **S3 Intelligent-Tiering storage –** Use for **unpredictable** access patterns. Is designed to **optimize costs** by automatically **moving data to the most cost-effective access tier**, without performance impact or operational overhead
* **Infrequent Access** – Use when files are not accessed often but when they are, need to be accessed quickly.
* **Glacier** – Use for archives. 3-5 hours for access. Amazon S3 Glacier and S3 Glacier Deep Archive are a secure, durable, **and extremely low-cost** Amazon S3 cloud storage classes for data archiving and long-term backup. Super compressed zip file

## Other Information

* Stores any number of objects
* Each object does have **a size limitation**. **0 bytes** to **5 TB**.
* **Amazon S3 Transfer Acceleration** enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket.
* Multi-AZ fault tolerance in mind automatically.
* ]alongside IAM policies to protect resources from unauthorized access and to prevent information disclosure, data integrity compromise or deletion.
* **Versioning**: Amazon S3 supports object versions. Versioning is disabled by default. Enable versioning to store a new version for every modified or deleted object from which you can restore compromised objects if necessary.
* **Replication**: Amazon S3 replicates each object across all Availability Zones within the respective region. Replication can provide data and service availability in the case of system failure but provides no protection against accidental deletion or data integrity compromise – it replicates changes across all Availability Zones where it stores copies.
* **Backup**: You can use application-level technologies to manually back up data stored in Amazon S3 to other AWS regions or to on-premises backup systems.
* **AVAILIABILITY AND DURABILITY**
* **Encryption**
  + **Server Side**: Amazon S3 supports server-side encryption of user data**. Server-side encryption is transparent to the end user**. AWS generates a unique encryption key for each object, and then encrypts the object using AES-256.
  + **Client side**: With client-side encryption **you create and manage your own encryption keys**. Keys you create are not exported to AWS in clear text. Your applications encrypt data before submitting it to Amazon S3

# S3 Related Services

## Storage Gateway

* **Connects on premise storage to S3**
* Not storage, just a link
* A hybrid cloud storage service that gives you **on-premises** access to **virtually unlimited cloud storage.**
* Include moving tape backups to the cloud, reducing on-premises storage with cloud-backed file shares, providing low latency access to data in AWS for on-premises applications, as well as various migration, archiving, processing, and disaster recovery use cases.
* Helps enterprise extend their on-premises storage to AWS in a cost-effective manner
* Main benefit is it Allows one to integrate on premises IT environments with Cloud Storage.

## AWS Snowball

* Snowball is **a petabyte-scale data transfer**. AWS literally sends you a thing to hook your data up to.

## AWS Snowmobile

* **An Exabyte-scale data transfer** service used to move extremely large amounts of data to AWS. You can transfer up to 100 Petabytes (PB) per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a **semi-trailer truck.**

# EBS (Amazon Elastic Block Store)

* **EBS is block storage** while S3 is object storage. USED WITH EC2!!!!
* Can only be attached to one EC2 instance at a time
* An easy to use, high performance block storage service designed for use with Amazon Elastic Compute Cloud (EC2)
* **Creating snapshots of EBS Volumes can help ensure that you have a backup of your EBS volumes just in case any issues arise.**
* **Snapshots backed up in s3**
* **ENSURE the EBS data is encrypted at rest.**
* **Best** **storage** to migrate a **database with high read to write** activity
* Priced based on the amount of GB you provision each month and the amount of data transferred out.

# Amazon EFS (Elastic File System)

* Provides a simple, scalable, fully managed elastic **NFS file system** for use with AWS Cloud services and on-premises resources.
* Difference from EBS -> Can be attached to multiple EC2 instances at once
* Offers 2 storage classes standard and infrequent

# AWS Identity & Access Management (IAM)

## IAM

* Used for **access control** for all AWS services
* Can be used to deploy the required SSL server certificates.
* AWS CLI and AWS SDK’s can be used by customers to interact with AWS IAM
* Assign permissions to an IAM USER USING IAM POLICY

