re **Cloud & Value Proposition**

Introduction

Cloud Computing - On-demand delivery of compute power, database, storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing. Cloud computing provides a simple way to access servers, storage, databases, and a broad set of application services over the internet. A cloud services platform … owns and maintains the network-connected hardware required for these application services, while you provision and use what you need via a web application

Cloud Computing Service Types

1. Infrastructure as a Service (IaaS)
    a. Provides basic components for cloud info technology
    b. Usually offers access to networking infrastructure, virtual or dedicated server computing, and data storage space
    c. Delivers maximum amount of elasticity and flexibility and control
   EX: Virtual Private Clouds (VPC)
    - Provision of isolated portion of AWS Cloud
2. Platform as a Service (PaaS)
    a. Eliminates the need for enterprises to manage underlying development infrastructure
    b. Some services are more managed by AWS than others
   EX: Amazon Lightsail
    - Offers everything needed to build an application or website, including virtual servers, storage, databases, and networking
3. Software as a Service (SaaS)
    a. Offers consumer a finished product that is run and managed entirely by the service provider
   EX: Web-based email, Cloud storage

Cloud Computing Deployment Models

1. Cloud-Based
    a. Fully deployed in AWS Cloud
2. Hybrid
    a. Method for connecting infrastructure and applications between AWS cloud-based resources and other resources that are not placed in the cloud

    b. Can be used to migrate, expand, or grow an organization’s infrastructure into a cloud solution while linking internal systems to AWS Cloud resources

  EX: AWS Outposts

    - Fully managed to compute and storage hardware built with prototypical AWS-designed solutions
    - Extends AWS services to consumer data centers

3. On-premises (Private cloud deployment)
    a. Uses virtualization and resource management tools on-site only

Core Services

1. Compute
    a. Server-Based (Linux and Windows)
    b. Serverless (AWS Lambda, AWS Fargate)
2. Networking & CDN (Content Delivery Network)
    a. IaaS
3. Storage
    a. Block Storage: Hard Disk and SSD
    b. Object Storage: Amazon S3
4. Database
    a. Structured Relational: MySQL
    b. Document Style: No SQL

Value Propositions

1. Agility/Flexibility
    a. Agile development and project management
    b. Rapid deployment, testing, experimentation, and innovation
    c. Overcoming geographical limitations
    d. Reducing time and cost for testing and experimentation
2. Elasticity
    a. Ability to almost instantly provision and de-provision resources
    b. Auto-scaling technologies
3. Cost
    a. Save on infrastructure devices, servers, racks, cablings, maintenance, labor, facilities, and databases and storage
4. Security

Cloud Economics

Free Tier Model

1. 12 Months Free
    a. If usage exceeds limits, pay-as-you-go rates apply
    EX: 750 hrs/month of Windows t2.micro and Linux t2.micro
    25 GB of Amazon DB Storage
2. Always Free
    a. AWS Shield
    b. Health Dashboard
3. Free Trials

Pricing Models

1. Pay as you go
    a. Only pay for specific services that you need and only for the time you are utilizing them
    b. Easily adapt to changing business needs
2. Save when you reserve
    a. AWS offers reserved instances for EC2 and RDS among others
    b. Higher upfront fee, but better discount
3. Pay less when you use more
    a. Use managed services
    b. Volume-based discounts
    c. S3 tier-based pricing

AWS TCO Calculator (Total Cost of Ownership)

- Now called AWS Pricing Calculator
- Estimates cost of architecture solution
- Enter services and configurations, and get estimates

AWS Cost Calendar

- Now called Cost Explorer
- Give preconfigured view of spending scenarios
- Customizable

Cloud Architecture Design Principles

Virtualization

1. Hypervisors

    a. Software that products and manages virtual infrastructure, allowing multiple operating systems to run and share resources
    b. The host system runs hypervisor (needs lots of computing power)
    c. The guest system runs virtual machines
        i. Native Hypervisor (Bare Metal)
        ii. Type 2 Hypervisor

Shared Responsibility Model

1. AWS functions manages and controls mechanisms from the host operating system and virtualization layer down to physical security of data center facility
2. The consumer takes responsibility for managing the guest operating system

Risk Treatment

1. Reduction
2. Acceptance
3. Avoidance
4. Transference

Managing Root Account

- Rotate access keys regularly

Root Account

- Change support plan, payment options, and billing
- Close an account

Virtual Private Cloud (VPC)

- Default VPC
- Non-Default VPC

Amazon Machine Image (AMIs)

- Template that contains software configuration required to launch instance
- (Infrastructure as a Service)

Networking in AWS

- Subnets for each available region
- Private Subnet
- VPN Subnet
- Public Subnet

