# Module 1

* What is a client-server model?

⇒


- client = can be a web browser or desktop application that a person interacts with to make request to computer servers.
- server = can be services such as Amazon Elastic Compute Cloud (Amazon EC2)

* What is cloud computing?

⇒ Cloud computing is the on-demand delivery of IT resources over the internet with pay-as-you-go pricing.

- on-demand delivery → AWS has the resources you need

* Deployment models for cloud computing

⇒ 3 models are

(i) Cloud-based deployment:

→ Run all parts of the application in the cloud

→ Migrate existing application to the cloud

→ Design and build new applications in the cloud

(ii) On-Premises Deployment:

→ Deploy resources by using virtualization and resource management tools

→ Increase resource utilization by using application management & virtualization technologies

→ Also known as private cloud deployment.

(iii) Hybrid Deployment:

→ Connect cloud-based resources to on-premise infrastructure.

→ Integrate cloud-based resources with legacy IT app^n.

*) Benefits of cloud computing

I) Trade upfront expense for variable expense

II) Stop spending money to run and maintain data centers

III) Stop guessing capacity

IV) Benefit from massive economies of scale

V) Increase speed and agility

VI) Go global in minutes

# Cloud Computing:

⇒ The practice of using a network of remote servers hosted on the Internet to store, manage & process data, rather than a local server or a personal computer.

⇒ 3 - Deployment model for Cloud Computing

a) Cloud based deployment
b) On-premises deployment
c) Hybrid Deployment

*) Benefits of cloud Computing:

i) Trade upfront expense for variable expense
ii) Stop spending money to run & maintain data centers
iii) Stop guessing capacity
iv) Benefit from massive economies of scale
v) Increase speed & agility
vi) Go global in minutes

---

# M2

## * Amazon Elastic Compute Cloud (Amazon EC2)

⇒ Benefits
- Highly flexible
- cost-effective
- Quick

⇒ Amazon EC2 is a service that lets you run virtual servers in the cloud.

*) How Amazon EC2 works:

i) Launch
ii) Connect
iii) Use

*) Amazon EC2 instance types:

i) General purpose Instances: → Provide a balanced compute, memory & Networking resources

ii) Compute optimized Instances: → For compute-bound appln that benefits from high-performance processors
→ batch processing workloads required many transaction in a single group

iii) Memory optimized Instances: → Deliver fast performance for workload that process large database in m/m

iv) Accelerated computing Instances: → Use hardware accelerators or coprocessors. to perform some functions more efficiently that is possible in software running in CPUs.

v) Storage Optimized Instance: → Designed for workloads that require high, sequential read & write access to large database on local storage.
→ Designed to deliver tens of thousands of low-latency, random IOPS to appln.
→ suitable for distributed file sim, data warehousing & high-frequency OLTP sim.

* Amazon EC2 pricing:

i) On-Demand: → Ideal for short-term, irregular workloads that cannot be interrupted.
→ No upfront costs or minimum contracts apply.
→ you pay for only the compute time you use.

ii) Amazon EC2 Saving plans: → Reduce compute costs by committing to a consistent amount of compute usage for a 1-YEAR or 3-YEAR term.
→ Commitment results in savings of up to 66% over on-demand costs.
↳ up to 72%.

iii) Reserved Instances :→ Billing discount applied to the use of on-demand instance in your ac.

→ At the end of a Reserved instance term, you are charged on-demand rates

iv) Spot Instance :→ Ideal for workloads with flexible start & end times

→ do not require contracts.

→ It uses unused Amazon EC2 computing capacity and offer you cost saving up to 90% off of on-demand price

→ If you make a spot req and Amazon EC2 capacity is available then spot instance lauches, However if unavailable the req is not succesful. unit capacity becomes available.

v) Dedicated Hosts :→ Physical servers with Amazon EC2 instance capacity that is fully dedicated to your use.

→ most expensive

## *) Scaling Amazon EC2 :

- If you wanted the scaling process to happen automatically, → AWS service that provide this functionality for Amazon EC2 instance is Amazon EC2 Auto Scaling

→ 2 Approaches of Amazon EC2

a) Dynamic - Scaling responds to changing demand.

b) Predictive - Scaling automatically schedules the right number of Amazon EC2 instance based on predicted demand.

*) Directing traffic with Elastic Load Balancing :

- Elastic Load Balancing : (ELB)
  - → Regional construct.
  - → Automatically distributes incoming application traffic across multiple resources, such as Amazon EC2

*) Messaging & Queuing :

→ 2 types

i) Amazon Simple Queue Service : (Amazon SQS)

→ Using Amazon SQS, you can send, store & receive msg b/w software components without losing messages or requiring other service to be available

→ It sends msg into a queue.

ii) Amazon Simple Notification Service : (Amazon SNS)

→ public/subscribe service.

→ Using Amazon SNS topics, a publisher publishes messages to subscribers.

→ Amazon SNS, subscribers can be web servers, email addresses, AWS Lambda functions or others.

*) Additional compute services :

#Serverless Computing :

→ Serverless means that your code runs on servers, but you do not need to provision or manage the servers

*) AWS Lambda :

→ serverless computing

→ AWS Lambda is a service that lets you run code without needing to provision or manage servers.

→ You pay only for the compute time that you consume. Charges apply only when your code is running

→ A simple Lambda function might involve automatically resizing uploaded images to the AWS cloud.

Works :
- Upload code to Lambda
- Set code to trigger from an event source.
- Code runs only when triggered
- Pay only for the compute time you use.

*) Containers :

→ Provides a standard way to package your applications code & dependencies into a single object.

→ Security, reliability & scalability.

→ Container Orchestration service help you to deploy, manage & scale your containerized appln.

*) Amazon Elastic Container Service : (Amazon ECS)

→ Amazon ECS is a highly scalable, high performance container management sim that enable you to run & scale containerized appln on AWS.

→ Amazon ECS supports Docker containers.
↳ build, test & deploy appln quickly

→ With Amazon ECS, you can use API calls to launch & stop Docker-enabled appln.

