ANS-C01 Q&As

AWS Certified Advanced Networking Specialty Exam

Pass Amazon ANS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/ans-c01.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 1

A network engineer needs to provide dual-stack connectivity between a company\\'s office location and an AWS account. The company\\'s on-premises router supports dual-stack connectivity, and the VPC has been configured with dual-stack support. The company has set up two AWSDirect Connect connections to the office location. This connectivity must be highly available and must be reliable for latency-sensitive traffic.Which solutions will meet these requirements? (Choose two.)

A. Configure a single private VIF on each Direct Connect connection. Add both IPv4 and IPv6 peering to each private VIF. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4 peering and IPv6 routes on the IPv6peering. Enable Bidirectional Forwarding Detection (BFD) on all peering sessions.

B. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with theIPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4peering and IPv6 routes on the IPv6 peering. Enable Bidirectional Forwarding Detection (BFD) on all peering sessions.

C. Configure a single private VIF and IPv4 peering on each Direct Connect connection. Configure the on-premises equipment with thispeering to advertise the IPv6 routes in the same BGP neighbor configuration. Enable Bidirectional Forwarding Detection (BFD) on allpeering sessions.

D. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with theIPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise all IPv4 routes and IPv6routes on all peering sessions. Keep the Bidirectional Forwarding Detection (BFD) configuration unchanged.

E. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with theIPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4peering and IPv6 routes on the IPv6 peering. Reduce the BGP hello timer to 5 seconds on both the on-premises equipment and the DirectConnect configuration.

Correct Answer: AB

Both ipv4 and ipv6 BGP sessions can be established with one private VIF

After creating an ipv4 BGP peering on the VIF at the beginning, you can add an ipv6 peering with "add peering" And you have to enable BFD

QUESTION 2

A company recently started using AWS Client VPN to give its remote users the ability to access resources in multiple peered VPCs andresources in the company\\'s on-premises data center. The Client VPN endpoint route table has a single entry of 0.0.0.0/0. The Client VPNendpoint is using a new security group that has no inbound rules and a single outbound rule that allows all traffic to 0.0.0.0/0.Multiple remote users report that web search results are showing incorrect geographic location information for the users.Which combination of steps should a network engineer take to resolve this issue with the LEAST amount of service interruption? (Choosethree.)

A. Switch users to AWS Site-to-Site VPNs.

B. Enable the split-tunnel option on the Client VPN endpoint.

C. Add routes for the peered VPCs and for the on-premises data center to the Client VPN route table.

D. Remove the 0.0.0.0/0 outbound rule from the security group that the Client VPN endpoint uses.

E. Delete and recreate the Client VPN endpoint in a different VPC.

F. Remove the 0.0.0.0/0 entry from the Client VPN endpoint route table.

Correct Answer: BCF

https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/split-tunnel-vpn.html

QUESTION 3

A company is establishing connectivity between its on-premises site and an existing VPC on AWS to meet a new security requirement.According to the new requirement, all public DNS queries must use an on-premises DNS security solution. The company\\'s security team hasallowed an exception for the AWS service endpoints because the company is using VPC endpoints to access AWS services.Which combination of steps should a network engineer take to configure the architecture to meet these requirements? (Choose three.)

A. Create a system rule for the domain name "." (dot) with a target IP address of the on-premises DNS security solution.

B. Create a new DHCP options set that provides the IP address of the on-premises DNS security solution. Update the VPC to use this newDHCP options set.

C. Create an Amazon Route 53 Resolver inbound endpoint. Associate this endpoint with the VPC.

D. Create an Amazon Route 53 Resolver outbound endpoint. Associate this endpoint with the VPC.

E. Create a system rule for the domain name amazonaws.com.

F. Create a forwarding rule for the domain name "." (dot) with a target IP address of the on-premises DNS security solution.

