AWS Certified Cloud Practitioner Cheat Sheet Guide:

Cloud Computing:

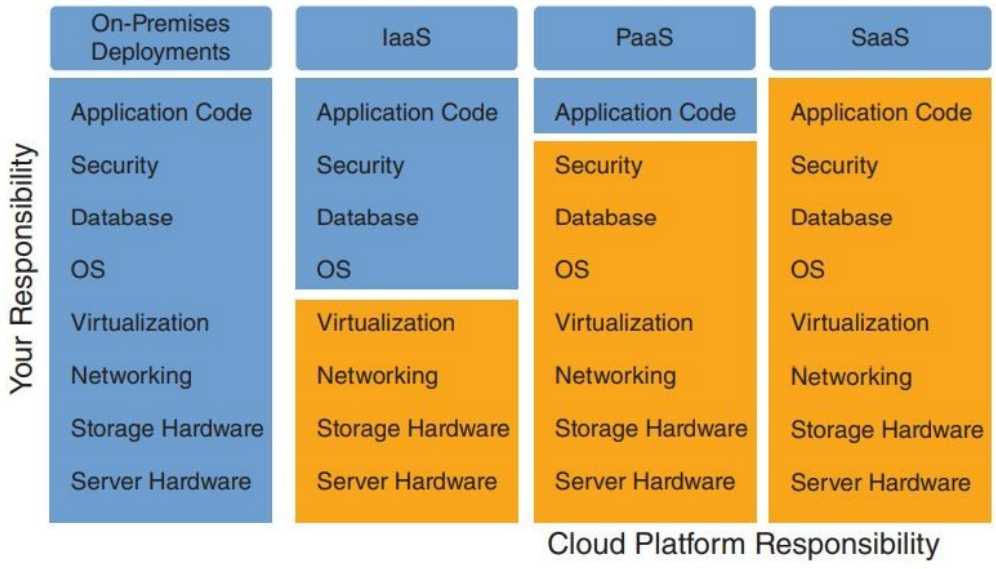
- Flexible
- Available over internet
- Little to no initial investment/Variety of resources

Before Cloud Computing:

- Host an application on a set of servers
    - Invest in physical servers and storage
    - Invest in networking
    - Build a data center
    - Invest in security
    - Invest in building and cooling
    - On-going maintenance

Types of Cloud Platform Models:

- Infrastructure-as-a-Service (IAAS):
    - Elastic Cloud Computing (EC2)
    - Elastic Block Store (EBS)
    - Elastic Load Balancing (ELB)
- Platform-as-a-Service (PaaS):
    - Elastic Beanstalk
    - Elastic Container Service (ECS)
- Software-as-a-Service (SaaS):
    - Simple Email Service
    - Amazon WorkSpaces



After Cloud Computing:

- Ability to create a virtual server on the internet
- No need to manage physical server, networking, cooling, and physical security
- No need for an initial investment
- Only pay for what you use

What is Amazon Web Services?

- On-demand cloud computing
- Subsidiary of Amazon
- Largest Cloud Services platform to date

Some AWS Services (there are over 100 services):

- Elastic Compute Cloud: Used to create virtual servers on the cloud
- Simple Storage Service: Object storage
- Relational database service: Host MySQL, Oracle, etc.
- Virtual Private Cloud: Create own isolated network on AWS

Regions & Availability Zones:

- AWS has various regions around the world that can host resources
- Your region can determine the resources you have available to you
- Use the zone that is closest to your users for efficiency purposes
- AWS resources are created in the AWS data center
- Customer is not responsible for the physical data centers
- Availability zones are replicated to various data centers for redundancy
- Regions are made of availability zones

AWS Support Plans:

- Developer: Good (Cheapest)
- Business: Better (Average)
- Enterprise: Best (Expensive)

S3 storage classes:

- Standard: Default class. Used if the object is accessed frequently
- Reduced Redundancy: Non-critical data storage. Lower cost storage, but reduced SLA (Service Level Agreement).
- STANDARD_IA & ONEZONE_IA: Infrequently accessed objects.
- Glacier & DEEP_ARCHIVE: Data archival. Storage at much lower costs

Simple Storage Service (S3) (Bucket):

- Object Level Storage

- Allows you to store and retrieve any amount of data
- Highly Scalable (Scales automatically)
- High Reliability (Automatically replicates data to another storage system)
- Versioning: Versions for modifications of objects
- S3 Bucket behaves as a static web site
- Cross Region Replication: Objects are available in other regions
- Bucket Policies manage access of objects

Amazon Glacier (Vault):