*) Amazon Elastic kubernetes service: Amazon (EKS)

→ Amazon EKS is a fully managed service that you can use to run kubernetes on AWS.

→ Deploy & manage containerized applications at scale.

*) AWS Fargate:

→ AWS Fargate is a serverless compute engine for containers.

→ Works with both Amazon ECS & Amazon EKS.

→ Do not need to provision or manage servers.

→ You pay only for the resources that are required to run your containers.

---

# M3

*) AWS Global Infrastructure:

→ AWS has Data Center in many Region.

→ A data that has at any region like London will not leave that region unless you explicitly with right credentials & permissions request the data be exported.

*) Selecting a Region:

⇒ 4-key business factors

i) Compliance with data governance & legal requirements:

→ Depending on your company & location you might run your data out of specific area.

ii) Proximity to your customers:

→ Selecting a Region that is close to your customers will help you to get content to them faster.

iii) Available services within a Region:

→ Sometimes, the closest Region might not have all features that you want to offer to customers.

→ Amazon Braket → AWS quantum computing platform

iv) Pricing:

→ If pricing is main concern to select a region.

*) Availability Zones: (AZ)

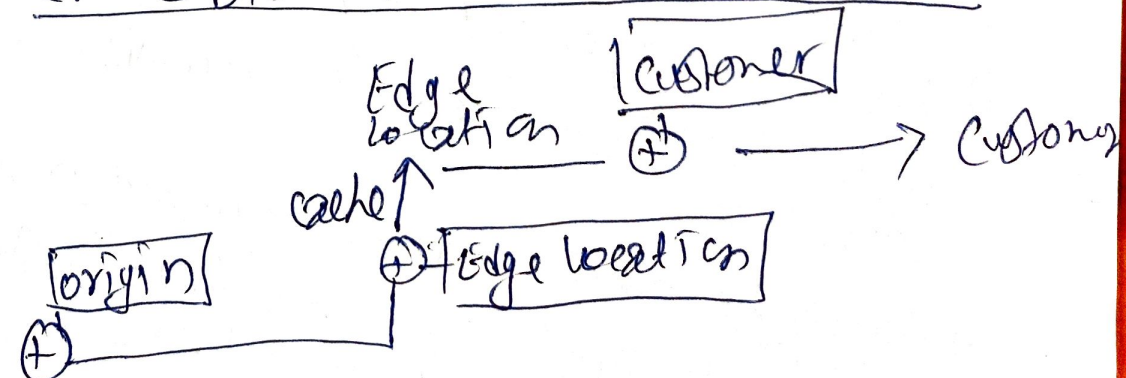
→ Availability Zone is a single data center or a group of data center within a Region.

→ Each Region is made up of multiple data centers.

→ Run across at least 2 Availability zones in a Region

*) Edge locations:

→ Edge location is a site that Amazon CloudFront uses to store cached copied of your content closer to your customers for faster delivery.



→ In AWS CDN called Amazon CloudFront.

↳ Amazon CloudFront helps to deliver data, video applications & APIs to customers around the world with low latency & high transfer speeds.

→ Edge locations are separate from Regions

→ AWS also run DNS. In AWS its called Amazon Route 53 → which helps direct customer to the correct web location with reliable low latency.

→ If your business want to use AWS services inside their own building → Using AWS outposts

AWS Outposts: AWS will install a fully operational mini Region, right inside your own data center.

* How to provision AWS resources:

→ APIs

→ In AWS, everything is an API call

* Ways to interact with AWS service:

i) AWS Management Console:

→ Web-based interface for accessing & managing AWS services.

→ Search by service name, keyword or acronym.

→ AWS Mobile Application to perform tasks such as monitoring resources, viewing alarms & accessing billing information.

ii) AWS Command Line Interface : (AWS CLI)

→ AWS CLI enables you to control multiple AWS services directly from the command line within one tool.

→ You can automate the actions that your services and applications perform through scripts.

iii) Software Development Kits : (SDKs)

→ SDKs allow you to interact with AWS resources through various programming languages.

→ Makes it easy for developers to create programs that use AWS without using the low level APIs.

→ SDKs enable you to use AWS services with your existing appln or create new appln

* Another Way Are : Using managed tools

i) AWS Elastic Beanstalk :

→ With AWS Elastic Beanstalk you provide code & configuration settings, & Elastic Beanstalk deploys the resources necessary to perform;

- Adjust capacity
- load balancing
- Automatic scaling
- Application health monitoring

→ Saves environment configurations, so they can be deploy again easily.

ii) AWS CloudFormation:

→ With AWS CloudFormation, you can treat your infrastructure as code.

This means that you can build an environment by writing lines of code instead of using the AWS management console to individually provision resources.

---

# #M4

*) Amazon Virtual Private Cloud (Amazon VPC):

⇒ It is a networking service that you can use to establish boundaries around your AWS resources.

→ VPC lets you provision logically isolated section of the AWS cloud.

→ These resources can be public facing so they have access to the internet or, private with no internet access, usually for backend services like database or application servers.

→ Within a virtual private cloud (VPC), you can organize your resources into subnets.

↳ A subnet is a section of a VPC that can contain resources such as Amazon EC2 instances, ELB etc.

✡ Internet Gateway:

→ To allow public traffic from the internet to access your VPC, you attach an internet gateway to VPC.

→ Connection b/w VPC & the Internet

## ✡ Virtual Private Gateway:

→ To access private resource in a VPC, you can use a virtual private gateway

→ virtual private gateway is the component that allows protected internet traffic to enter into the VPC.

→ It enable you to establish a virtual private network (VPN) connection b/w your VPC & a private n/w

→ Allows traffic only, if it is coming from an approved n/w.

## ✡ AWS Direct Connect:

→ It is a service that enables you to establish a dedicated private connection b/w your data center & a VPC

→ Reduce n/w costs & increase the amount of bandwidth that can travel through your n/w.

## #) Subnets & Network Access Control Lists:

→

### *) Subnets:

→ Chunks of IP Addresses

→ A subnet is a section of a VPC in which you can group resources based on security or operational needs.

