AWS Cloud Practitioner

Photo	
Last Edit :	@September 20, 2022 4:53 PM
Date	

So just after completing prod phase in PS, we need to do this(AWS cloud Practitioner) training.

PDF link : eVantage: AWS Cloud Practitioner Essentials 3.0.3 (EN): Student Guide (gilmoreglobal.com)

email to login : pankajkumarmath1@gmail.com

Visit here for some more

Some term

- Aggregate - a whole formed by combining several
- premises - private kind of thing
- agility - ability to move

Module 1

- ec2 is virtual server
- Cloud computing refers to the on-demand delivery of IT resources and applications through the internet
- The three cloud computing deployment models are cloud-based, on-premises, and hybrid deployments.
    1. In a cloud-based deployment model, you can migrate existing applications to the cloud, or you can design and build new applications in the cloud.
    2. On-premise infrastructure, or private cloud, is a cloud environment that is available for use only by one client
    3. In a hybrid deployment, cloud-based resources are connected to an on-premises infrastructure.
- AWS core services
    - Compute
    - Networking and Content Delivery
    - Storage
    - Database
    - Security, Identity, and Compliance
    - Management and Governance
- Benefit of cloud
    1. Variable expenses (pay only for what you use)
    2. cost optimization (focus on application and customer not on data center and other things)
    3. stop guessing capacity (scale in or scale out as per need, stop guessing about infrastructure)
    4. Benefit from massive economies of scal**e** (pay less for aggregation)
    5. speed and agility
    6. global in minute

Compute (module 2)

- EC2 - Elastic Compute Cloud
- secure, resize able compute service
- **Instance type** → When selecting an instance type, consider the specific needs of your workloads and applications. This might include requirements for compute, memory, or storage capabilities. Amazon EC2 instance types

1. **General purpose instance** → provide balance of compute, networking, memory (application server, gaming server, small and medium database, backend server)
2. **Compute optimized** → which need high processing instance (batch processing, gaming server)
3. **Memory optimized** → which need high memory preloaded for processing, process large data sets in memory. (high performance databases)
4. **Accelerated computing instances** → use hardware accelerators, or coprocessors (floating-point number calculations, graphics processing, and data pattern matching, graphics applications, game streaming, and application streaming)
5. **Storage optimized instances** → workloads that require high, sequential read and write access to large datasets on local storage. (distributed file systems, data warehousing applications, and high-frequency online transaction processing)

- **Amazon EC2 pricing**

1. **On-Demand** → are ideal for short-term, irregular workloads that cannot be interrupted. No upfront costs or minimum contracts apply. The instances run continuously until you stop them, and you pay for only the compute time you use.
2. **Amazon EC2 Savings Plans** → 1-year or 3-year term. This term commitment results in savings of up to 66% over On-Demand costs.

```
* Difference between reserved and saving plan
- To begin with, Reserved Instances are based on the commitment to use an instance at a particular price over a specific
period, while Savings Plans are based on the commitment to spend a particular dollar amount per hour over a specific
period.
```

3. **Reserved Instances** → Reserved Instances for a 1-year or 3-year term.
4. **Spot Instances** → ideal for workloads with flexible start and end times, or that can withstand interruptions. can save up to 90% as compare to on-demand pricing option.
5. **Dedicated Hosts** → are physical servers with Amazon EC2 instance capacity that is fully dedicated to your use. Dedicated Hosts are the most expensive.

- AWS auto scaling → automatically scale your aws instances according to your policies. If at some cases let suppose at any sale or any day your site may get more traffic, so you can use auto scaling to avoid service down cases.
    - dynamic scaling
    - predictive scaling

  During creation of auto scaling group, we need to define 3 things in policy. **minimum capacity**, **desired capacity** and **maximum capacity**

- Elastic load balancing

```
- A load balancer acts as a single point of contact for all incoming web traffic to your Auto Scaling group.
- Elastic Load Balancing and Amazon EC2 Auto Scaling are separate services, they work together to help ensure
that applications running in Amazon EC2 can provide high performance and availability.
```

- SNS service

```
- is a publish/subscribe service.
- use to send notification, messages to subscribers which can be web servers, email addresses, AWS Lambda functions,
or several other options.
```

- SQS service

```
- simple queue service which is used as a queue
- other service request, process and delete it from sqs.
```

cons of ec2 instance → we need to create it, upload code and manage it regularly according to our traffic. so for this reason term **serverless** came in picture.

- serverless

```
* benefit
- With serverless computing, you can focus more on innovating new products and features instead of maintaining servers.
- can adjust the applications' capacity by modifying the units of consumptions, such as throughput and memory.
- An AWS service for serverless computing is AWS Lambda.
```

- AWS Lambda

```
- you pay only for the compute time that you consume. Charges apply only when your code is running.
- You can also run code for virtually any type of application or backend service, all with zero administration.
- You can now configure your AWS Lambda functions to run up to 15 minutes per execution.
```

- **Container services** → Container orchestration services help you to deploy, manage, and scale your containerized applications.