- Cold/Archive Storage
- Cheaper than S3 service
- Retain data for longer periods of times (i.e. months and years)
- To upload, must use AWS CLI or the AWS SDK (not AWS Console used in S3)
- Can upload with Lifecycle Management feature in S3 (transitions objects from bucket to vault)
- Can take 3-5 hours for object to be downloadable through standard retrieval
- Expedited retrieval costs more, but can retrieve in a matter of minutes

Virtual Private Cloud (VPC):

- Isolated Virtual Network dedicated to your AWS account
- Region Specific resource
- Isolated from other Virtual Networks
- Can launch resources such as your EC2 (Virtual Server)
- Can create multiple VPCs
- By default, AWS creates a VPC in each region when your AWS account is created
- Administrators define the subnet for segmentation

Elastic Compute Cloud (EC2):

- The ability to create a virtual server on the cloud
- Can stop/start virtual server whenever
- Can terminate on-demand servers whenever
- Host various types of workloads on server
- AMI = Amazon Machine Image (Windows, Linux) the underlying OS on the server
- Different pricing models
- Can monitor instances through Cloudwatch

Elastic Block Storage (EBS):

- Block Storage for EC2 Instances
- Different Volume types available

    - General Purpose SSD: Typical workload such as a Web Servers
    - Provisioned IOPS: More resource intensive workloads such as databases
    - Throughput Optimized HDD: Workloads that need more throughput on the volume such as Big Data applications
    - Cold HDD: Good for archive Storage
- Multiple volumes for an instance
- Can enable encryption on volumes
- Can take snapshots of volumes (Known as EBS snapshots)
- Volume can be attached to any instance in any availability zone
- EBS must be in the same availability zone that the EC2 instance is in

Costing in AWS:

- Pricing Calculator: Allows you to get an indicative pricing on hosting resources in AWS
- Billing Section: Can see the costs to date and the billing details
- Cost Explorer: Allows you to analyze your expenses, but this has to be enabled in advance

Benefits of mobbing to the cloud:

- Cost effective model
    - No need for a company to buy expensive hardware as a capital investment
- Pay-as-you-go
- Can focus on business objectives instead of worrying about infrastructure needs and costs
- As more customers begin to use AWS costs will decrease
- New services are rolled out along with updates of all services

Service Continuity (Cloud Architecting):

- Fault tolerance: If a fault occurs at the infrastructure level, the services still need to be available
- High availability: If an infrastructure goes down, ensure there are redundant implementations in place to keep the applications available
- Availability Zones: Collection of data centers
- Deploy the EC2 instances across multiple availability zones
- For higher availability: deploy secondary solutions across multiple regions for disaster recovery
- Elastic Load Balancer: Distributes traffic to underlying EC2 instances incase one instance goes down

- Always ensure that you decouple components of your application (do not have tight integrations between components to prevent domino effect of downed applications)
- Always design with failure in mind
- Use the features that AWS provide

AWS Organizations:

- Account managing and consolidating bills for master account
- Volume pricing discounts
- Service control policies at an organizational level

TCO (Total Cost of Ownership) Calculator:

- On-premises vs AWS Cloud price comparison

Cost Allocation Tags:

- Tags are used to organize resources in AWS
- Can be used to track resources at a detailed level
- You can create the cost allocation tags

AWS Trusted Advisor:

- Recommendation service within AWS
- Recommendation Categories
    - Cost Optimization
    - Performance
    - Security
    - Fault Tolerance
    - Service Limits

Elastic Load Balancer Service

- Distributes requests to the underlying EC2 Instance
- Managed Service
- Various types available in AWS

Route53

- Register domain names
- Route traffic to resources hosted in AWS
- Check health of resources
- Routing Policies:
    - Simple Routing: single resource
    - Failover Routing: Active-passive failover
    - Geolocation Routing: routes traffic based on the location of users

    - Weighted Routing: routes traffic to different resources based on a weightage

Autoscaling:

- Allows you to scale EC2 instances on demand
- Ability to create autoscaling groups
- Ability to create conditions for the scaling process

AWS Cloudfront:

- Used for effective distribution of content to users across the world
- Distributes content with the help of edge locations
- Users receive content from the closest edge location

Relational Database Service:

- Allows you to setup a relational database in AWS
- Supports MySQL, Oracle, MariaDB, PostgreSQL, and Microsoft SQL server
- Can scale the underlying instance hosting the database at any point in time
- Monitoring aspects are implemented for the database via Cloudwatch
- Enable automated backups
- Enable high availability of your database by using the Multi-AZ feature
- Multi-AZ feature: Automatically replicates primary database into another availability zone

