A Cloud Guru - CPC

Domain	% of Examination
Domain 1: Cloud Concepts	26%
Domain 2: Security and Compliance	25%
Domain 3: Technology	33%
Domain 4: Billing and Pricing	16%
TOTAL	**100%**

Cloud Computing & AWS

Cloud computing types:

1. IAAS
2. PAAS
3. SAAS

Cloud Computing Deployments

1. Public Cloud - AWS, Azure, GCP
2. Hybrid - Mixture public/private
3. Private Cloud(on Premise)

AWS Global Infrastructure (Exam relevant)

Compute -

1. EC2
2. Lambda

Database -

1. Relational Database Service(RDS)
2. DynamoDB(Non-relational)

Storage -

1. Simple Storage Service(S3)
2. Glacier

Migration & Transfer

Network & Content Delivery

Security, Identity & Compliance

AWS cost management

Benefits of the cloud computing

- **Trade Capital Expense for variable expense -** No upfront costs such as paying for server. You can Pay On Demand.
- **Benefit of Massive Economies of scale -** you can simply save a lot of money since there are so many people using the cloud.
- **Stop guessing about capacity-** You can scale up or scale down based on your need.
- **Increase speed and agility -** With few clicks of a button your service is deployed.
- **Stop spending money on running & maintaining Data Centers -** No more maintenance costs.

- **Go global in few minutes -** since there are global regions where cloud servers are hosted.

AWS Global Infrastructure

1. Availability Zone - Data Center
2. Region - Geographical area Consisting of 2 or more availability zones
3. Edge locations- Endpoints for AWS used for caching content - CloudFront, Amazon's Content Delivery Network(CDN)

Choosing AWS Region

1. Data Sovereignty Laws
2. Latency to end users
3. AWS Services

Different support packages

1. Basic
2. Developer
3. Business
4. Enterprise

How to create a billing alarm - Cloud Watch service(Management & Governance)

IAM - Security, Identity & Compliance
IAM is global, you do not need to specify a region for it - User/Group created globally

Access AWS Console in 3 ways:-

1. Via Console
2. Programmatically (Using Command Line)
3. Software Development Kit(SDK)

Root Account
Root account is email address you used to setup your AWS account
Always has full admin access
You secure root account using MFA
You create users for individuals within your company

A group is a way to store all your users
Users will inherit all permissions of their groups
Permissions to a Group - apply policies (JSON format)

S3

1. Simple place to store your files(audio, video, csv and not DB files)
2. **Object based storage -** it allows you to store files
3. File size - 0 to 5 TB

4. Files are stored in buckets(just like a folder)
5. Bucket names must be unique **globally**
6. If upload successful- **HTTP 200 code** is received
7. Objects are stored in Key-Value pair-
   a. Key - name of object
   b. Value - data
8. Object consists of:-
   a. Key
   b. Value
   c. Version ID
   d. Metadata ID
   e. Subresources - Access control list/ Torrent
9. Data Consistency for S3
   a. Read after Write consistency for PUTS of new objects
   b. Eventual consistency for overwrite PUTS and deletes (it can take some time to sync)
10. S3 features
    a. Tiered Storage available
    b. Lifecycle Management
    c. Versioning
    d. Encryption
    e. Secure data using Access Control List and Bucket Policies
11. S3 - 6 Storage Classes
    a. S3 standard
    b. S3 - IA - Infrequently Accessed)
    c. S3 One Zone - IA: Low cost option
    d. S3 Intelligent Tiering: uses ML
    e. S3 GLACIER
    f. S3 Glacier Deep Archive: Can't access file for 12 hrs
12. S3 charges
    a. Storage
    b. Request
    c. Storage management pricing
    e. Data Transfer Pricing
    f. Transfer Acceleration
    g. Cross Region replication pricing
13. Restricting Bucket Policies
    a. Bucket Policies - Applies to whole bucket
    b. Object Policies - Applies to individual files
    c. IAM policies - users & groups
14. S3 can be used to host static websites. Dynamic websites with DB connection cannot be hosted on S3
15. S3 scales automatically

CloudFront

CDN delivers webpages based on user's geographic location.