→ 2 types of subnets

- Public subnets: Contains resources that need to be accessible by the public, such as online store's website.
- Private subnets: Contains resource that should be accessible only through your private n/w such as a database that contains personal info.

→ In a VPC, subnets can communicate with each other.

*) Network traffic in a VPC:

→ When customer request data from an app^n hosted in the AWS cloud, this req. is sent as a packet.

Packet: Unit of data

→ It enters into a VPC through an Internet Gateway, before a packet can enter into a subnet or exit from a subnet it checks for permissions.

→ VPC component that checks packet permission for subnet is a Network Access Control List (NCL).

*) Network Access Control List (NACLs):

→ A network access control list (ACL) is a virtual firewall that controls inbound & outbound traffic at subnet level.

→ AWS a/c includes a default NIW ACL.

→ By default Network ACL allows all Inbound & outbound traffic

→ For custom NIW ACL denied all inbound & outbound traffic until you specify rule.

→ Network ACLs perform Stateless packet filtering i.e They remember nothing & check packet that cross the subnet border each way: Inbound & outbound.

→ VPC component that checks packet permissions for an Amazon EC2 instance is a Security Group.

*) Security Groups:

→ A security group is a virtual firewall that controls inbound & outbound traffic for an Amazon EC2 instance.

→ By default, Security Group denies all inbound traffic & allows all outbound traffic.

⇒ Security groups performs stateful packet filtering. They remember previous decision made for incoming packets.

eg: If packet A is allowed to enter previously next time it doesn't check.

→ Both Network ACLs & Security Groups enable you to configure uniform rules for traffic in your VPC.

## ⇒ Domain Name System (DNS):

→ In AWS we called

- **Amazon Route 53:**

↳ DNS web service.

→ It translates website name into IP, or Internet Protocol, addresses that computer can read.

→ Helps direct customer to the correct web location.

## ⇒ Routing Policies:

- latency-based
- geolocation DNS
- geoproximity
- weighted Round Robin.

# M5

*) Instance Stores : → If you stop/terminate EC2 all the data gets deleted.

→ An instance store provides temporary block-level storage for an Amazon EC2 instance.

→ Block-level storage volumes behave like physical hard drives.

→ An instance store is disk storage that is physically attached to host.

*) Amazon Elastic Block Storage : (Amazon EBS)

→ Amazon EBS is a service that provides block-level storage volumes that you can use with Amazon EC2 instance.

→ If you stop or terminate Amazon EC2 instance all the data on the attached EBS volume remains available.

→ With EBS, we can create virtual Hard drives, and we call EBS volume which attach to Amazon EC2 and these are separate from local instance store volumes, and they aren't tied directly to the host.

→ Create EBS → You define configuration (like volume size & type)

→ Stores data in a single Availability zone

*) Amazon EBS Snapshots :

→ Take incremental backups of EBS volumes by creating Amazon EBS snapshots.

→ EBS snapshot 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.

→ Incremental backups are diff. from full backups.

iv) S3 Intelligent - Tiering :

→ Ideal for data with unknown or changing access patterns
→ Requires a small monthly monitoring & automation fee per object
→ If you haven't accessed an object for 30 consecutive days Amazon S3 automatically moves it to S3 Standard IA tier.
→ If you access an object in the infrequent access tier, Amazon S3 automatically moves it to frequent access tier i.e. S3 Standard.

V) S3 Glacier :

→ Low-cost storage designed for data archiving
→ Able to retrieve objects within a few minutes to hours
→ optimized for Archive data.

VI) S3 Glacier Deep Archive :

→ Lowest-cost object storage class ideal for archiving
→ Able to retrieve object within 12 hours.

| Amazon EBS | Amazon S3 |
|---|---|
| → Stores as block | → Write once/read many<br>→ 99.999999 % durability |
| → Volume attach to EC2 instance.<br>→ Availability zone level resource.<br>→ Need to be in the same availability zone to attach EC2 instance<br>→ volume do not automatically scale.<br>→ Reupload just changed block. | → Web enabled<br>→ Regionally distributed (Across 3's)<br>→ store as cost savings<br>→ serverless.<br>→ Stores as object in buckets.<br>↳ complete discrete file<br>any change of object → you must complete re-upload all/complete object. |

## *) Amazon Elastic File System (EFS) :

→ Multiple instances can access the data in EFS at the same time.
→ Scales-up & down automatically when needed.
→ As you add & remove files, Amazon EFS grows & shrinks automatically.
→ Compared to Block Storage & Object Storage, File Storage is ideal for use cases in which a large number of services & resources need to access the same data at same time.
→ Multiple instances reading & writing simultaneously.
→ Linux file sys
→ Regional resource
→ Used with AWS cloud services & on-premises resources

| Amazon EBS | Amazon EFS |
|---|---|
| → Stores data in a single Availability zone. | → Is a regional service. Stores data in & across multiple Availability zone. |
| → To attach Amazon EC2 to an EBS volume, both must reside within same Availability zone | → Duplicate storage enables you to access data concurrently from all the Availability zone<br>→ on-premises servers can access Amazon EFS using AWS Direct Connect. |

## *) Relational Databases :

→ In a relational database, data is stored in a way that relates it to other pieces of data.
→ Relational databases use Structured Query Language (SQL) to store & query data.

*) Amazon Relational Database Service : (RDS)

→ Amazon RDS is a service that enables you to run relational databases in the AWS cloud.

→ Automates tasks such as Hardware provisioning, database setup & backups.

→ Amazon RDS database engines offers encryption at rest (protecting data while it is stored) and encryption in transit (protecting data while it is being sent & received.)

→ Lift-and-shift migration → to cloud.

• Benefits:
  → Automated patching
  → Backups
  → Redundancy
  → Failover
  → Disaster recovery

* Amazon RDS database engines:
→ Available on 6 database engines, which optimize for memory, performance or input/output (I/O)

i) Amazon Aurora
ii) PostgreSQL
iii) MySQL
iv) MariaDB
v) Oracle Database
vi) Microsoft SQL Server.