1. ECS (Elastic container service)
    - it is a aws container services
    - Amazon ECS supports Docker containers.
    - limited to aws
    - can be used with fargate and ec2
2. EKS (Elastic Kubernetes service**)**
    - it is a aws container services
    - fully managed service that you can use to run Kubernetes on AWS.
    - open source
    - can be used with fargate and ec2

- **AWS Fargate** → It is a serverless compute engine for containers. It works with both Amazon ECS and Amazon EKS. It is limited to container only.

Global Infrastructure (module 3)

- Select a right region
    - Compliance with data governance and legal requirements
    - Proximity to your customers
    - Available services within a Region
    - Pricing
- Availability Zone

```
- An Availability Zone is a single data center or a group of data centers within a Region.
- it is inside a region.
- In a region min 2 and max 6 AZ
```

- Edge Location and Cloud Front

```
- An edge location is a site that Amazon CloudFront uses to store cached copies of your content closer to your customers for faster deliver
- CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you
the request is routed to the edge location that provides the lowest latency (time delay), so that content is delivered with the best possib
- CloudFront is a global content delivery network.
```

- Ways to interact with AWS services
    - via aws console
    - via cli

    - via software kit (SDK)
- AWS Elastic Beanstalk → With AWS Elastic Beanstalk, you provide code and configuration settings, and Elastic Beanstalk deploys the resources necessary to perform the following tasks: (quickly deploy and scale applications)
    - Adjust capacity
    - Load balancing
    - Automatic scaling
    - Application health monitoring
- AWS outpost → AWS Outposts is a family of fully managed solutions delivering AWS infrastructure and services to virtually any on-premises or edge location for a truly consistent hybrid experience. (extend aws infrastructure to your on premises data center)
- 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.

Networking (Module 4)

- **VPC** → enables you to provision an isolated section of the AWS Cloud.
- **Internet gateway** → An internet gateway is a connection between a VPC and the internet. It **allow public** traffic to access VPC.
- **Virtual private gateway (VGW)**→ A virtual private gateway enables you to establish a virtual private network (VPN) connection between your VPC and a private network, such as an on-premises data center or internal corporate network. A virtual private gateway allows traffic into the VPC only if it is coming from an approved network. To **access private** resources in a VPC, you can use a virtual private gateway
- **AWS direct connect** → is a service that enables you to establish a dedicated private connection between your data center and a VPC. It use fiber connection, and it is fast
- **Subnet** → Inside VPC, small seprate area called subnet which is collection of resources.
    - Public subnet → resources like ec2 instances should keep inside public subnet
    - Private subnet → resources like database should keep inside private subnet

```
- When a customer requests data from an application hosted in the AWS Cloud, this request is sent as a packet. A packet is a unit of data s
- 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 permission
 and how the packet is trying to communicate with the resources in a subnet.
```

- **Firewall** → control incoming and outgoing data to/from server

- **Network access control lists (NACLs)**
    - a virtual firewall that controls inbound and outbound traffic at the subnet level.
    - stateless (check permission at inbound as well as at outbound level, no state preserve)
    - allow all inbound and outbound traffic by default
- **Security groups**
    - a virtual firewall that controls inbound and outbound traffic at the instance level
    - statefull (preserve state, check at inbound level only)
    - denies all inbound traffic and allows all outbound traffic

- **DNS** (Domain name system) → You can think of DNS as being the phone book of the internet. DNS resolution is the process of translating a domain name to an IP address.
    - DNS resolution → Translating a domain name to an IP address
- **Amazon Route 53** → It is aws DNS service. 53 is tcp port.

Database and Storage (Module 5)

▼ Difference between database and storage

Storage → can store data, no structure, no query, no updation but in database we can update, modify query about data.