Key terminology:-

1. **Edge location -** The location where content is cached. Separate to a AWS region
2. **Origin -** origin of all the files that CDN will distribute. This can be S3 bucket, EC2 instance, Elastic Load balancer, Route53
3. **Distribution -** Name given to CDN which consist of collection of Edge locations

CloudFront can be used to deliver your website using global network of edge locations.

CloudFront can be found under **Networking & Content Delivery** in Access Management Console

2 types of distribution:

1. Web
2. RTMP

Edge locations are not just Read Only, you can put objects in them too

Objects are cached for the duration of TTL(Time to Live)

You can clear cached objects but you will be charged

EC2 Elastic Compute Cloud

1. EC2 is a compute based service. It's not server less. It's a server
2. Virtual server in cloud
3. Use a private key to connect to EC2
4. It is a web service that provides resizable compute capacity in the cloud
5. Quickly scalable
6. EC2 Pricing models
   a. On Demand
   b. Reserved - Standard Reserved Instances, Convertible Reserved Instances, Scheduled Reserved Instances
   c. Spot
   d. Dedicated Hosts
5. If spot instance is terminated by Amazon EC2 you will not be charged for partial hour usage
6. If you terminate the spot instance, by yourself then you will be charged
7. Recommendation- Always design for failure. Have one EC2 instance in each availability zone
8. **Security Groups -**
   a. Are virtual firewalls in the cloud.

b. You need to open ports in order to use them.
c. Popular ports are SSH(22), HTTP(80), HTTPS(443), RDP(3389)

Practice Lab(command line):

1. Connecting to you EC2 instance on MAC - ssh ec2-user@<ip_address> -i <private_key.pem>
2. Yum update -y: updates security patches for your EC2 instances
3. Get root level privileges- sudo su

Amazon EBS Elastic Block Store

1. Virtual hard disk used for storage
2. Attached to EC2 instances
3. Placed in specific availability zones
4. Types of EBS
   a. SSD
   1. General purpose SSD(GP2)
   2. Provisional IOPS SSD(IO1)
   b. Magnetic
   1. Throughput Optimized HDD(ST1)
   2. Cold HDD(SC1)

Using Roles

1. Roles are much more secured than using access Key IDs and Secret access Keys
2. Easier to manage
3. You can apply roles to EC2 instances at any time. When you do this, the change takes place immediately
4. Roles are universal. No need to specify regions they are in, similar to users

Load Balancer

1. 3 types of Load Balancers:
   a. Application LB - HTTP/HTTPS
   b. Network LB - TCP
   c. Classic LB - Previous Generation
2. Application LB - Layer 7 (Make Intelligent Decisions)
3. Network LB - Extreme Performance/Static Ip Addresses
4. Classic LB - Test & Dev, Keep Costs Low

Databases 101

1. Relational Databases on AWS are called RDS:
   a. SQL Server
   b. Oracle
   c. MySQL Server
   d. PostgreSQL

e. Aurora
f. MariaDB

2. RDS has 2 key features:
    1. Multi-AZ(availability zones) - For disaster recovery
    2. Read Replicas - for performance
3. Non Relational Databases:
    1. Collection = Table
    2. Document = row
    3. Key Value Pairs = Fields
    4. The columns in the table can vary
    5. This will not affect other rows in the database
    6. **Amazon's Non-Relational DB is called DynamoDB**
4. OLTP - just like simple SQL queries
5. OLAP - complex SQL queries - Sum of a column, aggregation etc
6. Data Warehousing - Used for BI - used for large and complex data sets
7. **Amazon's Data Warehouse solution - Redshift (OLAP)**
8. **ElastiCache -** Webservice that makes it easy to deploy, operate and scale in-memory cache in the cloud
    1. Supports 2 in-memory cache engines:
        1. Memcached
        2. Redis

