Gujarati Dharmi

CWID - 20018001

CS 524-A Introduction to Cloud computing – Homework #3

Answer 1.

- We must calculate the maximum number of tokens that can accumulate in the token bucket in order to establish the maximum burst duration T. The number of tokens that can be used at once is equal to token bucket size b. R bytes/sec is the pace at which tokens are added to the bucket. Therefore, b/r seconds are needed to fill the bucket.
- At the maximum output rate of M bytes/sec, the maximum burst time T is the amount of time needed to empty the bucket. The formula for this is T = b/ (M - r).
- The token bucket will never full up and there won't be any tokens available for bursts if the maximum output rate M exceeds the token rate r.
- New tokens are added at the rate of r bytes/sec which is 2Mbps in the given question. Capacity of the token bucket (b) = 16 M bits Maximum possible transmission rate (M) = 10Mbps.
- So, the maximum burst time = b/ (M-r) = 16/ (10-2) = 2 seconds.

Answer 2. A)

- I would think about selecting an AWS Direct Connect Partner to link my company's data center in Sapporo, Japan, to the Amazon service. In internet-based connections, AWS Direct Connect Partners offer dedicated network connections between customer locations and AWS, which can help to lower network costs, enhance bandwidth and provide more reliable network experience. I'll select locations that give more profits to my company.

  [**Source:** https://aws.amazon.com/directconnect/locations/?nc=sn&loc=4&dn=3]

- I would start by going to the AWS Direct Connect pricing page on the AWS website to learn more about pricing and QoS guarantees. Port hours, connection capacity and data transfer out (DTO) carried over the connection that affects how much AWS Direct Connect costs. Pricing is often determined by a usage-based data transmission fee in addition to a fixed port fee. Customers that require higher bandwidth connections or who want to connect to several AWS regions have a variety of alternatives from AWS as well. Although the service is intended to offer high dependability and low latency, AWS does not explicitly provide guarantees for the quality of service for AWS Direct Connect. Customers are advised to use their AWS Direct, according to AWS.

[**Source:** https://aws.amazon.com/directconnect/pricing/]

2. B)

- The IEEE standard 802.1q, which governs networking and specifies virtual LANs (VLANs) function on Ethernet networks. A single physical network can support several VLANs, each of which is identifiable by a different VLAN ID, thanks to the standard. This standard is used by the AWS Direct Connect service to let users divide a dedicated connection into various virtual interfaces, each with a unique VLAN ID.
- Customers can now access both public and private resources, such as Amazon EC2 instances running inside an Amazon Virtual Private Cloud (VPC) and objects stored in Amazon S3, using the same connection and public IP address space. This allows you to use the same connection to access public resources such as objects stored in Amazon S3 using public IP address space, and private resources such as Amazon EC2 instances running within an Amazon Virtual Private Cloud (VPC) using private IP space while maintaining network separation between the public and private environments. Virtual interfaces can be reconfigured at any time to meet our changing needs.

[**Source:** https://www.datacenters.com/]

Answer 3.

- To create a private network link using AWS Direct Connect and Amazon Virtual Private Cloud (VPC), establish a dedicated connection from an on-premises network to one or more VPCs in the same region. Using private VIF on AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or collocation environment. Multiple dynamically routed AWS Direct Connect connections are necessary to support high availability. Since Direct

Connect avoids using the public internet, it is more dependable, secure and economical than connecting over the internet for data transmission between on-premises and VPC settings.

- Here is the steps for connectivity of Amazon VPC and AWS Direct Connect:
  1) A dedicated network connection must first be made between the on-premises environment and the AWS Direct Connect location.
  2) Construct a virtual interface, on the AWS side of the connection connected to the Amazon VPC, then create a virtual interface. Traffic will be able to move between the on-premises environment and the Amazon VPC thanks to this virtual interface.
  3) Set up the virtual interface: Set up the virtual interface to correspond to the Amazon VPC's IP address range. Traffic between the on-premises environment and the VPC will be able to flow as a result.
  4) Utilize the virtual interface: After the virtual interface has been set up, Direct Connect traffic can be used to send and receive data to and from the Amazon VPC. Customers can now use private IP addresses to access their Amazon VPC resources, exactly as they would if they were on-premises.