Dynamo DB:

- Fully managed NoSQL database
- Provides better performance and scalability for underlying data
- You don't manage any infrastructure
- No configuring, just start entering your items into the table
- A table is a collection of items
- An item is a collection of attributes
- There are 2 different types of keys that are supported:
    - Simple Primary Key (Partition key): Here the value of the attribute is sent to an internal hash function. That function decides where on the physical storage the item is stored
    - Composite Key (Partition and Sort Key): If items are on the same partition, you can then decide on another key which can be used to sort the item in this partition.
- Read and write throughput is the primary usage to determine the cost aspect.
- Don't use DynamoDB as a service if you're going to perform:
    - Complex queries on the data
    - Perform table joins

AWS Lambda:

- Serverless computer service
- Does not require infrastructure maintenance
- Supports programming languages: **Node.js, Python, Ruby, Java, Go and .Net**
- Max memory for Lambda is **3GB**
- Max timeout for Lambda is **15 min**

CloudFormation:

- Spin up infrastructures in AWS via templates
- Control your infrastructure via code

Elastic Beanstalk Service:

- Allows you to quickly deploy and manage applications in AWS
- Can deploy different types of applications
- Not required to worry about the underlying infrastructure
- Supports programming languages: Node.js, Python, Java, Go and .Net
- Supports application servers such as Tomcat and the Internet Information services

Simple Queue Service:

- Hosted queue service
- Fully managed, secure, and durable
- Not required to worry about the underlying infrastructure
- Used to decouple components of a distributed application
- Two different queues: Standard & FIFO

Simple Notification Service:

- Manages the delivery of messages
- Different endpoints can subscribe to the Simple Notification service
- Consumers can receive messages via different protocols

Other AWS Services:

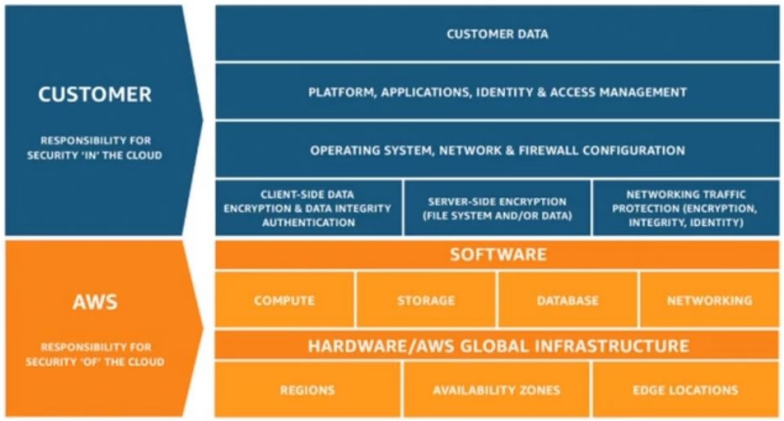
- Amazon Redshift
    - Data Warehousing service
    - Stores petabytes of data
    - Fully managed service
    - Used to create a cluster of nodes that will be used to host the data warehouse

- Amazon Kinesis

    - Collect, process, and analyze real time data
    - Data Streams: Capturing real time data; Fully managed service
    - Video streams: Securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing
    - Data Firehose: Capture, transform, and load streams of data into an AWS data stores
    - Data Analytics: Process data streams in real time with SQL & Java
- Amazon Aurora
    - Database engine with the AWS Relational Database Service
    - Compatible with MySQL and PostgreSQL
    - Delivers higher throughput than the traditional MySQL and PostgreSQL database engines
- Amazon ElastiCache
    - In-memory data store
    - Fully managed Redis and Memcached service
    - Fully manage and scalable service
    - Normally used for gaming type applications and IoT apps
- Amazon EMR (Elastic Map Reduce)
    - Serverless service
    - Run Big Data frameworks such as Apache Hadoop and Apache Spark
    - Used to process and analyze large amounts of data

Shared Responsibility Model:

- Responsibilities of AWS and Customer
- AWS:
    - The underlying physical infrastructure
    - Decommissioning of old hardware
    - Patching of firmware
    - Data Center Security
- Customer:
    - Patching of EC2 instances
    - Encryption of data at rest
    - Encryption of data in transit
    - Costing of all resources



AWS Identity and Access Management (IAM):