*) Amazon Aurora :

→ Amazon Aurora is an enterprise-class relational database.
→ Compatible with MySQL & PostgreSQL relational databases.
→ 5-times faster than standard MySQL & 3-times faster than standard PostgreSQL database.
→ High availability.
→ It replicates 6-copies of your data across 3-Availability zones & continuously backs up your data to Amazon S3
→ 1/10th cost of commercial database
→ Upto 15 read replicas
→ Point-in-time recovery.

*) Amazon DynamoDB :

→ Serverless Database
→ Non-Relational database (NoSQL)
→ Purpose built
→ Millisecond response time → delivers single-digit millisecond performance at any scale.
→ Full managed
→ Highly scalable.
→ It is a key-value database service.
→ Automatically scales.

* Non-Relational Databases :

→ In a non relational database, you create tables. A table is a place where you can store & query data.
→ Structure other than rows & columns to organize data.
→ key-value pairs.
→ In a key-value database, you can add or remove attributes from items in the table at any time.

| *) Amazon RDS | Amazon Dynamo DB |
|---|---|
| → Rows & Columns | → key-value pair |
| → Relational | → Non-Relational (Nosql) |
| → Server | → scaling up to 10-trillion req. per day. → serverless |

## *) Amazon Redshift:

→ Amazon Redshift is a data warehousing service that you can use for Big-Data Analytics.

→ Datawarehousing as a service
→ 10-times higher performance than traditional databases
→ Single API call
→ Less time waiting for results, more time getting answers.
→ It offers the ability to collect data from many sources & helps you to understand relationships & trends across your data.

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

→ AWS DMS enables you to migrate relational databases, nonrelational databases & other types of data stores.
→ Source database remains fully operational during the migration.
→ Downtime is minimized for applications that rely on that database.
→ Source & target databases don't have to be of the same type.

- Homogeneous migration: → Source & Target databases are of same type
- Heterogeneous migration: → Source & Target databases are of different type.
  → 2 Step process:
  ↳ Step 1 = convert using AWS schema conversion tool.
  ↳ Step 2 = Use DMS to migrate.

- Use case of DMS:
→ Development & test database migrations
→ Database consolidation
→ Continuous database replication.

*) Additional Database Services:

i) Amazon DocumentDB:
→ Document database service that supports MongoDB workloads.
→ MongoDB is a document database program.

ii) Amazon Neptune:
→ Graph database service
→ Work with highly connected datasets such as recommendation engine, fraud detection & knowledge graphs

iii) Amazon Quantum Ledger Database (Amazon QLDB):
→ Ledger database service
→ Use for review a complete history of all the changes that have been made.

iv) Amazon managed Blockchain:
→ To create & manage blockchain nlw with open-source frameworks.
→ Blockchain is a distributed ledger sim.

v) Amazon Elastic Cache:
→ Is a service that adds caching layers on top of your database to help improve the read times of common request.
→ Supports 2 types of data stores: Redis & Memcached

vi) Amazon DynamoDB Accelerator: (DAX)
→ DAX is an in-memory cache for DynamoDB
→ Helps to improve response times from single-digit millisecond to microsecond

# #M6

## *) Shared Responsibility model :

AWS responsibility ↙

→ AWS controls security of the cloud. → data centers, security of our services, All layers in this security

→ Customers controls security in the cloud

↑ Customer responsibility

| • Customer ⇒ Customer Data | • AWS ⇒ Software |
|---|---|
| → Platform, Appln, Identity & Access management | → Compute, storage, Database, Networking |
| → OS, Network & Firewall config" | → Hardware/AWS Global Infrastructure |
| → Client-side Data Encryption, server-side Encryption, Networking Traffic Protection | → Regions, Availability zones, Edge locations. |

**Qns:**
Which tasks are the responsibilities of customers ?

→ Patching SW on Amazon EC2 instances

→ Setting permissions for Amazon S3 object

**Qns:**
Which tasks are the responsibilities of AWS

→ Maintaining HW infrastructure

→ Implementing physical security controls at data centers

→ Maintaining servers that run Amazon EC2 instances.

## *) User Permissions & Access :

⇒ IAM

*) AWS Identity & Access Management : (IAM)

→ AWS IAM enables you to manage access to AWS services & resources securely.

→ Flexibility to configure access based on your company's specific operational & security needs.

→ • IAM users, groups and roles
• IAM policies
• Multi-factor authentication

*) AWS Account Root User :

→ Access and control any resources in the account.

→ First create an AWS account, you begin with an identity knows as Root User.

→ Root user is accessed by signing in with email address & password that you used to create your AWS account.

→ Do not use the Root user for everyday task. Instead, use the root user to create your first IAM user & assign it permissions to create other users.

*) IAM Users : → Person / App ~~in~~ that interact with AWS services & resources.
→ name & credentials.

→ By default, When you create a new IAM user in AWS, It has no permission associated with it.

→ To allow IAM user to perform specific actions in AWS, such as launching an Amazon EC2 instance or creating an Amazon S3 bucket, you must grand permissions ~~Explicitly~~.

→ Recommend that you create individual IAM users for each person who need to access AWS.

→ This idea called Principle of least privilege:
↳ A user is granted access only to what they need.

*) IAM Policies: → JSON
→ An IAM policy is a document that allows or denies permissions to AWS services & resources.
→ IAM Policies enables you to customize user's levels of access to resources.
→ Follow the security Principle of Least Privilege when granting permissions.
- Actions: Any AWS API call
- Resource: Which AWS resource the API call is for.

*) IAM Groups:
→ 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.

*) IAM Roles:
→ An IAM role is an identity that you can assume to gain temporary access to permissions.
→ must be granted permissions to switch to the roles.
→ When some assumes an IAM role, they abandon all previous permissions.

- Associated permissions
- Allow or Deny
- Assumed for temporary amounts of time
- No username or password
- Access to temporary permissions
- AWS service
- Users
- External identity
- Apps
- Other AWS services

*) Multi-Factor Authentication : (MFA)

→ In IAM, Multi-Factor authentication (MFA) provides an extra layer of security for your AWS accounts.