## IAM Groups, IAM Roles,

* A collection of **IAM users** that are managed as a unit. **Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users.**
* **An IAM role** is an IAM identity that you can create in your account that has specific permissions. IAM roles **allow you to delegate access (for a limited time) to users or services that normally don't have access to your organization's AWS resources.**
* **IAM Users** an entity that you create in AWS to represent the person or application that uses it to directly interact with AWS. A primary use for IAM users is to give people the ability to sign into the AWS Management Console for interactive tasks and to make programmatic requests to AWS services using the API or CLI. **Assign permissions to a user using IAM policy: The policy is a JSON document that consists of:**

1. **Actions: what actions you will allow. Each AWS service has its own set of actions.**
2. **Resources: which resources you allow the action on.**
3. **Effect: what will be the effect when the user requests access—either allow or deny.**
4. **Conditions – which conditions must be present for the policy to take effect. For example, you might allow access only to the specific S3 buckets if the user is connecting from a specific IP range or has used multi-factor authentication at login.**

# Security

## AWS WAF (Web Application Firewall)

* a **web application firewall that helps protect your web applications or APIs against common web exploits** that may affect availability, compromise security or consume excessive resources.
* a managed **Distributed Denial of Service (DDoS**) protection service that safeguards applications running on AWS.
* **Protect your application from sql injections.**

## AWS Artifact

* **Central resource for compliance-related information** that matters to you. It provides on-demand access to AWS’ security and compliance reports and select online agreements.

Amazon Macie **-** a fully managed **data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data** in AWS.

AWS Certificate Manager (ACM) -a service that lets you easily provision, **manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates**

## AWS KMS (Key Management Service)

* a secure and resilient service that **uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys**
* integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.
* Encryption.

## AWS Multi-Factor Authentication (MFA)

* AWS Multi-Factor Authentication (MFA) is a simple best practice that **adds an extra layer of protection on top of using just your username and password to authenticate.**
* U2F Security Key

## AWS Security

* Access keys consist of an access key ID and select access key, which are used to sign programmatic requests to AWS using the CLI or the SDK.
* **Scales quickly with your AWS usage**

## Amazon Inspector

* an automated security assessment service that **helps improve the security and compliance of applications deployed on AWS.**
* automatically **assesses applications for exposure, vulnerabilities, and deviations from best practices.**

AWS Config

* **enables you to assess, audit, and evaluate the configurations of your AWS resources.**

# Containers

## Elastic Container Registry (ECR)

* **Stores** your **containers**
* Amazon ECR is integrated with Amazon Elastic Container Service (Amazon ECS), simplifying your development to production workflow.
* Amazon ECR **hosts your images in a highly available and scalable architecture, allowing you to reliably deploy containers for your applications**.

## Elastic Container Service (ECS)

* A fully managed container orchestration service.
* Used to **run containerized applications** either using Amazon EC2 (server-based) or AWS Fargate (serverless).

# Deployment Services (All Free)

## AWS CloudFormation

Allows you create resources as infrastructure as code (IAC).

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.** You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation **takes care of provisioning and configuring those resources for you.** You don't need to individually create and configure AWS resources and figure out what's dependent on what; AWS CloudFormation handles all that for you.

* Allows customers to create a template that programmatically defines policies and configs of all AWS resources as code and so that the same template can be reused among multiple projects.
* Benefits: Automates the provisioning and updating of your infrastructure in a safe and controlled manner & allows you to model your entire infrastructure in a text file.
* CloudFormation is FREE, you only pay for the resources you create

## AWS Elastic Beanstalk

* In **easy-to-use service for deploying and scaling web applications and services** developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS.
* **Deploy stuff in EC2**
* **A PaaS solution to automate application deployment to EC2.**

## AWS CLI

Can use these commands to interact with AWS resources

AWS SDK  
Boto3, Can use programming languages like python ruby Javascript to interact with AWS resources

## AWS Management Console

The AWS Management Console **allows you to access and manage Amazon Web Services through a simple and intuitive web-based user interface**. You can also use the AWS Console mobile app to quickly view resources on the go.

# Networking Services

## Elastic Load Balancer (ELB)

* Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.
* Elastic Load Balancing offers three types of load balancers:
  1. **Application Load Balancer:**  **Application Load Balancer is best suited for load balancing of HTTP and HTTPS traffic**.
  2. Network Load Balancer: best suited for load balancing of TCP and TLS traffic.
  3. Classic Load Balancer: Weak sauce no one uses anymore

## AWS Direct Connect

* Cloud service solution that makes it easy to establish a dedicated **network connection from your premises to AWS.**
* **Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter,** office, or colocation environment

## AWS Global Accelerator

* A networking service that improves the availability and performance of the applications that you offer to your global users.

