AWS Solution Architect Associate

Version : C03

Domain 4

Task 4

Design cost-optimized network architectures

NAT Instance Vs NAT Gateway Costs

Feature	NAT Instance	NAT Gateway
Hourly Usage Cost	Depends upon the EC2 instance type	Fixed Rate
Data Processing Cost	Included in Instance Cost	Fixed Rate
High Availability	Requires Manual setup of multiple instances	Built-In high availability
Performance	Depends on instance type and configuration	Scales automatically to handle traffic
Management overhead	Requires maintenance and management of EC2 instances	Fully Managed service , Minimal Overhead

Network Connectivity

AWS offers a variety of network connectivity options to meet different workload requirements and integration needs. These options include :

- **Amazon VPC** : Allows you to create a private, isolated section of the AWS cloud where you can launch AWS resources in a virtual network you define
- **VPC Peering** : Enables connectivity between two VPCs using private IP addresses, making it simple to route traffic between them
- **AWS Direct Connect** : Provides a dedicated network connection from your premises to AWS, enhancing network performance and security
- **VPN Connections** : Allows secure connections from on-premises networks to AWS VPCs via encrypted VPN tunnels over the internet
- **Transit Gateway** : Acts as a hub that controls how traffic is routed among all the connected networks, simplifying network architecture and management

Network Routing, Topology and Peering

Network Routing in AWS

- **VPC Peering**
  - AWS offers Virtual Private Cloud (VPC) peering, enabling communication between VPCs within the same or different AWS regions
- **AWS Transit Gateway**
  - It facilitates routing between multiple VPCs and VPNs. It's a highly scalable and centralized solution for routing traffic within AWS
- **Network Peering Policy**
  - AWS has specific policies for parties interested in peering with Amazon's AS16509 network and its downstream networks on a settlement-free basis
- **AWS Network Firewall Deployment**
  - Different deployment models exist for AWS Network Firewall, which can be integrated with VPC routing enhancements for enhanced security and routing control
- **VPC Peering Diagram**
  - Visual representations, like the AWS VPC peering diagram by Hava, can help understand the routing architecture and connections within AWS VPCs

Network Routing, Topology and Peering

Network Topology in AWS

- **Planning Network Topology**
  - When designing systems in AWS, planning network topology is crucial.
  - Involves architecting IP address-based networks to facilitate launch of resources in a virtual network
- **AWS Network Topology Diagram**
  - Visual representations like AWS Network Topology Diagram provides an overview of the network architecture within AWS, illustrating connections, components and their relationships
- **Visualizing Global Networks**
  - AWS Cloud WAN enable users to understand the connectivity and topology of their networks
- **Amazon EC2 Instance Topology**
  - Understanding instance topology provides insight into the physical placement of EC2 instances within the AWS infrastructure, offering a hierarchical view of their host placement
- **AWS Cloud Topologies**
  - Different cloud topologies exist in AWS, addressing various architectural needs
  - Topologies outline how AWS resources and services can be structured to meet specific requirements

Network Routing, Topology and Peering

Network Peering in AWS

- **VPC Peering Connection**
  - It's a networking connection between two Virtual Private Clouds (VPCs) in AWS
  - This enables routing of traffic between them using private IPv4 or IPv6 addresses
- **Creation**
  - To establish VPC peering, configure the necessary information including the VPC IDs and optionally assign a name to the connection.
  - After configuration, initiate the creation process in the AWS Management Console
- **Functionality**
  - Peered VPCs can communicate with each other as if they are on the same network, allowing the exchange of traffic privately.
  - However, the traffic remains within the AWS network and doesn't traverse the public internet
- **Global Routes**
  - When peering with AWS, peers can receive all global routes, enhancing connectivity and enabling efficient traffic routing within AWS infrastructure

Appropriate Network Connections

- **Latency Requirements**
  - If low-latency performance is crucial, consider options like AWS Direct Connect or AWS Transit Gateway
- **Security**
  - Prioritize secure connections by choosing options that provide private and encrypted network traffic, such as AWS VPN
- **Scalability**
  - For scalable and efficient network management across distributed AWS environments, AWS Transit Gateway offers automation and visualization capabilities
- **Flexibility**
  - Evaluate options based on your network design and requirements, as AWS offers multiple connectivity options tailored to different use cases