→ Your credentials like username / email & password then Random code/token sent to your phone to access.

*) AWS organizations :

→ A central location to manage multiple AWS accounts.
Consolidate and

→ When you create an organization, AWS organization automatically creates a root, which is parent containers for all the accounts in your organization.

→ You can manage ⇒ • Billing
• Control Access
• Compliance
• Security
• Shared resources

* Advantages : Features :
→ Centralized management
→ Consolidated billing
→ Hierarchical groupings of accounts
→ AWS service & API actions access control,

→ In AWS Organizations, you can centrally control permissions for the accounts in your organization by using Service-Control-Policies (SCPs)

→ SCPs specify the maximum permissions for member accounts in the organization.

→ SCPs enable to place restrictions on the AWS services, resources, and individual API actions that users & roles in each account can access

*) Organizational Units:

→ In AWS Organizations, you can group accounts into organizational units (OUs) to make it easier to manage accounts with similar business or security requirements.

→ When you apply a policy to an OU, all the accounts in the OU automatically inherit the permissions specified in the policy.

→ Easily isolate workloads or applications that have specific requirements.

Ans: You are configuring Service-Control-Policies (SCPs) in AWS organizations.
Which identities & resources can SCPs be applied to ?

(i) An Individual Member Account

(ii) An organizational unit (OU)

*) Compliance:

GDPR → EU

HIPAA → US

*) AWS Artifact:

→ AWS Artifact is a service that provides on-demand access to AWS security & compliance reports and select online agreements.

→ Depending on your company's industry you may need to uphold specific standards.

→ 2 main sections:

(i) AWS Artifact Agreements:

→ your company can sign agreement with this.

→ you can review, accept & manage agreements for an individual account and for all your a/c in AWS organization

(ii) AWS Artifact Report:

→ Need info^m about responsibility for complying with certain regulatory standards.

→ AWS Artifact Reports provide compilance reports from third-party auditors.

*) Customer Compliance Center:

→ Customer compliance center contains resources to help you learn more about AWS compliance.

→ Have solved various compilance, governance & audit challenges

→ You can also access compliance whitepapers & documentation on topics such as;

- AWS answers to key compliance questions
- An overview of AWS risk & compliance
- An auditing security checklist.

*) Denial-of-Service (DoS) Attack:

→ A Denial-of-Service (DoS) attack is a deliberate attempt to make a website or application unavailable to users.

*) Distributed Denial-of-Service Attack: (DDos)

→ In DDoS attack, multiple sources are used to start an attack that aims to make a website or application unavailable.

→ This can come from a group of attackers or even a single attacker which uses bots.

eg:- UDP Flood → solve: security Group
- HTTP Level attack → ELB
- Slowloris attack →

→ To minimize the effect of DoS & DDoS attack on your application, you can use AWS SHIELD

*) AWS Shield:

→ AWS shield is a service that protects applications against DDos attack.

→ It provides 2 levels of protection

(i) AWS Shield Standard

→ Automatically protects all AWS customers with no-cost.

→ Protect from most common, frequently occuring types of DDos attack.

→ It uses a variety of analysis techniques to detect malicious traffic in real-time & automatically mitigates it.

(ii) AWS Shield Advanced

→ Paid service that provides detailed attack diagnostics & the ability to detect & mitigate sophisticated DDos attack.

→ Integrates with Amazon CloudFront, Amazon Route 53 & ELB

→ you can integrate AWS Shield with AWS WAF by writing custom rule to mitigate complex DDos attack.

*) Additional Security Services:

*) AWS Key Management Service (AWS KMS):

→ AWS KMS enables you to perform encryption operations through the use of cryptographic keys.

→ You can use AWS KMS to create, manage & use cryptographic keys.

→ Encryption-at-rest & Encryption-in-transit

→ You can also control the use of key across a wide range of services & in your appln.

* AWS Inspector:

→ Amazon Inspector helps to improve the security & compliance of applications by running automated security assessments.

→ It checks appln for security vulnerabilities & deviations from security best practices.

→ Services of 3-parts:
- Network configuration reachability piece
- Amazon Agent
- Security assessment service.

*) AWS WAF:

→ AWS WAF is a Web Application Firewall that lets you monitor network requests that come into your web application.

→ AWS WAF works with Amazon CloudFront & Application load Balancer.

→ AWS WAF works in a similar way to block or allow traffic. However, it does this by using a web Access control List (ACL) to protect your AWS resources.

*) Amazon GuardDuty :

→ Amazon GuardDuty is a service that provides intelligent threat detection for your AWS infrastructure & resources.

→ It identifies threats by continuously monitoring the network activity & account behavior within your AWS environment.

→ Runs independently from your other AWS services.

---

*) Identity Federation :

→ comes with IAM

→ If you have an existing corporate identity store, you can federate those users to AWS, using role based access, which allows your users to use one login for both your corporate sim as well as AWS.

→ with IAM you make sure to turn-on MFA for Root Users.

# M7

*) Monitoring :

⇒ Observing systems, collecting metrics, and then using data to make decisions.

*) Amazon CloudWatch :

→ Amazon CloudWatch is a web service that enables you to monitor & manage various metrics and configure alarm action based on data from those metrics. ← in real time

• Metrics : Variable tied to your resources.

→ CloudWatch uses Metrics to represent the data points for your resources.

→ CloudWatch uses metrics to create graph automatically that show how performance has changed over time.

*) Benefits :

→ Access all your metrics from a central location.

→ Gain visibility into your appln, infrastructure & services.

→ Reduce MTTR & improve TCO

→ Give insights to optimize appln & operational issues.

*) CloudWatch Alarms :

→ With CloudWatch, you can create alarms that automatically perform actions, if the value of your metric has gone above or below a predefined threshold.

→ When configuring the alarm, you can specify to receive a notification whenever this alarm is triggered.

* CloudWatch Dashboard :

⇒ The CloudWatch dashboard feature enables you to access the metrics for your resources from a single location.

*) AWS CloudTrail :

→ AWS CloudTrail records API calls for your account.

→ It is the comprehensive API auditing tool.