## Route 53

* a global service that provides highly available and scalable Domain Name System (DNS) services, domain name registration, and health-checking web services.

# Amazon CloudWatch

* Amazon CloudWatch is a service that **monitors AWS cloud resources and the applications you run on AWS**. **You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.**
* In CloudWatch, you can set up a billing alarm that triggers if your costs exceed a threshold that you set. This CloudWatch alarm can also be configured to trigger an SNS notification to your email address.

## **AWS CloudTrail**

* AWS CloudTrail is **a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account.** With CloudTrail, you can **log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.**

## **AWS Regions**

* Each AWS Region **contains multiple distinct locations, or Availability Zones**. Each Availability Zone is engineered to be independent from failures in other Availability Zones. An Availability Zone is a data center, and in some cases, an Availability Zone consists of multiple data centers. **Availability Zones within a Region provide inexpensive, low-latency network connectivity to other zones in the same Region.** **This allows you to replicate data across data centers in a synchronous manner so that failover can be automated and appear transparent to your users.**
* **To create a backup of your data in another geographical location. You should create a backup in another region.**
* AWS Region is a physical location around the world where AWS cluster data centers.
* Edge locations used in CloudFront for caching.

# Other Services

## Auto Scaling (free)

* the feature that automates the process of adding/removing the server capacity (based on demand). Autoscaling allows you to reduce your costs by automatically turning off resources that aren’t in use. On the other hand, Autoscaling ensures that your application runs effectively by provisioning more server capacity if required.
* May help reduce AWS monthly costs. Enabling Amazon EC2 Auto scaling for all workloads.
* **Cloud9 – IDE**
* **Amazon Athena -** query service used to analyze data in Amazon S3 using standard SQL.
* **AWS Elastic Load Balancer (ELB)** – **Automatically distributes incoming application traffic across multiple targets**, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. **Makes sure only healthy targets are hit**
* **Amazon Rekognition -** Facial recognition software
* **AWS X-Ray -** provides tools you can use to view, filter, and gain insights into that data to identify issues and opportunities for optimization. **Helps improve application performance and Facilitates tracking of user requests to identify application uses.**
* **AWS Application Discovery Service - helps enterprise customers plan migration projects** by gathering information about their on-premises data centers.
* **AWS Organizations - helps you centrally govern your environment** as you grow and scale your workloads on AWS.For billing purposes, the consolidated billing feature of AWS Organizations treats all the accounts in the organization as one account.
* **AWS Systems Manager - gives you visibility and control of your infrastructure on AWS.**
* **AWS Marketplace -** helps you get the visibility you need to gain traction in the market, allowing you more time to focus on your core business
* **Amazon Elasticache** - a web service that makes it easy to **deploy, operate, and scale an in-memory data store or cache in the cloud.** improves the performance of web applications by **allowing you to retrieve information from fast, managed, in-memory data stores**, instead of relying entirely on slower disk-based databases. The primary purpose of an in-memory data store is to provide ultrafast (sub millisecond latency) and inexpensive access to copies of data.
* **AWS Abuse Team -** The AWS Abuse team can assist you when AWS resources are being used to engage in the following types of abusive behavior: Spam, Port Scanning, Denial of Service Attacks, Intrusion attempts, hosting objectionable or copyrighted content, distributing malware
* **AWS Cost & Usage Report -** The AWS Cost & Usage Report is your one-stop shop **for accessing the most detailed information available about your AWS costs and usage.**
* **AWS Cost Explorer - a** **free tool that you can use to view your costs and usage**. You can view data up to the last 13 months, forecast how much you are likely to spend for the next three months, and get recommendations for what Reserved Instances to purchase.
* **Infrastructure Event Management –**Event Management include advertising launches, new product launches, and infrastructure migrations to AWS. **partners with your technical and project resources to gain a deep understanding of your use case and provide architectural and scaling guidance for an event.**
* **Amazon SQS –** messages between software components. Can be used to decouple the components of the application.
* **AWS Shared Controls –** Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. **Includes patch management, configuration management and Awareness and training.**