DNS

1. Domain Name System is the process computers use to resolve domain names to IP addresses
2. **Networking & Content Delivery - Amazon DNS Service is called Route53**
    1. DNS management
    2. Traffic Management
    3. Availability monitoring
    4. Domain Registration
    5. You can use Route53 to direct traffic all around the world
    6. You can use it to register a domain name
    7. It is global, similar to IAM and S3

EBS - Elastic Beanstalk

1. Quickly deploy and manage applications in AWS CLOUD without worrying about the infrastructure that runs those applications.
2. You can simply upload your application, EBS automatically handles the details of capacity provisioning, load balancing, scaling, application health monitoring

AWS CloudFormation

1. It's a service that helps you model and set up you AWS resources so that you can spend less time managing those resources and more time focusing on your applications that runs in AWS

2. You can create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances)
3. It takes care of provisioning and configuring those for you
4. **EBS and CLoudFormation are both Free services however the resources they provision are not free.(such as EC2, RDS etc)**
5. **EBS is limited in what it can provision and is not programmable. Cloud Formation can provision almost any AWS service and is completely programmable**

Architecting for Cloud - Best Practices

1. IT Assets as Provisioned Resources
2. Global, Available and Scalable Capacity
3. Higher Level Managed Services
4. Built-in Security
5. Architecting for Cost
6. Operations on AWS

Scalability

1. Scale Up - t2.micro to t2.large
2. Scale Out - Add Multiple virtual machines
    1. Stateless applications
    2. Distribute Load to Multiple Nodes
    3. Stateless Components
    4. Stateful Components
    5. Implement Session Affinity - Sticky sessions: stuck to particular EC2 instance; You put a cookie in users browser and application load balancer will send them to exact EC2 instance
    6. Distributed Processing - Process large/complex jobs
    7. Implement Distributed Processing

Disposable Resources instead of Fixed Servers

1. Instantiating Compute Resources
    1. Bootstrapping
    2. Golden Images - Autoscaling
    3. Containers
    4. Hybrid
2. Infrastructure as Code
    1. CloudFormation

Automation

1. Server-less Management and Deployment
2. Infrastructure Management and Deployment
    1. AWS EBS
    2. EC2 auto recovery
    3. AWS systems manager

    4. Auto Scaling
3. Alarms and Events
    1. Amazon CloudWatch alarms
    2. Amazon CloudWatch Events
    3. AWS Lambda scheduled events
    4. AWS WAF(Web Application Firewall) security automations

Loose Coupling

1. Well Defined Interfaces - Amazon API Gateway
2. Service Discovery - Implement Service Discovery
3. Distributed Systems Best Practices - Graceful Failure in Practice

Services Not Servers

1. Managed Services
2. Server-less Architecture

Databases

1. **Relational DB(Aurora)**
    1. Scalability
    2. High Availability-Multi-AZ
    3. Anti-Patterns-no need for joins or complex transactions, use No-SQL
2. **Non-Relational DB(Dynamo DB)**
    1. Scalability
    2. Hight Availability - Multi AZ
    3. Anti-Patterns - requires joins or complex transactions, use relational DB(Aurora and others). If you have large blob files, consider storing files in Amazon S3
3. **Data Warehouse(Redshift)**
    1. Scalability
    2. High Availability-Multi AZ
    3. Anti Patterns - not meant for OLTP
4. **Graph Databases**
    1. **Graph Databases - Amazon Neptune**
        1. Scalability
        2. High Availability
5. **Managing Large Volumes of Data**
    1. **Data Lakes**
        1. Architectural approach that allows you to store massive amounts of data in a central location
        2. Data can be stored as-is, no need to convert into pre-defined schema
6. **Removing Single Point of Failure**
    1. Introducing Redundancy
    2. Detect Failure
    3. Durable Data Storage
    4. Automated Multi-Data Centre Resilience