- Internet gateways allow traffic in and out of VPC and translate private IP addresses to public ones
- NAT Gateway is a secure way for a private subnet to access the internet (Uses Elastic IP Addresses) (iPv4)
- Egress Only Internet Gateways (iPv6)
- Endpoints (Doesn't use internet, directly connects to service)
    - Gateway: Used to access instance in VPC to DynamoDB or store in S3
    - Interface: Logical network interface (Uses private IP address)
- Peering Connections - Connect VPCs to each other

Connectivity Options

- Customer Gateways
- Virtual Private Gateways

Cloud Security & Compliance

AWS Artifact

- Console based, on-demand self-service auditing object retrieval service, offers quick and easy access to AWS compliance documentation and agreements
- Contains compliance documentation
- CSA Star Level 1, 2, and 3

Access Management

IAM Password Policies

- Establish password policy
- Grant least privilege access
- Groups and Users (Programmatic access, AWS Management Console access)

IAM Managed Policy

- Can be applied to groups or roles
- Up to 10 managed policy to entity

IAM Roles

- Identity that has permission assigned
- Assumed by user
- No long term credentials (temporary)

Bastion (Jump Hosts)

- Bastion host is a system whose goal is to offer secure access to a private network from external network like the internet
- AppStream 2.0 (Creates and terminates instances when access)

AWS Cognito

- Provides user pools and identity pools
- Sign in service

Security Support Resources

Network ACLs

- Inbound/Outbound rules
- Checks each packet

Security Groups

- Applies to all traffic inbound and outbound from specific instance
- List of rules for each instance

Web Application Firewall (WAF)

- Lets you control and monitor HTTP and HTTPS requests forwarded to Amazon CloudFront, ELB, or API Gateway
- Permissive: Allows all requests made through WAF except for specific ones
- Restrictive: Blocks all requests except specific ones
- Counting: Counts requests that match properties specified

AWS Shield

- Dos and DDos protection
- AWS Shield Advanced (Expanded protection)

Amazon Inspector

- Assessment tool that enhances security and compliance of applications running on AWS

Amazon GuardDuty

- Fully managed threat detection service
- Look for attacks, anomalies, and unauthorized actions

AWS Key Management Service (KMS)

- Symmetric
- Asymmetric

Cloud Deployment & Operation

Auto Scaling and ELB

- Auto Scaling Group (Minimum, desired capacity, maximum size)
- ELB automatically dispenses incoming traffic across several targets
- Application Load Balancer: HTTP and HTTPS traffic
- Network Load Balancer: TCP, UDP, and TLS traffic routing traffic to VPS
- Classic Load Balancer

EBS and Instance Store

- EBS is a permanent store
- Instance store is for temporary work, disappears when instance disappears
- Minimum size is 1 GB

JSON

- JavaScript Object Notation
- Object
- Array

AWS CloudFormation

- Configuration in simple text file
- Infrastructure as code
- Common language to templatize cloud environment

AWS CloudFront

- Fast content delivery networking service
- Securely delivers data with low latency

Core Services

Amazon EC2

- Amazon EC2: Service that offers secure, resizable compute capacity to consumers in the cloud (Uses AMIs)
- On-demand instances: Default type where customers pay for compute capacity by hour
- Reserved Instances: Discount by paying all upfront or partial upfront
- Spot Instances: Allows consumers to bid on spare Amazon EC2 computing capacity based on spot price

Containers

- Delivers standardized method for packaging an application’s code, configurations, and dependencies into single modular and portable object

Lightsail

- One of the quickest and easiest methods for launching and managing virtual private web server
- Can use CloudFront
- Offers Virtual Machine, SSD storage, Data transfer, DNS Management, static IP address

Elastic Beanstalk

- Platform as a service offering deploying, monitoring, and scaling web applications and services developed on a variety of platforms and applications

AWS Lambda

- Function as a service
- Serverless run code

Amazon Elastic Container Registry

- Fully managed docker container registry that makes it simple for application developers to store, manage, and deploy docker container images
- Integrated with ECS

Amazon S3 Glacier

- Long-term archival storage (Vaults: Container for storing archives)

AWS Storage Gateway

- Service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration

AWS Snow Family

- Transfer large amounts of data
- Snowcones, snowballs, snow mobiles

Elastic File System (EFS)

- Scalable shared file system for Linux

Security Fundamentals

- Bucket Policies (JSON documents)
- Access Control Lists (ACL)

Amazon Aurora

- Fully managed MySQL and PostgreSQL relational database engine

Technology Support Resources

- AWS Support Plans
  - Developer, Business, Enterprise
- AWS Trusted Advisor
  - Cost optimization, Security, Fault tolerance, Performance, Service limits

AWS CloudTrail

- Managed service that empowers governance, compliance, operational auditing, and risk auditing of AWS accounts
- Logging, monitoring, preserving account activity
- Compliance assistance, Tracking resource lifecycles, Troubleshooting AWS operations, performing security analytics

AWS CloudWatch

- Management and monitoring
- Logs

AWS Organizations

- Centrally manage your environment as you scale and evolve AWS workloads
- Share resources across AWS accounts
- Programmatically generate new AWS accounts

Questions

Under the shared responsibility model, which of the following is the customer responsible for?