- Customers can build a hybrid environment that combines the scalability and flexibility of Amazon's cloud services with the security and control of a private network by combining AWS Direct Connect with Amazon VPC. Customers may develop hybrid architectures, shift apps to the cloud, and lower their overall network expenses thanks to this.

Answer 4. A)

- NAT gateway is a Network Address Translation(NAT) service. We can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances. It enables instances within the VPC to communicate with the internet while yet retaining a private IP address space. As it keeps the VPC separate from the general internet while yet enabling access to some resources, this can be advantageous for security and control reasons.

- The NAT gateway replaces the source IP address of the instances with the IP address of the NAT gateway. For a public NAT gateway, this is the elastic IP address of the NAT gateway. For a private NAT gateway, this is the private IPv4 address of the NAT gateway. When sending response traffic to the instances, the NAT device translates the addresses back to the original source IP address.
- However, NAT might not always be required. For instance, if all of the resources in the VPC are internal, then do not require connectivity to the public internet. We can use a public NAT gateway to connect to other VPCs or your on-premises network. In this case, we route traffic from the NAT gateway through a transit gateway or a virtual private gateway.

4. B)

- The maximum number of connections that a single NAT box can support varies depending on a number of variables, including the amount of CPU and memory that is available, the kind of network traffic being used (e.g., TCP or UDP), and the number of concurrent connections.
- The maximum number of connections per NAT instance is 65,536 for TCP and UDP traffic and 32,000 for SCTP traffic, according to the AWS documentation. It's crucial to remember that this restriction can change depending on the size of the instance, network traffic patterns, and other elements.

Answer 5. A)

- Border Gateway Protocol (BGP) is used by AWS Direct Connect to learn the IP address ranges that are published by AWS and to broadcast the customer's IP address range to AWS. To establish the routing between the customer's network and the AWS VPC, this is required.

5. B)

- Yes, a client may connect to an AWS VPC using their own Autonomous System Number (ASN), provided that the ASN is registered with an RIR and that the customer possesses the tools and resources required implementing BGP peering with AWS. This number is used in both the exchange of exterior routing information and as an identifier of the AS itself.

5. C)

- The Asia Pacific Network Information Centre (APNIC) is the Regional Internet Registry (RIR) covering the Asia-Pacific area. So, in order to seek an ASN for a data center in Sapporo, Japan, the firm would need to get in touch with APNIC.

5. D)

- The use of BGP can result in a number of security issues, including route hijacking, unauthorized route announcements, and BGP protocol flaws. Network managers can take a number of steps to mitigate these problems, including prefix-lists, route filtering and safeguarding BGP sessions with Transport Layer Security (TLS) or TCP MD5 authentication. Monitoring BGP traffic and putting best practices for network security into practice are also advised.

Answer 6.

- We need to calculate the time required for the St. Bernard dogs to travel between the data centers while carrying the DVD-ROM disks in order to establish whether they are capable of providing this data delivery service.
- First, we need to convert the data rate of the data pipes from megabits per second (Mbps) to gigabytes per hour (GB/h), which is the same unit as the DVD-ROM disks' capacity.
  150 Mbps = 18.75 MB/s = 67.5 GB/h
- This means that a total of 135 GB/h of data can be sent between the data centers via the two data pipelines.
- The amount of data that can be transported by Alpha and Beta in a single round trip between the data centers must then be determined. Because each DVD-ROM disk can hold 15 GB of data and each dog can carry three of them, the total amount of data that can be transported by both dogs is:
  2 dogs x 3 disks/dog x 15 GB/disk = 90 GB

- We must divide the total quantity of data carried by both dogs by the data transmission rate of the pipes in order to calculate how long it would take the dogs to go back and forth between the data centers:
  90 GB / 135 GB/h = 0.67 h = 40 minutes
- As a result, it takes the dogs 40 minutes to transmit data between data centers, which is quicker than setting up a physical network or renting pipes from service providers. The canines must be able to travel the 5.5 kilometers between the data centers without any problems, and the DVD-ROM disks must stay intact and readable the entire way.