Block level storage, Object level storage, File storage

- **Block level storage** → OS, hard disk are using block level storage
    1. **Instance stores** → it is a block level storage which is directly attached to ec2 instances like RAM. once instance dead whole data will get erase.
    2. **Elastic Block store (EBS)** → It is also directly attached to ec2 instances but data is persistent like hard disk. If you stop or terminate an Amazon EC2 instance, all the data on the attached EBS volume remains available. both EBS and ec2 should be in same AZ.
    3. **EBS snapshot** → for incremental(means only changed data will get copy not whole) backup.
- **Object Storage** → In object storage, each object consists of data, metadata, and a key.
    1. S3(simple storage service) → a service that provides object-level storage. Amazon S3 stores data as objects in buckets. The maximum file size for an object in Amazon S3 is 5 TB.
        - classes of s3
            - **S3 standard** → good choice for a wide range of use cases, such as websites, content distribution, and data analytics. S3 Standard has a higher cost than other storage classes, Designed for frequently accessed data with high availability, Stores data in a minimum of three Availability Zones. If you haven't accessed an object for 30 consecutive days, Amazon S3 automatically moves it to the infrequent access tier, S3 Standard-IA.
            - **S3 Standard-Infrequent Access (S3 Standard-IA)** → Ideal for infrequently accessed data, Similar to S3 Standard but has a lower storage price and higher retrieval price. store data in minimum 3 AZ
            - **S3 One Zone-Infrequent Access (S3 One Zone-IA)** → Stores data in a single Availability Zone, has a lower storage price than S3 Standard-IA
            - **S3 Intelligent-Tiering** → In the S3 Intelligent-Tiering storage class, Amazon S3 monitors objects' access patterns. If you haven't accessed an object for 30 consecutive days, Amazon S3 automatically moves it to the infrequent access tier, S3 Standard-IA.
            - **S3 Glacier** → Low-cost storage designed **for data archiving**, Able to retrieve objects within a few minutes to hours.
            - **S3 Glacier Deep Archive** → Lowest-cost object storage class ideal for archiving, Able to retrieve objects within 12 hours.
- **File storage (EFS)**

```
- multiple clients (such as users, applications, servers, and so on) can access data that is stored in shared file folders.
- In this approach, a storage server uses block storage with a local file system to organize files.
- Clients access data through file paths. Compared to block storage and object storage, file storage is ideal for use cases
in which a large number of services and resources need to access the same data at the same time.
- As you add and remove files, Amazon EFS grows and shrinks automatically.
- It can scale on demand to petabytes without disrupting applications.
- as on premises can use EFS via direct cloud
```

- **RDS** → service that enables you to run relational databases in the AWS Cloud. RDS is available on six database engines
    1. Amazon Aurora → It is an enterprise-class relational database. It is compatible with MySQL and PostgreSQL relational databases. It is up to five times faster than standard MySQL databases and up to three times faster than standard PostgreSQL databases. limited to aws only
    2. PostgreSQL
    3. MySQL
    4. MariaDB
    5. Oracle Database

6. Microsoft SQL Server

- **Amazon DynamoDB** → key-value database service(NoSQL). It delivers single-digit millisecond performance at any scale. It is **serverless** and auto scaling. (10 trillion requests per day)
- **Amazon Redshift** → It is a **data warehousing service** that you can use for big data analytics
- **AWS Database Migration Service (AWS DMS)** → enables you to migrate relational databases, non-relational databases, and other types of data stores. With AWS DMS, you move data between a source database and a target database. The source and target dataset can be of the same type or different types
- **Amazon DocumentDB** → document database service that supports MongoDB workloads.
- **Amazon Neptune** → graph database(recommendation engines, fraud detection, and knowledge graphs)
- **Amazon Quantum Ledger Database (Amazon QLDB)** → to review a complete history of all the changes that have been made to your application data.
- **Amazon Managed Blockchain** → blockchain
- **Amazon ElastiCache** → adds caching layers on top of your databases to help improve the read times of common requests.
- **Amazon DynamoDB Accelerator** → an in-memory cache for DynamoDB, It helps improve response times from single-digit milliseconds to microseconds.

Security(Module 6)

- Shared responsibility model
  - customer is responsible for security in the cloud
  - aws is responsible for security of the cloud.
- **IAM** (Identity and access management)
  - **AWS account root user** → It is main account which you create in starting and It have all type of permission and access. Do not use the root user for everyday tasks. Instead, use the root user to create your first IAM user and assign it permissions to create other users.
  - **IAM users** → An **IAM user** is an identity that you create in AWS. It represents the person or application that interacts with AWS services and resources. It consists of a name and credentials. By default, when you create a new IAM user in AWS, it has no permissions associated with it
  - **IAM policies** → document having permission of resources
  - **IAM groups** → collection of IAM user.
  - IAM roles → temporary access
  - **Multi-factor authentication**
- **AWS organization** → helps you consolidate and manage multiple AWS accounts within a central location. you can centrally control permissions for the accounts in your organization by using **service control policies (SCPs).** Consolidated billing is another feature of AWS Organizations
  - **Organizational Unit(OU)** → In AWS Organizations, you can group accounts into organizational units (OUs) to make it easier to manage accounts with similar business or security requirements.
- **AWS Artifact** → a service that provides on-demand access to AWS security and compliance reports and select online agreements. AWS Artifact consists of two main sections: AWS Artifact Agreements and AWS Artifact Reports.
- **Customer Compliance Center** → contains resources to help you learn more about AWS compliance.
- **Denial-of-service attacks (DOS attack)** → hacker might flood a website or application with excessive network traffic until the targeted website or application becomes overloaded and is no longer able to respond.
- **Distributed denial-of-service attacks (DDos attack)** → DOS attack via bot or multiple source