→ Every request gets logged in the CloudTrail engine.

→ The engine records exactly:
- Who made the request & which operator, when did they send the API call?
- Where were they? What was their IP? And what was the response?
- Did something change? And what is the new state? Was the request denied?

→ Events are typically updated in CloudTrail within 15 minutes after an API call.

→ It saves logs indefinitely in secure S3 buckets.

→ you can filter events by specifying the time & date that an API call occured.

*) CloudTrail Insights :

→ With CloudTrail, you can also enable CloudTrail insights.

→ This optional feature allows cloudTrail to automatically detect unusual API activities in your AWS account

*) AWS Trusted Advisor :

→ AWS Trusted Advisor is a web service that inspect your AWS environment & provides real-time recommendations in accordance with AWS best practices.

→ Trusted Advisor compares it finding to AWS best practices in 5 categories / pillars :

a) Cost Optimizations
b) Performance
c) Security
d) Fault Tolerance
e) Service limits

CPSFS

*) AWS Trusted Advisor Dashboard :

→ You can view all 5 pillars of Trusted Advisor in the AWS management console. And can do complete checks for the pillars.

→ For each category

- The green check → No problem
- The Orange triangle → Recommended Investigations
- The Red Circle → Recommended Actions

---

Q.No: Which service enables you to review the security of your Amazon S3 bucket by checking for open access permissions ?

→ AWS Trusted Advisor

# M 8

## Pricing And Support

*) **AWS Free Tier:**

⇒ The AWS Free Tier enables you to begin using certain services without having to worry about incurring costs for the specified period.

→ Free Tier offers 3-diff types to try out a service.

i) Always Free
ii) 12 Months Free
iii) Trials

**Ex:**

(i) **Always Free:**

→ offers do not expire & are available to all AWS customers

→ Ex: AWS Lambda allows 1 million free requests & up to 3.2 millions seconds of compute time per month.

: Amazon DynamoDB allows 25 GB of free Storage per month.

(ii) **12 Months Free:**

→ Free for 12 months following your initial sign-up

→ Ex: Amazon S3 Standard Storage

: Amazon EC2 compute time

: Amazon CloudFront

(iii) Trials :

→ Short-term free trials offer

→ Length of each trials might vary no. of days or the amount of usage in the service.

→ Ex: Amazon Inspector offers 90-days free trials

:→ Amazon Lightsail offer 750 free hours of usage over a 30-days period.

## *) AWS Pricing Concepts :

*) How AWS Pricing works :

→ AWS offers a range of cloud computing services with pay-as-you-go pricing

→ They are: →

a) Pay for what you use :

→ For each service, you pay for exactly the amount of resources that you actually use, without requiring long-term contracts or complex licensing.

b) Pay less when you reserve :

→ Some services offers reservation options that provide a significant discount compared to on-demand Instance pricing.

→ Ex: Amazon EC2 Instance Saving plans which save up to 72% over equivalent on-demand Instance capacity.

c) Pay less with volume-based discounts when you use more:

→ Some service offer tiered pricing, so the per-unit cost is incrementally lower with increased usage.

→ eg: The more Amazon S3 Storage space you use, the less you pay for it per GB.

## *) AWS Pricing Calculator:

→ AWS pricing calculator lets you explore AWS services & 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.

→ You can save your estimate and generate a link to share it with others.

## *) AWS Pricing Examples:-

### A) AWS Lambda:

→ For AWS Lambda, you are charged based on the no. of requests for your functions & the time that it takes for them to run.

→ 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 Compute Saving plans.

→ Committing to a consistent amount of usage over 1-year or 3-year term

↳ example of Pay less when you reserve

B) Amazon EC2:

→ Here, you pay for only the compute time that you use while your instance are running.

→ Ex: Spot Instance → can save upto 90%.

: Can consider Saving plans & Reserved Instance.

C) Amazon S3:

→ For Amazon S3 pricing, consider the following cost components:

i) Storage: → Pay for only the storage that you use.
→ Charged rate to store object in Amazon S3 bucket.

ii) Requests & Data Retrievals: → Pay for requests made to your Amazon S3 objects & buckets.

iii) Data transfer: → There is no cost to transfer data b/w diff. Amazon S3 buckets or from Amazon S3 to other services within the same AWS Region.

→ However, you pay for data that you transfer into & out of Amazon S3

iv) Management & Replication: → Pay for the storage management features that you have enabled on your account's Amazon S3 bucket.

→ features: inventory, analytics & object tagging.

*) Billing Dashboard

→ Use the AWS Billing & Cost Management Dashboard to pay your AWS bill, monitor your usage & analyze and control your costs.

*) Consolidated Billing :

→ One of the lovely feature of AWS organization.

→ The Consolidated billing feature of AWS organizations enables you to receive a single Bill for all AWS accounts.

→ Default max^m no. of accounts allowed per an organization is (4), but you can contact AWS support to increase your quota if needed.

→ You can get Bulk discount pricing, Saving Plans & Reserved Instance across the accounts in your organization.

- Benefits :
  - → Usage for AWS services is rolled up to the organization level.
  - → offer bulk pricing

* Summary :
- Simplifies billing process
- Share savings across accounts
- Free feature

*) AWS Budgets :

→ AWS Budgets, you can create budgets to plan your service usage, service cost & instance reservation.

↳ Its like allows you to set custom budgets.

→ The information in AWS Budgets update (3) times a day.

→ You can also set custom alerts when your usage exceeds the budgeted amount.

*) AWS Cost Explorer :

→ AWS Cost Explorer is a tool that enables you to visualize, understand & manage your AWS costs & usage over time.

→ Console base service.

→ AWS Cost Explorer includes a default report of the costs & usage for your top 5-cost-accruing AWS services.

→ You can apply custom filters & groups to analyze your data.

Ex: Tag → user-defined key-value pairs

→ It allows you to create custom reports.

---

*) AWS Support Plans :

⇒ AWS offers 4-different support plans to help you troubleshoot issues, lower costs, & efficiently use AWS services.