- Controls access to services in AWS
- You can build custom policies or use default ones
- Identities in AWS:
    - AWS Root User: Has full admin privileges in AWS
    - IAM User: Represents person or user
    - IAM Group: Used to represent a group of users
    - IAM Role: Similar to IAM user, but does not associate itself with any credentials
- Policies in IAM:
    - Policies are used to control permissions
    - Policies can be attached to users, groups or roles
    - Policies can be assigned to resources as well
- Securing access in IAM
    - Do not use root account for regular day-to-day activities
    - Enable the option of MFA for privileged users
    - Ensure users are granted only the required privileges via policies – This is known as least privilege
    - You can also use password policies

AWS Cloudwatch:

- Monitoring service within AWS
- Metrics for various services
- Can create alarms
- Can store logs within it
- Create dashboard of the various metrics
- Can create billing alarms
- Can create custom metrics
- Cloudwatch event can be used to connect to events triggered from AWS resources

AWS Cloudtrail:

- Service is used for governance and compliance perspective
- All actions taken in the AWS account are recorded by the service
- Actions take from the console CLI, SDK, and API
- Automatically enabled when an account is created

VPC and EC2 Security:

- Network Access Control Lists (Subnet Level):

    - Used to protect traffic into subnets hosted in a VPC
    - Gives and extra layer of security at the subnet/network level
    - Inbound and Outbound rules can be defined
    - Each rule can decide which protocol, port range and source to allow or deny traffic
- Security Groups (Instance Level):
    - These are associated with the Network Interfaces attached to the EC2 instances
    - These can decide what traffic can flow into and out of an EC2 instance
    - There are inbound and outbound rules that can be defined
    - Each rule can decide which protocol, port range and source

Additional Security:

- AWS Web Application Firewall:
    - Can be applied with the Application Load Balancer, Cloudfront distributions or the API gateway
    - Can create web access control lists to filter out the traffic that flows into your infrastructure
    - Can create rules to stop traffic coming from specific IP addresses
    - Can create rules to stop traffic based on a header value in the incoming request
- AWS Shield:
    - Can be used to protect against DDoS attacks
    - Is given free for some of the AWS services
    - There is an Advanced AWS Shield also that provides better support against DDoS attacks, but with an extra price
- AWS Artifact:
    - Can use this service to download AWS Secuirty and compliance documents
    - If you want AWS ISO certifications or Service Organization Control (SOC) reports, you can refer to the AWS Artifact service

Amazon Rekognition:

- Used to analyze videos and images
- Face-based user verification
- Detect unsafe content
- Can detect face in images and videos
- Search for faces in a container known as a collection
- Track paths of people detected in a stored video
- Recognize thousands of celebrities in images and stored videos
- Can detect text in images and convert it into a machine-readable text

AWS OpWorks:

- Configuration Management Service
- Allows to enforce the desired state of your infrastructure
- Allows you to integrate existing tools such as Chef and Puppet

AWS Certificate Manager:

- Service is used to generate and manage public SSL/TLS certificates for AWS websites
- Can be integrated with other AWS services such as Elastic Load Balancing, Amazon Cloudfront, and Elastic Beanstalk
- Can also import existing certificate into ACM
- Can't export a public certificate to install on your individual sites or servers

AWS Artifact:

- Provides on-demand downloads of AWS security and compliance documents
- AWS ISO certifications, Payment Card Industry (PCI), and Service Organization (SOC) reports
- Submit these to auditors who need proof that of the security and compliance of the AWS infrastructure

Personal Health Dashboard:

- Provides health events about the underlying AWS physical infrastructure
- Issues by default are categorized into open issues, scheduled changes and other notifications
- You can see all the health events that pertain to your AS account
- You can see the details of each event
- You can also setup notifications for the event via Cloudwatch rules

AWS Quicksight:

- Business Intelligence cloud service
- Used to create and publish interactive dashboards
- Can give other users access to reports
- You only pay for what you use

AWS CodeDeploy:

- Deployment Service
- Can automate deployments
- Can automate deployments to Amazon EC2 instances, on-premise instances, Lambda functions or amazon ECS services

AWS Cognito:

- Provides authentication, authorization, and user management for web and mobile applications
- Users can use this service to either directly sign in with a user name or password
- Can use third party identity providers such as Facebook or google

AWS Cloud9:

- An integrated development environment which is available on the AWS Cloud
- Can access the IDE through the web browser itself
- Can work with various programming languages such as .Net, Go, and Python
- Used mainly for writing, running, and debugging of code

AWS X-Ray:

- Service used to collect data about your request
- Tool to optimize your application
- Can be used for organization applications and AWS Lambda

AWS CloudHSM:

- Provides hardware security modules on the cloud
- HSM are devices that can be used to process cryptographic operations
- Provides secure storage for cryptographic keys