5. Fault Isolation and Traditional Horizontal Scaling(scale out) ; vertical scaling is scale up
6. Sharding(split your data across multiple shards and process data faster) - using Elastic Map Reduce(EMR)

7. **Optimize for Cost**
    1. Right Sizing
    2. Elasticity
    3. Take Advantage of variety of Purchasing options
        1. Reserved Capacity
        2. Spot Instances
8. **Caching**
    1. Application Caching - Elastic Cache
    2. Edge Caching - CloudFront
9. **Security**
    1. Use AWS Features for defense in depth - Firewalls etc.
    2. Share Security Responsibility with AWS
    3. Reduce Privileged Access - Least Privileges to user
    4. Security as Code - security patch templates can be applied to multiple regions
    5. Real-time Auditing - AWS Inspector
    6. **Check aligned white-paper before exam**

AWS Global Services

1. IAM
2. Route53
3. CloudFront
4. SNS - not available in all region
5. SES - available in all region
6. Global Views
    1. S3 - Global view but are regional

AWS Services Deployed on Premise

1. Snowball
2. Snowball Edge
3. Storage Gateway
4. CodeDeploy
5. Opsworks
6. IoT Greengrass

Which Services can be used to deploy applications On Premise:

1. CodeDeploy
2. Opsworks

CloudWatch 101

1. Used for monitoring performance

2. Can monitor most of AWS as well as your applications that run on AWQS
3. CloudWatch with EC2 will monitor events evert 5 minutes by default
4. You can have 1minute interval by turning on detailed monitoring
5. You can create cloud watch alarms which trigger notifications
6. Cloudwatch is all about performance

AWS Systems Manager

1. Allows you to manage fleets of EC2 instances and virtual machines
2. EC2 fleet - multiple instances of EC2
3. Can be both inside AWS and on premise
4. A piece of software is installed on each VM
5. Run command is used to install, patch, uninstall software
6. Integrates with CloudWatch to give you a dashboard of your entire estate

Summary of Cloud Concepts and Technology

Advantages of Cloud Computing

1. Trade capital expense for variable expense
2. Benefit from massive economies of scale
3. Stop guessing about capacity
4. Increase speed and agility
5. Stop spending money running and maintaining data centers
6. Go global in minutes

3 types of Cloud computing

1. IAAS
2. PAAS
3. SAAS

3 types of Cloud computing Deployments

1. Public Cloud - AWS, Azure, GCP
2. Hybrid - Mixture of public and Private
3. Private Cloud(or on Premise) - You manage it, in your datacenter, typically using openstack or VMware

Region/Availability Zone/Edge Location

1. A region is physical location in the world which consists of two or more AZs
2. An AZ is one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities
3. Edge Locations are endpoints for AWS which are used for caching content. Typically this consists of CloudFront, Amazon's Content Delivery Network (CDN)

Choosing the right AWS region

1. Data Sovereignty Laws
2. Latency to end users
3. AWS Services

Different support packages

1. **Basic -** Free
2. **Developer -** $29 a month (scales based on usage)
3. **Business -** $100 A MONTH (scales based on usage)
4. **Enterprise-** $15k a month (scales based on usage) - TAM(Technical Account Manager)

Billing Alert/Billing Alarms

1. Will alert you automatically when a certain level of AWS spend has been reached.
2. If you are learning AWS for the first time you should turn it on so that you don't spend money without realizing it.