Correct Answer: DEF

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-autodefined-rules

QUESTION 4

A company is moving its record-keeping application to the AWS Cloud. All traffic between the company\\'s on-premises data center and AWSmust be encrypted at all times and at every transit device during the migration.The application will reside across multiple Availability Zones in a single AWS Region. The application will use existing 10 Gbps AWS DirectConnect dedicated connections with a MACsec capable port. A network engineer must ensure that the Direct Connect connection is securedaccordingly at every transit device.The network engineer creates a Connection Key Name and Connectivity Association Key (CKN/CAK) pair for the MACsec secret key.Which combination of additional steps should the network engineer take to meet the requirements? (Choose two.)

A. Configure the on-premises router with the MACsec secret key.

B. Update the connection\\'s MACsec encryption mode to must_encrypt. Then associate the CKN/CAK pair with the connection.

C. Update the connection\\'s MACsec encryption mode to should encrypt. Then associate the CKN/CAK pair with the connection.

D. Associate the CKN/CAK pair with the connection. Then update the connection\\'s MACsec encryption mode to must_encrypt.

E. Associate the CKN/CAK pair with the connection. Then update the connection\\'s MACsec encryption mode to should_encrypt.

Correct Answer: AD

According to AWS, you need to do the following 4 steps in order.

1.

Create a new connection with MACsec support

2.

Associate the CKN/CAK with the connection

3.

Verify the connection status

4.

Migrate traffic to new connection as appropriate

When you first create the DX connection, the default encryption mode is should encrypt. You need to update it to must encrypt in step 3. There\\'s no way to specify that during the creation of DX.

https://aws.amazon.com/blogs/networking-and-content-delivery/adding-macsec-security-to-aws-direct-connect-connections/

QUESTION 5

A team of infrastructure engineers wants to automate the deployment of Application Load Balancer (ALB) components by using the AWSCloud Development Kit (AWS CDK). The CDK application must deploy an infrastructure stack that is reusable and consistent across multipleenvironments, AWS Regions, and AWS accounts.The lead network architect on the project has already bootstrapped the target accounts. The lead network architect also has deployed corenetwork components such as VPCs and Amazon Route 53 private hosted zones across the multiple environments and Regions. Theinfrastructure engineers must design the ALB components in the CDK application to use the existing core network components.Which combination of steps will meet this requirement with the LEAST manual effort between environment deployments? (Choose two.)

A. Design the CDK application to read AWS CloudFormation parameters for the values that vary across environments and Regions.Reference these variables in the CDK stack for resources that require the variables.

B. Design the CDK application to read environment variables that contain account and Region details at runtime. Use these variables asproperties of the CDK stack. Use context methods in the CDK stack to retrieve variable values.

C. Create a dedicated account for shared application services in the multi-account environment. Deploy a CDK pipeline to the dedicatedaccount. Create stages in the pipeline that deploy the CDK application across different environments and Regions.

D. Write a script that automates the deployment of the CDK application across multiple environments and Regions. Distribute the script toengineers who are working on the project.

E. Use the CDK toolkit locally to deploy stacks to each environment and Region. Use the --context flag to pass in variables that the CDKapplication can reference at runtime.

Correct Answer: BC

Multi account = AWS organization Fetch such values automatically in CDK via contexts
https://docs.aws.amazon.com/cdk/v2/guide/context.html

QUESTION 6

A company recently experienced an IP address exhaustion event in its VPCs. The event affected service capacity. The VPCs hold two or moresubnets in different Availability Zones.A network engineer needs to develop a solution that monitors IP address usage across resources in the VPCs. The company needs to receivenotification about possible issues so that the company can act before an incident happens.Which solution will meet these requirements with the LEAST operational overhead?

A. Set up Amazon VPC IP Address Manager (IPAM) with a new top-level pool. In the top-level pool, create a pool for each VPC. In each VPCpool, create a pool for each subnet in that VPC. Turn on the auto-import option for the VPC pools and the subnet pools. Configure anAmazon CloudWatch alarm to send an Amazon Simple Notification Service (Amazon SNS) notification if the availability limit threshold isreached.