- Ensuring that data is encrypted at rest.

What AWS team assists customers with accelerating cloud adoption through paid engagements in any of several specialty practice areas?

- AWS Professional Services

A customer would like to design and build a new workload on AWS Cloud but does not have the AWS-related software technical expertise in-house. Which of the following AWS programs can a customer take advantage of to achieve that outcome?

- AWS Partner Network Consulting Partners

Which AWS services can host a Microsoft SQL Server database?

- Amazon EC2
- Amazon Relational Database Service (Amazon RDS)
    - Collection of managed services that makes it simple to set up, operate, and scale databases in the cloud

Which of the following Amazon EC2 pricing models allow customers to use existing server-bound software licenses?

- Dedicated Host

Cost Allocation Tags - AWS Cost Allocation Tags are labels that you can assign to any applicable AWS resource.

Consolidated billing is the method of combining multiple subscriptions of a customer into a single invoice
Which of the following are advantages of AWS consolidated billing?

- Potential volume discounts, as usage in all accounts is combined

What costs are included when comparing AWS Total Cost of Ownership (TCO) with on-premises TCO?

- On premises Security

Convertible RIs: These provide a discount (up to 54% off On-Demand) and the capability to change the attributes of the RI as long as the exchange results in the creation of Reserved Instances of equal or greater value. Like Standard RIs, Convertible RIs are best suited for steady-state usage.

According to best practices, how should an application be designed to run in the AWS Cloud?

- Use loosely coupled components.
- As application complexity increases, a desirable attribute of an IT system is that it can be broken into smaller, loosely coupled components. This means that IT systems should be designed in a way that reduces interdependencies—a change or a failure in one component should not cascade to other components.

AWS RedShift - Data warehouse product which forms part of the larger cloud-computing platform Amazon Web Services.

High Availability is synonymous to failure and recovery. This is the keyword in the question which is only complemented by applications can absorb failures in one instance by handing over to another instance or more.

AWS supports which of the following methods to add security to Identity and Access Management (IAM) users?

- Using Multi-Factor Authentication (MFA)
- Enforcing password strength and expiration

Which of the following components of the AWS Global Infrastructure consists of one or more discrete data centers interconnected through low latency links?

- Availability Zone

One of the advantages to moving infrastructure from an on-premises data center to the AWS Cloud is:

- Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking, and powering servers.
- it allows the business to focus on business activities

What is the lowest-cost, durable storage option for retaining database backups for immediate retrieval?

- S3

Amazon DynamoDB is a fully managed proprietary NoSQL database service that supports key–value and document data structure

What approach to transcoding a large number of individual video files adheres to AWS architecture principles?

- Using many instances in parallel

Which of the following is the customer's responsibility under the AWS shared responsibility model?

- Patching Amazon EC2 instances

Which of the following are features of Amazon CloudWatch Logs?

- Real-time monitoring
- Adjustable retention

Which of the following AWS Cloud services can be used to run a customer-managed relational database?

- Amazon EC2

Amazon Kinesis Data Streams is a serverless streaming data service that makes it easy to capture, process, and store data streams at any scale.

Which of the following AWS services can be used to serve large amounts of online video content with the lowest possible latency

- Amazon S3
- Amazon CloudFront

What is the benefit of using AWS managed services, such as Amazon ElastiCache and Amazon Relational Database Service (Amazon RDS)?

- They have better performance than customer-managed services.

Under the shared responsibility model, which of the following is a shared control between a customer and AWS?

- Patch management

Which AWS service allows companies to connect an Amazon VPC to an on-premises data center?

- AWS VPN

Which AWS service provides alerts when an AWS event may impact a company's AWS resources?

- AWS Personal Health Dashboard

Which task is AWS responsible for in the shared responsibility model for security and compliance?

- Updating Amazon EC2 host firmware

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.

Which of the following services could be used to deploy an application to servers running on-premises?

- AWS OpsWorks
- AWS CodeDeploy

Which is the MINIMUM AWS Support plan that allows for one-hour target response time for support cases?

- Business

How would an AWS customer easily apply common access controls to a large set of users?

- Apply an IAM policy to an IAM group

A company is migrating an application that is running non-interruptible workloads for a three-year time frame.
Which pricing construct would provide the MOST cost-effective solution?