IAM

1. Identity Access Management
2. It's Global, you do not specify a region when dealing with IAM
3. When you create a user or a group, this is created Globally

Access AWS platform in 3 ways:

1. Via Console
2. Programmatically (using command line)
3. Using SDK

Root Account

1. It's the email address you used to setup your AWS account
2. Always has full admin access
3. Always create a user for each individual within your organization
4. Always secure root account using MFA

Group

1. It's a place to store your users
2. Your users will inherit all permissions that the group has
3. Group examples- developers, system admins, HR, Finance etc.
4. To set the permissions in a group yo need to apply policies
    1. Policies can be Java Script Object Notation (JSON)
    2. These are referred to as key value pairs - {"name":"Nabh"}

S3

1. Object based - allows you to upload files
2. File can be - 0 bytes to 5 TB
3. There is unlimited storage
4. Files are stored in buckets
5. S3 is a universal namespace. Names must be unique globally
6. Not suitable to install OS
7. Successful uploads will generate a HTTP 200 status code

8. Key Fundamentals of S3
    1. **Key(name of object)**
    2. **Value(data and is made up of sequence of bytes)**
9. Read after Write consistency for PUTS of new objects
10. Eventual Consistency for overwrite PUTS and DELETES (can take some time to propagate)
11. You view buckets globally but you can have buckets in individual regions
12. You can replicate the contents of one bucket to another bucket automatically by using cross region replication
13. 6 different types of S3:
    1. **S3 standard**
    2. **S3-IA(Infrequently Accessed)**
    3. **S3 One Zone - IA**
    4. **S3 - Intelligent Tiering**
    5. **S3 Glacier**
    6. **S3 Glacier Deep Archive**
14. You can use bucket policies to make entire S3 buckets public
15. You can use S3 to host STATIC websites (such as .html)
16. Websites that require DB connections such as Wordpress etc cannot be hosted on S3

Edge Location - Location where content will be cached. This is separate to an AWS Region/AZ
Origin - This is the origin of all the files that the CDN will distribute. This can be either an S3 bucket, an EC2 instance, an Elastic Load Balancer or Route53
Distribution - This is the name given the CDN which consists of a collection of Edge Location
Web Distribution - Typicality used for Website
RTMP - Used for Media Streaming

EC2

1. It's a web service that provides resizable compute capacity in the cloud
2. Reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, with up and down, as your computing requirements change
3. Pricing models:
    1. **On Demand -** fixed rate by hour
    2. **Reserved -** capacity reservation
    3. **Spot -** bid for price
    4. **Dedicated hosts -** Physical EC2 server dedicated for your use
4. If spot instance is terminated by Amazon EC2 you will not be charge for a partial hour of usage
5. If you terminate the instance yourself you will be charged for any hour in which the instance ran
6. EC2 is compute based. It's not server less. It's a server
7. You use private key to connect to EC2

EBS

1. **SSD**
    1. General purpose SSD(GP2) - balances price and performance for a wide variety of workloads
    2. Provisioned IOPS SSD(IO1) - Highest performance SSD volume for mission critical low latency or high throughput workloads
2. **Magenetic**
    1. Throughput Optimized HDD(ST1) - Low cost HDD volume designed for frequently accessed, throughput intensive workloads
    2. Cold HDD(SC1) - Lowest cost HDD volume designed for less frequently accessed workloads(File servers)
    3. Magnetic - Previous generation

Common Ports

1. **Linux -** SSH - port 22
2. **Microsoft -** Remote desktop protocol - port 3389
3. **HTTP -** port 80
4. **HTTPS -** port 443

Roles

1. are much more secure than using access key ids and secret access keys and are easier to manage
2. You can apply roles to EC2 instances at any time. When you do this the change takes place immediately
3. Roles are universal. You do not need to specify what region they are in, similar to users

Load balancers

1. Application Load DB - Layer 7(make Intelligent Decisions)
2. Network LB - Extreme Performance/static IP Addresses
3. Classic LB - Test & Dev, Keep Costs Low

RDS(SQL/OLTP)

1. SQL
2. PostGre SQL
3. Oracle
4. Aurora
5. MariaDB

DynamoDB - NoSQL
RedShift - OLAP - BI/Data Warehousing

ElasticCache

1. Memchached
2. Redis

3. Speed up performance of existing Databases

Graph DBs - Amazon Neptune

1. Scalability
2. High Availability

RDS has 2 key features:

1. Multi AZ - for disaster recovery
2. Read Replicas - For performance

Autoscaling

1. Allows you to provision multiple EC2 instances behind a load balancer automatically depending on your demand

DNS - Domain Name System

1. Process computers use to resolve domain names to IP addresses
2. **Amazon's DNS service is called Route53**
    1. Its global, similar to IAM and S3
    2. You can use it to direct traffic all around the world
    3. You can use it to register a domain name

Elastic Beanstalk

1. You can quickly deploy and manage applications in the AWS cloud
2. You simply upload application and EBS automatically handles capacity provisioning, load balancing, scaling and application health monitoring

AWS CloudFormation

1. Similar to EBS, but if you know what you are doing in AWS unlike EBS where you're not sure about AWS environment
2. It's a service that helps you model and setup your Amazon web service Resources so that you can spend less time managing those Resources and more time focusing on you applications that run in AWS
3. You can create a template that describes all the AWS resources that you want e.g. - EC2, RDS etc
4. Takes care of provisioning and configuring those Resources for you

Differences EBS and CloudFormation -

1. Are FREE services but resources they provision are not free
2. EBS is limited to what it can provision and it is not programmable
3. CloudFormation can provision almost any AWS Service and is completely programmable

AWS Global Services

1. IAM
2. Route53

3. CloudFront
4. SNS - not available in all region
5. SES - available in all region
6. Global Views
    1. S3 - Global view but are regional

AWS Services Deployed on Premise

1. Snowball
2. Snowball Edge
3. Storage Gateway
4. CodeDeploy
5. Opsworks
6. IoT Greengrass

Which Services can be used to deploy applications On Premise:

1. CodeDeploy
2. Opsworks

CloudWatch 101

1. Used for monitoring performance
2. Can monitor most of AWS as well as your applications that run on AWQS
3. CloudWatch with EC2 will monitor events evert 5 minutes by default
4. You can have 1minute interval by turning on detailed monitoring
5. You can create cloud watch alarms which trigger notifications
6. Cloudwatch is all about performance

AWS Systems Manager

1. Allows you to manage fleets of EC2 instances and virtual machines
2. EC2 fleet - multiple instances of EC2
3. Can be both inside AWS and on premise
4. A piece of software is installed on each VM
5. Run command is used to install, patch, uninstall software
6. Integrates with CloudWatch to give you a dashboard of your entire estate

Billing & Pricing - 25-30% weightage unofficial as per exam pattern)

AWS Pricing 101

1. Fundamental principle -
    1. You pay as you go
    2. Pay for what you use
    3. Pay less as you use more
    4. Pay even less when you reserve capacity
2. White paper link - https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf
3. **Capex vs Opex**

    1. **Capex** is Capital expenditure which is where you pay upfront. Fixed, sunk cost
    2. **Opex** is Operational Expenditure which is where you pay for what you use. Utility billing - electricity, gas water etc.
4. Basic pricing policies:
    1. Pay as you go
    2. Pay less when you reserve
    3. Pay even less per unit by using more
    4. Pay even less as AWS grows
    5. Custom Pricing
5. **3 fundamental drivers of cost:**
    1. Compute
    2. Storage
    3. Data Outbound
6. **Start early with cost optimization**
7. By turning off instances you're not use, you can reduce costs by 70% or more compared to using them 24/7
8. What services are free**(resources they provision are not free):**
    1. Amazon VPC
    2. EBS
    3. CloudFormation
    4. IAM
    5. AutoScaling
    6. Opsworks
    7. Consolidated Billing
9. **What Determines Price:**
    1. Clock hours of server time
    2. Instance Type
    3. Pricing Model
    4. Number of Instances
    5. Load Balancing
    6. Detailed Monitoring
    7. Auto Scaling
    8. Elastic IP Address
    9. OS and software packages
10. **EC2 Pricing models**
    1. **On Demand**
    2. **Reserved**
    3. **Spot**
    4. **Dedicated Hosts**
11. You can use EC2 Reserved Instances to reserve capacity and receive a discount on your instance usage compared to running On-Demand instances
12. What determines Price for Lambda?
    1. **Request Pricing**
    2. **Duration Pricing**