Network Services with usecases

- **Amazon VPC (Virtual Private Cloud)**
  - Virtual network with complete control over IP addressing, subnets, route tables and network gateways
  - Useful for hosting scalable, highly available applications securely
  - Commonly used for VPN connections
- **AWS Direct Connect**
  - Establish a dedicated network connection from on-premises to AWS
  - Ideal for large data transfers, consistent network performance and hybrid cloud architectures
- **Amazon CloudFront**
  - Deliver content, videos, applications and APIs globally with low latency and high transfer speeds
  - Ideal for websites and applications requiring fast and secure content delivery
- **Amazon Route 53**
  - Scalable DNS (Domain Name System) service
  - Useful for routing end users to internet applications by translating human-readable domain names into IP addresses
  - Beneficial for managing domain registration, DNS routing, and health checks
- **AWS PrivateLink**
  - Access services hosted on AWS privately, without exposing data to the public internet
  - Ideal for secure communication between VPCs, VPNs and on-premises networks

Appropriate Network Routes

To minimize network transfer costs, consider the following network routes :

- **Region to Region** - Utilize inter-region data transfer mechanisms provided by cloud service providers like AWS or Azure. This may involve setting up direct connections between regions or using services optimized for inter-region data transfer
- **Availability Zone to Availability Zone** - Leverage intra-region data transfer within Availability Zones. This ensures low-latency and cost-effective communication between resources deployed in different zones within the same region
- **Private to Public** - Establish private connections, such as AWS Direct Connect or Azure ExpressRoute, to connect on-premises infrastructure directly to cloud environments. Use private IP addresses and avoid data transfer over the public internet to minimize costs
- **Global Accelerator** - Implement a global accelerator service to improve the availability and performance of your applications. This service optimizes the path and routes traffic through the AWS global network, reducing latency and data transfer costs
- **VPC Endpoints** - Utilize VPC endpoints to privately connect your VPC to supported AWS services without traversing the internet. This minimizes data transfer costs associated with public data transfer and enhances security by keeping traffic within the AWS network

Strategic Needs for CDN's

Considering the following steps ,Strategic needs for CDNs and edge caching can be determined -

- **Analyze Website Traffic** : Evaluate website traffic patterns to identify regions with high user concentration
- **Assess Latency** : Determine regions experiencing high latency to prioritize CDN placement for faster content delivery
- **Content Type** : CDN caching is ideal for static content, while dynamic caching or edge computing is best for dynamic content
- **Security Requirements** : Consider security needs. CDNs often include DDoS protection and SSL termination
- **Cost Analysis** : Evaluate the cost of CDN services versus potential savings in bandwidth and server load
- **Scalability** : Assess scalability requirements to ensure CDN services can accommodate future growth
- **Monitoring and Optimization** : Continuous monitoring and optimization ensures CDN and caching strategies remains effective
- **Resilience** : Redundancy and failover mechanisms ensures service continuity in case of CDN or edge caching failures

Throttling Strategy

AWS implements throttling across various services to manage API request rates and ensure system stability -

- **API Gateway Throttling**
  - AWS API Gateway offers throttling settings to control request rates, including account-level and per-API throttling
  - Throttling limits are applied at both account and client levels within a region
- **HTTP API Throttling**
  - AWS API Gateway provides throttling capabilities for HTTP APIs, including account-level throttling per region to manage steady-state requests per second (RPS)
- **AWS Lambda Throttling**
  - AWS Lambda applies throttling to manage concurrent executions and prevent resource exhaustion
- **Amazon EC2 API Throttling**
  - Amazon EC2 throttles API requests per AWS account on a per-region basis to enhance service performance and ensure fairness

Implementing throttling strategies in AWS helps maintain system stability, prevents overloading, and ensures fair resource allocation across various services

Single\Multiple VPNs & Direct Connect Speeds

Single VPN vs. Multiple VPNs :

- **Single VPN**
  - Suitable for individual users or small-scale applications where simplicity and cost-effectiveness are prioritized
- **Multiple VPNs**
  - Ideal for larger organizations needing separate VPN connections for various purposes, providing better segmentation and security
  - Good for where more number of resources are required

Direct Connect Speed :

- 1 Gbps, 10 Gbps, 100 Gbps
- Offered by AWS Direct Connect
- Cater to different needs and scales of operations with higher speeds suitable for demanding workloads and large data transfers

AWS Solution Architect Associate

Version : C03

Domain 4

Task 4

The END