* **Amazon VPC – networking, allows you to carve out a set of IP addresses for your account.**
* **AWS Personal Health Dashboard - provides alerts and remediation guidance when AWS is experiencing events that may impact you.** Benefits include A personalized view of service health, proactive notifications & detailed troubleshooting guidance.
* **AWS Consolidated Billing -** AWS consolidated billing **enables an organization to consolidate payments for multiple Amazon Web Services (AWS) accounts within a single organization by making a single paying account. Each AWS account gets volume discounts**
* **Amazon Elastic MapReduce (EMR) -**  industry-leading cloud big data platform **for processing vast amounts of data using open source tools** such as [Apache Spark](https://aws.amazon.com/emr/features/spark/), [Apache Hive](https://aws.amazon.com/emr/features/hive/), [Apache HBase](https://aws.amazon.com/emr/features/hbase/), [Apache Flink](https://aws.amazon.com/blogs/big-data/use-apache-flink-on-amazon-emr/), [Apache Hudi](https://aws.amazon.com/emr/features/hudi/), and [Presto](https://aws.amazon.com/emr/features/presto/) fFv. Enables you to analyze large amounts of datasets in a timely manner.
* **AWS QuickStart Reference Deployments - automated reference deployments for key workloads on the AWS Cloud.**and provide AWS CloudFormation templates to automate their deployment.
* **AWS Opswork -** a configuration management service that **provides managed instances of Chef and Puppet**.
* **Amazon SNS (simple Notification service) – messaging to phone. Can send push notifications as well to phones.**
* **Amazon SES (Simple Email Service) – Sending emails**
* **Amazon Cognito – add user sign-up/sign in & can connect other identitiy providers such as (facebook, amazon etc)**
* **AWS TCO (Total Cost of Ownership) Calculator - The number of on-premise virtual machines is required to calculate the potential savings of using AWS vs. on-premises. Cooling & power consumption and Labor and IT costs should be taken into account when doing a TCO analysis.**
* **APN Consulting Partners -** professional services firms that help customers design, architect, build, migrate, and manage their workloads and applications on AWS
* **AWS Professional Services -** global team of experts that can help you realize your desired business outcomes when using the AWS Cloud. We **work together with your team and your chosen member of the AWS Partner Network (APN) to execute your enterprise cloud computing initiatives.**
* **AWS Partners Network - helps companies build, market, and sell their AWS offerings by providing valuable business, technical, and marketing support.**
* **Amazon Pinpoint – Targeted email, SMS, push notifications, and voice messages.**
* **AWS Migration Hub - track the progress of application migrations**
* **AWS Service Catalog Service – organizations manage catalogs of IT services that are approved for use on AWS.**
* **Amazon Simple Workflow Service (SWF) – coordinate work across distributed components.**
* **AWS Simple Monthly Calculator -** easy-to-use online tool that enables you to estimate the monthly cost of AWS services for your use case based on your expected usage. **Ubuntu/linux billed by the second and windows is billed for full hours.**
* **Security Bulletins – Notify customers about security and privacy events pertaining to AWS Services.**
* **(CAF) Cloud Adoption Framework –** help organizations design and travel an accelerated path to successful cloud adoption.
* **AWS Support API -** programmatic access to AWS Support Center features to create, manage, and close support cases, and operationally manage Trusted Advisor check requests and status.
* **AWS Resource Groups -** Resource groups make it easier to manage, monitor, and automate tasks on large numbers of resources at one time.
* **Amazon Connect -** omnichannel cloud contact center that helps companies provide superior customer service at a lower cost.
* **Amazon Elasticsearch Service** is a fully managed service that makes it easy for you to deploy, secure, and run Elasticsearch cost effectively at scale.
* **Amazon Kinesis** makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. / processing big data
* **AWS Fargate** a serverless container
* **AWS CloudHSM** is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

# AWS Important Topics

**TODO**

## The 5 Pillars of the AWS Well-Architected Framework

1- **Operational Excellence:** The operational excellence pillar includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.

2- **Security**: The security pillar includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

3- **Reliability**: The reliability pillar includes the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

4- **Performance Efficiency:** The performance efficiency pillar includes the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve.

5**- Cost Optimization:** The cost optimization pillar includes the ability to avoid or eliminate unneeded cost or sub-optimal resources.