→ They are:
(i) Basic
(ii) Developer
(iii) Business
(iv) Enterprise

} B D B E

(i) Basic Support:
→ Free for all AWS customer.
→ Access to whitepapers, documentation & support community forum
→ 24/7 customer service → billing qns & service limit increase
→ Access to a limited selection of AWS Trusted Advisor checks
→ You can use the AWS Personal Health Dashboard.
↳ provides alerts & remediation guidance

(ii) Developer Support:
→ Includes all the benefits of Basic support
→ Ability to open an unrestricted no. of technical support cases.
→ Pay-by-the-month pricing & required no-long-term contract

common for Business & Enterprise ⇒ common

→ Customers in the 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 & services together

- Email customer support directly with a 24 hours response time
- Response less than 12 hours in case our sim are impaired.

(iii) Business Support :

→ (a) Common → Basic & Developer

→ Customers with a Business Support plan have access to additional features including:

- Use-case guidance to identify AWS offerings, features & services that can best support your specific needs.
- All AWS Trusted Advisor checks.
- Limited support for third-part software, such as common operating systems & application stack components.
- Direct phone access to support team that has 1-hour response SLA.
- 1 hours response if your production sim is impaired

(iv) Enterprise Support :

→ (a) Common

→ In addition to all features including Basic, Developer & Business support plans, Customer have access to features such as:

- Application Architecture guidance, which is a consultative relationship to support your company's specific use cases & 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 & scaling guidance.
- A Technical Account Manager. (TAM)
- 15-minutes SLA for Business critical workloads

*) Technical Account Manager : (TAM)

→ Includes with Enterprise support plan.

→ TAM is your primary point of contact at AWS, if your company has Enterprise Support plan.

→ Provide guidance, architectural reviews and ongoing communication with your company as you plan, deploy & optimize your applications.

→ Your TAM provides expertise across the full range of AWS services.

→ They help you design solutions that efficiently use multiple services together through an integrated approach

**) AWS Five Pillars of the Well-Architected Framework:

a) Operational Excellence
b) Security
c) Reliability
d) Performance Efficiency
e) CoST Optimization

} OSR P C

• Well-Architected Review:

→ TAM work with customers to review architectures using Well-Architected Framework.

→ Architectures are checked against 5-pillars of Well-Architected Framework.

*) AWS Marketplace :

⇒ AWS Marketplace is a curated digital catalog that includes thousands of software listing from independent software vendors.

→ can use to find, test & buy software / find, deploy & manage third party software that run on AWS.

→ You can access detailed information for each listing i.e,
- pricing options
- available support
- Review from other AWS customers.

→ Can explore SW solutions by industry & use case.

→ Allow customer to run third party applications like one-click deployment.

→ Offer on-demand pay-as-you-go option.

⊛ Enterprise focused features :

→ Custom terms & pricing
→ A private marketplace
→ Integration into your procurement systems
→ Cost management tools.

*) AWS Marketplace categories:

I) Business Applications
II) Data & Analytics
III) DevOps
IV) Infrastructure software
V) Internet of Things (IOT)
VI) Machine Learning
VII) Migrations
VIII) Security

---

# M9

*) Migration Strategies AND Innovation: ***

*) AWS Cloud Adoption Framework (AWS CAF):

→ Help you to manage migration process through guidance
→ Provide advice to company to enable quick & smooth migration to AWS.

*) Six Core Prespective of the Cloud Adoption Framework:

→ Business, People & Governance → Focus on Business capability
→ Platform, Security & Operations → Focus on Technical capability

→ They are : B P G P S O

i) Business Perspective :

→ Business or Finance analysts
→ Ensures that IT aligns with business needs and that IT investments link to key business results.
→ To create a strong business case for cloud adoption & prioritize cloud adoption initiatives.

→ Common roles :
- Business managers
- Finance managers
- Budget owners
- Strategy Stakeholders.

ii) People Perspective :

→ HR
→ Supports development of an organization-wide change management strategy for successful cloud adoption.
→ To evaluate organizational structures & roles, new skill & process requirements and identify gaps.
→ Helps prioritize Training, Staffing & Organizational changes

→ Common roles :
- Human Resource
- Staffing
- People managers

iii) Governance Perspective:

- Focuses on the skills & process to align IT strategy with business strategy.
- Maximize the business value & minimize risks.
- Use to understand how to update the staff skills & process necessary to ensure business governance in the cloud.
- Manage & measure cloud investment
- Common role:
  - Chief Information officer (CIO)
  - Program managers
  - Enterprise Architects
  - Business analysts
  - Portfolio managers

iv) Platform Perspective:

- Includes principles & patterns for implementing new solutions on the cloud, and migrating on-premises workloads to the cloud.
- Use a variety of architectural models to understand & communicate the structure of IT sln & their relationship
- Common roles
  - Chief technology officer (CTO)
  - IT manager
  - solution architects.
  - cloud architect

v) Security Perspective:

→ Ensures that the organization meets security objectives for visibility, auditability, control & agility.

→ Use the AWS CAF to structure the selection & implementation of security controls that meet the organization's needs.

→ Common roles:
- Chief Information Security officer (CISO)
- IT security managers
- IT security analysts

vi) Operations Perspective:

→ Helps to enable, run, use, operate & recover IT workloads to the level agreed upon with your business stakeholders.

→ Define how day-to-day, quarter-to-quarter & year-to-year business is conducted.

→ AWS CAF help these stakeholders define current operating procedures & identify the process changes & training needed to implement successful cloud adoption

→ Common roles:
- IT operations managers
- IT support managers

Q's: Which perspective of the AWS Cloud Adoption Framework helps you design, implement & optimize your AWS infrastructure based on your business goals & perspective?

Ans: Platform Perspective

*) Migration Strategies:

⇒ 6 R's of migration

↳ There are 6 Strategies for migration based on time, cost, priority, criticality

i) Rehosting:

→ "Lift-and-Shift" ⇒ Moving Appln without changes - (No code changes)

→ 30% cost save

→ Implement its migration & scale quickly to meet a business case.

ii) Replatforming:

→ "Lift, tinker, & Shift" ⇒ making a few cloud optimizations to realize a tangible benefit.