- Amazon EC2 Reserved Instances

Which AWS Cost Management tool allows you to view the most granular data about your AWS bill?

- AWS Cost and Usage report

Which of the following can an AWS customer use to launch a new Amazon Relational Database Service (Amazon RDS) cluster?

- AWS Management Console

- AWS CloudFomation

AWS Storage Gateway is a hybrid cloud storage service that gives you on-premises access to virtually unlimited cloud storage. Customers use Storage Gateway to simplify storage management and reduce costs for key hybrid cloud storage use cases.

Which options does AWS make available for customers who want to learn about security in the cloud in an instructor-led setting?

- AWS Online Tech Talks
- AWS Classroom Training

Which of the following features can be configured through the Amazon Virtual Private Cloud (Amazon VPC) Dashboard?

- Security Groups
- Subnets

How do customers benefit from Amazon's massive economies of scale?

- Periodic price reductions as the result of Amazon's operational efficiencies

Which of the following common IT tasks can AWS cover to free up company IT resources?

- Patching databases software
- Backing up databases

Which is the minimum AWS Support plan that includes Infrastructure Event Management without additional costs?

- Enterprise

How does AWS shorten the time to provision IT resources?

- It provides the ability to programmatically provision existing resources.

What can AWS edge locations be used for?

- Reducing traffic on the server by caching responses

Which is the MINIMUM AWS Support plan that provides technical support through phone calls?

- Business

An administrator needs to rapidly deploy a popular IT solution and start using it immediately.
Where can the administrator find assistance?

- AWS Quick Start reference deployments

Which of the following can a customer use to enable single sign-on (SSO) to the AWS Console?

- AWS Directory Service

What function do security groups serve related to Amazon Elastic Compute Cloud (Amazon EC2) instance security?

- Act as a virtual firewall for the Amazon EC2 instance.

How is asset management on AWS easier than asset management in a physical data center?

- AWS performs infrastructure discovery scans on the customer's behalf.

What feature of Amazon RDS helps to create globally redundant databases?

- Cross-Region read replicas

AWS Direct Connect is a network service that provides an alternative to using the Internet to utilize AWS cloud services.

What is the MINIMUM AWS Support plan that provides designated Technical Account Managers?

- Enterprise

AWS CodeCommit is a version control service hosted by Amazon Web Services that you can use to privately store and manage assets (such as documents, source code, and binary files) in the cloud.

Which of the following services have Distributed Denial of Service (DDoS) mitigation features? (Choose two.)

- Amazon CloudFront
- Amazon WAF

Which AWS tool will identify security groups that grant unrestricted Internet access to a limited list of ports?

- AWS Trusted Advisor

Which services use AWS edge locations?

- AWS Shield

According to the AWS shared responsibility model, who is responsible for configuration management

- It is shared between AWS and the customer.

A user is running an application on AWS and notices that one or more AWS-owned IP addresses is involved in a distributed denial-of-service (DDoS) attack.
Who should the user contact FIRST about this situation?

- AWS Abuse Team

Pillars of AWS Well-Architected Framework
1- Operational excellence
2- Security
3- Reliability
4- Performance efficiency
5- Cost optimization

Amazon Athena is a serverless, interactive query service to query data and analyze big data in Amazon S3 using standard SQL.

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

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage service

AWS Global Accelerator combines advanced networking features with the dedicated AWS Global Network to improve your application network performance by up to 60%.

AWS Budgets - send an alert when the utilization of Reserved Instances drops below a certain percentage, simplest way to monitor your AWS spend and be alerted when you exceed or are forecasted to exceed your desired spending limit.

The AWS Trusted Advisor checks include recommendations regarding which of the following? (Choose two.)

- Information on Amazon S3 bucket permissions
- Multi-factor authentication enabled on the AWS account root user

A company is launching an ecommerce application that must always be available. The application will run on Amazon EC2 instances continuously for the next
12 months.
What is the MOST cost-effective instance purchasing option that meets these requirements?

- Savings Plan

A VPC can span all Availability Zones within an AWS Region.

AWS Enterprise Support

- Support of third-party software integration to AWS

Economy of Scale

- Proprotionate saving in costs gained by increased level of production

Network ACLS

- They process rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic.
- They are stateless.

AWS IAM Access Analyzer

AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub

Which AWS service supports the creation of visual reports from AWS Cost and Usage Report data?

- Amazon Quicksight

AWS Local Zones (Similar to edge locations)

Amazon AppStream 2.0 is a fully managed application streaming service that provides users with instant access to their desktop applications from anywhere

AWS Snowball Edge - Remote locations

Amazon Elastic Transcoder

Pricing Calculator - Estimates and anticipations