3. **Additional Charges**
    1. Incur extra charges if your Lambda function uses other AWS Services or transfers data

13. What Determines Price for EBS

1. Volumes/GB
2. Snapshots/GB
3. Data Transfer

14. What Determines Price for S3

1. Storage Class (Standard or IA or 1 AZ IA etc)
2. Storage
3. Requests(GET, PUT, COPY)
4. Data Transfer

15. What determines Price for Glacier

1. Storage
2. Data Retrieval Times

16. **What is Snowball**

1. It is petabyte scale data transport solution that uses secure appliances to transfer large amounts of data into and out of AWS cloud

17. What determines price for Snowball

1. **Service fee per job**
    1. **Snowball 50 TB**
    2. **Snowball 80 TB**
2. **Daily Charge -** First 10 days are free, after that its $15 a day
3. **Data Transfer -** Data Transfer into S3 is free. Data transfer out is not

18. What determines price for RDS

1. Clock hours of server time
2. Database Characteristics
3. Database Purchase Type
4. Number of Database Instances
5. Provisioned Storage
6. Additional Storage
7. Requests
8. Deployment Type
9. Data transfer

19. What determines price for CloudFront

1. Traffic distribution
2. Requests
3. Data Transfer Out

AWS Budgets vs Cost Explorer (AWS console Billing Dashboard)

1. **AWS Budget**
    1. Gives you ability to set custom budget that alert you when your costs or usage exceed (or are forecasted to exceed) your budget
    2. It is used to budget costs BEFORE they have been incurred

2. **Cost Explorer**
    1. Has an easy to use interface that lets you visualize, understand and manage your AWS costs and usage over time
    2. Used to explore costs AFTER they have been incurred

Different Support Plans

1. **Basic -** Free
2. **Developer -** $29/month
3. **Business -** $100/month
4. **Enterprise -** $15000/month
5. **What level of support do you need for a Technical Account Manager(TAM)**
    1. Enterprise

Tagging & Resource Groups

1. **Tags**
    1. Key Value pairs attached to AWS Resources
    2. Metadata
    3. Tags can sometimes be inherited
2. **Resource Groups**
    1. They make it easy to group your Resources using the tags that are assigned to them
    2. You can group the Resources that share one or more tags
    3. Resource Group contain information such as
        1. **Region**
        2. **Name**
        3. **Employee ID**
        4. **Department**
    4. Using Resource Groups you can apply automation to resources tagged with specific tags. For example we stopped all EC2 instances in Stockholm Region(example)
    5. Resource Groups in combination with AWS systems manager allow you to control and execute automation against entire fleet of EC23 instances all at a push of a button
3. Tags can contain specific information such as
    1. For EC2 - Public/Private IP Addresses
    2. For ELB - Port Configurations
    3. For RDS - Database Engine etc

Consolidated Billing

1. **AWS Organizations** is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage
2. Available in 2 feature sets:
    1. Consolidated Billing
    2. All Features

3. Advantages of Consolidated Billing Include:
    1. One Bill per AWS account
    2. Very easy to track charges and allocate costs
    3. **Volume pricing discount**
4. Some best practices with AWS Organizations
    1. Always enable multi-factor authentication on root account
    2. Always use a strong and complex password on root account
    3. Paying account should be used for billing purposes only. Do not deploy resources into the paying account
5. **CloudTrail vs CloudWatch**
    1. Cloud Watch monitors performance
    2. Cloud Trail monitors API calls in the AWS platform(It is an auditing tool)
    3. CloudTrail:
        1. Per AWS account and is enabled per region
        2. Can consolidate logs using an S3 bucket:
            1. Turn on cloud trail in paying account
            2. Create a bucket policy that allows cross-account access
            3. Turn on cloud trail in the other accounts and use the bucket in the paying account