## AWS Shared Responsibility Model

* **Customers should be aware that their responsibilities may vary depending on the AWS services chosen.**  For example, when using Amazon EC2, you are responsible for applying operating system and application security patches regularly. However, such patches are applied automatically when using Amazon RDS.
* **AWS is responsible for the hardware and software that run AWS services.** This includes patching the infrastructure software and configuring infrastructure devices.
* **Customers are responsible for implementing best practices for data encryption, patching guest OS and applications, identifying an access management and network & firewall configurations.**

## Decoupling

* Decoupling refers to components remaining autonomous and unaware of each other as they complete their work for some greater output

## Penetration Testing

* Attempting to hack into your own instances prior to AWS authorization from AWS.

## Global Infrastructure

* built around Regions and Availability Zones (AZs). Each **AWS Region is a separate geographic area.**
* Each AWS Region has multiple, isolated locations known as Availability Zones. Availability Zones in a region are connected with low latency, high throughput, and highly redundant networking.
* CREATE BACKUP IN ANOTHER REGION.
* Global Reach is the AWS characteristic that can help improve your international users’ experience.
* Multiple Availiability zones allows you to build resilient and highly available architectures.
* Edge locations are not used to distribute traffic. Edge Locations are used in conjunction with the Cloudfront service to cache common responses and deliver content to end users with low latency.

## Tagging

* Each tag is a label consisting of a user-defined key and value. Tags can help you manage, identify, organize, search for, and filter resources. You can create tags to categorize resources by purpose, owner, environment, or other criteria.
* Track AWS spending across multiple resources.
* Quickly identify resources that belong to a specific project.

# AWS Best Practices

## Based on the cloud architecture principle of elasticity

* By automatically provisioning the required AWS resources based on changes in demand.

## Reliability of AWS

* Ability to recover quickly from failures
* Automatically provisioning new resources to meet demand

## The Principles of Least Privilege

* You should grant your users only the permissions they need when they need them and nothing more.

## Infrastructure Hosted in AWS(Benefits)

* Increase speed and agility
* All of the physical security and most of the data/network security are taken care of for you.

## Single Point of Failure

* Single points of failure occur **when a single CloudHSM(cloud based hardware security module) device fails in a non-HA configuration, which can result in the permanent loss of keys and data.**
* You can use services like ELB and Amazon Route53 to configure health checks and mask failure by only routing traffic to healthy endpoints.
* Single point of failure is having a backup
* Make sure you collect enough logs and metrics to understand normal system behavior.

## Horizontal and Vertical Scaling

* **Scaling horizontally** takes place through an increase in the number of resources (e.g., adding more hard drives to a storage array or adding more servers to support an application).
* **Scaling vertically takes** place through an increase in the specifications of an individual resource (e.g., upgrading a server with a larger hard drive, adding more memory, or provisioning a faster CPU)

## Greatest Impact on cost

* Compute and Data Transfer out

## Key design principles of the AWS Cloud

* Disposable resources instead of fixed servers
* Loose coupling

## Serverless more Economical

* With the server-based architectures, servers continue to run all the time but with the serverless architectures the code runs only when needed.

# Enterprise vs. Business level Customers

## Enterprise

**Technical Account Manager (TAM)**

* For enterprise-level customers
* provides technical expertise for the full range of AWS services and **obtains a detailed understanding of your use case and technology architecture.**

## AWS Support Concierge

* included as **part of the Enterprise Support plan**, the Support Concierge Team are AWS billing and account experts that specialize in working with **enterprise accounts**. The Concierge team will quickly and **efficiently assist you with your billing and account inquiries, and work with you to help implement billing and account best practices so that you can focus on running your business.**
* Enterprise accounts get concierge free
* Support Concierge service includes:

1. \*\* 24 x7 access to AWS billing and account inquires. (minimum business support)
2. \*\* Guidance and best practices for billing allocation, reporting, consolidation of accounts, and root-level account security.
3. \*\* Access to Enterprise account specialists for payment inquiries, training on specific cost reporting, assistance with service limits, and facilitating bulk purchases.

## Business

* 24 x7 access to AWS billing and account inquires. (minimum business support)
* Access to the infrastructure Event Management (IEM) feature for additional fee.