- **AWS Shield** → AWS Shield is a service that protects applications against DDoS attacks. AWS Shield provides two levels of protection:
  - Standard → automatically protects all AWS customers at no cost. It protects your AWS resources from the most common, frequently occurring types of DDoS attacks.
  - Advanced → a paid service that provides detailed attack diagnostics and the ability to detect and mitigate sophisticated DDoS attacks. It also integrates with other services such as Amazon CloudFront, Amazon Route 53, and Elastic Load Balancing. Additionally, you can integrate AWS Shield with AWS WAF by writing custom rules to mitigate complex DDoS attacks.
- **AWS Key Management Service (AWS KMS)** → enables you to perform encryption operations through the use of cryptographic keys. You can use AWS KMS to create, manage, and use cryptographic keys.
- **AWS WAF** → **AWS WAF** is a web application firewall that lets you monitor network requests that come into your web applications.
- **Amazon Inspector** → To perform automated security assessments.
- **Amazon GuardDuty** → **Amazon GuardDuty** is a service that provides intelligent threat detection for your AWS infrastructure and resources.

Monitoring and Analytics (Module 7)

- **Amazon CloudWatch** → **Amazon CloudWatch** is a web service that enables you to monitor and manage various metrics and configure alarm actions based on data from those metrics.
- **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.
- **AWS CloudTrail** → **AWS CloudTrail** records API calls for your account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, and more.
- **CloudTrail Insights** → feature allows CloudTrail to automatically detect unusual API activities in your AWS account.
- **AWS Trusted Advisor** → **AWS Trusted Advisor** is a web service that inspects your AWS environment and provides real-time recommendations in accordance with AWS best practices.
  - cost optimization
  - performance
  - security
  - fault tolerance
  - service limits.

Pricing and Support (Module 8)

- **AWS Free Tier**
  - always free
  - 12 month free
  - Trials
- **AWS Pricing Calculator** → lets you explore AWS services and create an estimate for the cost of your use cases on AWS.
- **Consolidated billing** → The consolidated billing feature of AWS Organizations enables you to receive a single bill for all AWS accounts in your organization.
- **AWS Budgets** → The information in AWS Budgets updates three times a day. you can set custom alerts that will notify you when your service usage exceeds (or is forecasted to exceed) the amount that you have budgeted.
- **AWS Cost Explorer** → **AWS Cost Explorer** is a tool that enables you to visualize, understand, and manage your AWS costs and usage over time.
- **AWS Support** → AWS offers four different **Support plans** to help you troubleshoot issues, lower costs, and efficiently use AWS services.

1. **Basic Support** → free for all AWS customers. It includes access to whitepapers, documentation, and support communities. With Basic Support, you can also contact AWS for billing questions and service limit increases. you can use the **AWS Personal Health Dashboard (**a tool that provides alerts and remediation guidance when AWS is experiencing events that may affect you).
2. **Developer Support** → have access to features such as:
    - Best practice guidance
    - Client-side diagnostic tools
    - Building-block architecture support, which consists of guidance for how to use AWS offerings, features, and services together
3. **Business Support** → have access to additional features, including:
    - Use-case guidance to identify AWS offerings, features, and services that can best support your specific needs
    - All AWS Trusted Advisor checks
    - Limited support for third-party software, such as common operating systems and application stack components
4. **Enterprises Support** → A Technical Account Manager (TAM). TAM is your primary point of contact at AWS.

- **AWS Marketplace** → we can use third party software
- **Cloud Adoption Framework (CAF)** →
    1. Business Perspective
    2. People Perspective
    3. Governance Perspective
    4. Platform Perspective
    5. Security Perspective
    6. Operations Perspective
- **6 strategies for migration**
    1. Rehosting → Rehosting also known as “lift-and-shift” involves moving applications without changes.
    2. Replatforming → involves making a few cloud optimizations to realize a tangible benefit.
    3. Refactoring/re-architecting
    4. Repurchasing
    5. Retaining
    6. Retiring
- **AWS Snow Family members** → collection of physical devices that help to physically transport data into and out of AWS.
    1. **AWS Snowcone** → **AWS Snowcone** is a small, rugged, and secure edge computing and data transfer device. It features 2 CPUs, 4 GB of memory, and 8 TB of usable storage.
    2. **AWS Snowball** → large data migration
        a. Snowball edge storage optimized → up to 80 TB
        b. Snowball edge compute optimized → up to 42 TB(based for uses like ML)
    3. **AWS Snowmobile** → exabyte-scale data transfer service used to move large amounts of data to AWS.(up to 100 PB)