AWS QuickStart -

1. It is a way of deploying environments quickly
2. Using CloudFormation templates built by AWS solutions architects who are experts in that particular technology

AWS LandingZone -

1. AWS Landing Zone is a solution that helps customers more quickly setup a secure, multi-account AWS environment based on AWS best practices

AWS Calculators

1. **AWS Simply Monthly Calculator** - used to calculate your running costs on AWS on a per month basis. It's not a comparison tool.
2. **AWS Total Cost of Ownership Calculator** - used to compare costs of running your infrastructure on premise vs in the AWS cloud. It will generate reports that you can give to your C-level execs to make a business case to move to the cloud.

Compliance on AWS & AWS artifact - https://aws.amazon.com/compliance/

Shared Responsibility Model - https://aws.amazon.com/compliance/shared-responsibility-model/

1. While AWS manages security of the cloud, security in the cloud is the responsibility of the customer

2. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would in an on-site datacenter
3. Encryption is a shared responsibility; If you're providing your own key than it's your responsibility

AWS WAF(Web Application Firewall) & AWS Shield

AWS WAF

1. Layer 7 firewall
2. It's a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources

AWS Shield

1. It's a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS.
2. It provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS support to benefit from DDoS protection
3. There are 2 tiers of AWS Shield
    1. Standard
    2. Advanced - Cost protection covered - Reimburse related to Route53, CloudFront, and ELB DDoS charges

AWS Inspector vs AWS Trusted Advisor vs CloudTrail

AWS Inspector

1. It's an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.
2. It automatically assesses applications for vulnerabilities or deviations from best practices
3. After performing an assessment, Amazon inspector produces a detailed list of security findings privatized by level of security
4. These findings can be reviewed directly or as part of detailed assessment reports which are available via Amazon inspector console or API

AWS Trusted Advisor

1. An online resource to help you reduce cost, increase performance and improve security by optimizing your AWS environment
2. Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.
3. Advisor will advise you on Cost Optimization, Performance, Security, Fault Tolerance
4. Comes in 2 flavors
    1. Core Checks and Recommendations
    2. Full Trusted Advisor - Business and Enterprise Companies Only

AWS CloudTrail

1. It increases visibility into your user and resource activity by recording AWS Management Console actions and API calls
2. You can identify which users and accounts called AWS, the source IP address from which the calls were made and when calls occurred

AWS CloudWatch

1. It is a monitoring service to monitor your AWS resources, as well as the applications that you run on AWS
2. It monitors performance
3. Host level metrics consists of:
    1. CPU
    2. Network
    3. Disk
    4. Status check

AWS Config

1. It provides a detailed view of the configuration of AWS Resources in your AWS account.
2. This includes how the Resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time

Athena vs Macie

Athena

1. It is an interactive query service which enables you to analyze and query data located in S3 using social standard SQL
2. Server-less, nothing to provision, pay per query/per TB scanned
3. No need to set up complex ETL
4. Works directly with data stored in S3
5. What can Athena be used for:
    1. Can be used to query log files stored in S3 e.g. ELB logs, S3 access logs etc
    2. Generate business reports on data stored in S3
    3. Analyze AWS cost and usage reports
    4. Run queries on click stream data

Macie

1. **What is PII (Personally Identifiable Information)**
    1. Personal data used to establish an individual's identity
    2. This data could be exploited by criminals, used in identity theft and financial fraud
    3. Home address, email, SSN etc
2. Macie is a security service which used ML and NLP to discover, classify and protect sensitive data stored in S3
3. Uses AI to recognize if your S3 objects contain sensitive data such as PII

4. Dashboards, reporting and alerts
5. Works directly with data stored in S3
6. Can also analyze CloudTrail logs
7. Great for PCI-DSS and preventing ID theft