→ Optimization is achieved without changing the core architecture of the application.

→ No code changes

iii) Retire / Retiring:

→ Retiring is the process of removing applications that are no longer needed.

iv) Retain / Retaining:

→ Keeping applications that are critical for the business in the source environment.

→ Might include applications that are require major refactoring before they can be migrated or work.

→ Don't turn off for 3-months or 8-months.

v) Repurchase :

→ Repurchasing involves moving from a traditional license to a software-as-a-service model → moving to a diff. model

→ Total upfront expenses goes up but potential benefits could be substantial.

vi) Refactoring/Re-architecting :

→ Involves reimagining how an application is architected & developed by using cloud-native features.

→ Refactoring is driven by a strong business need to add feature, scale or performance that would otherwise be difficult to achieve in the application's existing environment.

→ You will write new code

→ Highest initial cost in terms of planning & human effort.

*) AWS Snow Family :

→ The AWS Snow Family is a collection of physical devices that help to physically transport up to exabytes of data into & out of AWS.

→ AWS Snow Family members :

a) AWS Snowcone

b) AWS Snowball

c) AWS Snowmobile

ii) AWS Snowcone :

→ Small, rugged & secure edge computing & data transfer device

→ It features 2 CPUs, 4 GB of mem & 8 TB of storage

iii) AWS SnowBall :

→ offers 2 types of devices :

(a) Snowball Edge Storage Optimized :

→ Suited for large-scale data migration & recurring transfer workflows,

→ Storage : 80 TB of HDD for Amazon S3 compatible object storage

: 1 TB of SATA for block volumes

→ Compute : 40 vCPU, & 80 GiB of mem to support Amazon EC2 sbe1 instances (eg. C5)

(b) Snowball Edge Compute Optimized :

→ provide powerful computing resources for use cases such as machine learning, full motion video analysis analytics & local computing stacks

→ Storage : 42 TB HDD for Amazon S3 or Amazon EBS

: 7.68 TB of NVMe SSD for Amazon EBS Volume

→ Compute : 52 vCPUs, 208 GiB of mem & an optional NVIDIA Tesla V100 GPU .

iii) AWS SnowMobile :

→ An exabyte-scale data transfer service used to move large amount of data to AWS.

→ You 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 :

*) Innovation with AWS Services :

→ You are properly equipped to drive innovation in the cloud if you can clearly articulate the following conditions :

- The current state
- The desired state
- The problems you are trying to solve

II) Serverless Application :

→ Refers to appln that don't require to provision, maintain or administer servers.

eg: AWS Lambda

→ No need to worry about fault tolerance or availability.

→ Developers can focus on their core product instead of managing & operating servers.

(II) Artificial Intelligenel :

→ AWS offers variety of services powered by AI

eg:

- Convert speech to text with Amazon Transcribe
- Discover patterns in text with Amazon Comprehend
- Identify potentially fradulent online activities with Amazon Fraud Detector.
- Build voice & text chatbots with Amazon Lex

(III) Machine Learning :

→ AWS offers Amazon SageMaker to remove the difficult work from the process & empower you to build, train & deploy ML models quickly

→ Use ML to analyze data, solve complex problems & predict outcome before they happen

Ex: SageMaker

: Amazon Augmented AI (A2I)

# M10

*) The AWS Well-Architected Framework :

→ Tool to evaluate the architectures you build for excellence in a few diff. categories.

→ Helps you to understand How to design and operate reliable, secure, efficient & cost-effective sim in the AWS.

→ Provides a way for you to consistently measure your architecture against best practices & design principles & identify areas for improvement.

→ The Well-Architected Framework is based on 5 pillars:
<O S R P C>

> Operational Excellence :

→ The ability to run & monitor sim to deliver business value & to continually improves supporting processes & procedures.

→ Design principles for operational excellence includes
- operations as code,
- annotating documentation
- anticipating failure
- frequently making small, reversible change

(iii) Security : → encryption

→ The ability to protect information, systems & assets while delivering business value through risk assessments and mitigation strategies.

→ Security best practices:
- Automate security best practices when possible.
- Apply security at all layers
- protect data in transit & at rest

(iii) Reliability :

→ Focuses on recovery planning

→ Ability of a sim to do :
- Recover from infrastructure or service disruptions
- Dynamically acquire computing resources to meet demand
- Mitigate disruptions such as misconfigurations or transient nlw issues.

→ Reliability includes testing recovery procedures, scaling horizontally to increase aggregate sim availability, & automatically recovering from failure.

(iv) Performance Efficiency :

→ Ability to use computing resources efficiently to meet sim requirements & to maintain that efficiency as demand changes & technologies evolve.

→ Evaluating performance efficiency of your architecture includes experimenting more often, using serverless architecture & designing sim to be able to go global in minutes

(v) Cost Optimization :

→ The ability to run sim to deliver business value at the lowest price point.

→ Includes - adopting a consumption mode,
- analyzing & attributing expenditure,
- using managed services to reduce the cost of ownership.

*) Benefits of the AWS Cloud :

→ six main benefits

(i) Trade upfront expense for variable expense :

→ Includes - Data center
- physical servers
- other resources that you would need to invest in before using compute resources.

→ Instead of investing heavily in data centers & servers, you can pay only when you consume computing resources.

(ii) Benefit from massive economies of scale :

→ you can achieve a lower variable cost

→ AWS achieve higher economies of scale.

→ Economies of scale translate into lower pay-as-you-go prices.

(iii) Stop guessing Capacity:

→ You don't have to predict how much infrastructure capacity you will need before deploying an appln.

(iv) Increase speed & agility:

→ The flexibility of cloud computing makes it easier to develop & deploy applications.

→ Flexibility also provide development teams with more time to experiment & innovate.

(v) Stop spending money running & maintaining data centers:

→ You don't have to spend more money & time managing infrastructure & servers.

→ Focus less on these tasks & more on your applications & customers.

(vi) Go global in minutes:

→ AWS cloud global footprint enables you to quickly deploy appln to customers around the world, while providing them with lowest latency.

low