B. Set up a log group in Amazon CloudWatch Logs for each subnet. Create an AWS Lambda function that reads each subnet\\'s IP addressusage and publishes metrics to the log group. Configure an Amazon CloudWatch alarm to send an Amazon Simple Notification Service(Amazon SNS) notification if the availability limit threshold is reached.

C. Set up a custom Amazon CloudWatch metric for IP address usage for each subnet. Create an AWS Lambda function that reads eachsubnet\\'s IP address usage and publishes a CloudWatch metric dimension. Schedule the Lambda function to run every 5 minutes. Configurea CloudWatch alarm to send an Amazon Simple Notification Service (Amazon SNS) notification if the availability limit threshold is reached.

D. Set up Amazon VPC IP Address Manager (IPAM) with a new top-level pool. In the top-level pool, create a pool for each VPC. In each VPCpool, create a pool for each subnet in that VPC. Turn on the auto-import option for the VPC pools and the subnet pools. Configure anAmazon EventBridge rule that monitors each pool availability limit threshold and sends an Amazon Simple Notification Service (AmazonSNS) notification if the limit threshold is reached.

Correct Answer: A

https://docs.aws.amazon.com/vpc/latest/ipam/cloudwatch-ipam.html

QUESTION 7

A company is using custom DNS servers that run BIND for name resolution in its VPCs. The VPCs are deployed across multiple AWS accountsthat are part of the same organization in AWS Organizations. All the VPCs are connected to a transit gateway. The BIND servers are running ina central VPC and are configured to forward all queries for an on-premises DNS domain to DNS servers that are hosted in an on-premises datacenter. To ensure that all the VPCs use the custom DNS servers, a network engineer has configured a VPC DHCP options set in all the VPCsthat specifies the custom DNS servers to be used as domain name servers.Multiple development teams in the company want to use Amazon Elastic File System (Amazon EFS). A development team has created a newEFS file system but cannot mount the file system to one of its Amazon EC2 instances. The network engineer discovers that the EC2 instancecannot resolve the IP address for the EFS mount point fs-33444567d.efs.us-east-1.amazonaws.com. The network engineer

needs to implementa solution so that development teams throughout the organization can mount EFS file systems.Which combination of steps will meet these requirements? (Choose two.)

A. Configure the BIND DNS servers in the central VPC to forward queries for efs.us-east-1.amazonaws.com to the Amazon provided DNSserver (169.254.169.253).

B. Create an Amazon Route 53 Resolver outbound endpoint in the central VPC. Update all the VPC DHCP options sets to useAmazonProvidedDNS for name resolution.

C. Create an Amazon Route 53 Resolver inbound endpoint in the central VPUpdate all the VPC DHCP options sets to use the Route 53Resolver inbound endpoint in the central VPC for name resolution.

D. Create an Amazon Route 53 Resolver rule to forward queries for the on-premises domain to the on-premises DNS servers. Share therule with the organization by using AWS Resource Access Manager (AWS RAM). Associate the rule with all the VPCs.

E. Create an Amazon Route 53 private hosted zone for the efs.us-east-1.amazonaws.com domain. Associate the private hosted zone withthe VPC where the EC2 instance is deployed. Create an A record for fs-33444567d.efs.us-east1.amazonaws.com in the private hostedzone. Configure the A record to return the mount target of the EFS mount point.

Correct Answer: BD

https://aws.amazon.com/blogs/security/simplify-dns-management-in-a-multiaccount-environment-with-route-53-resolver/

"You can mount an Amazon EFS file system on an Amazon EC2 instance using DNS names. The file system DNS name automatically resolves to the mount target\\'s IP address in the Availability Zone of the connecting Amazon EC2 instance. To be able to do that, the VPC must use the default DNS provided by Amazon to resolve EFS DNS names.

If you plan to use EFS in your environment, I recommend that you resolve EFS DNS names locally and avoid sending these queries to central DNS because clients in that case would not receive answers optimized for their availability zone, which might result in higher operation latencies and less durability."

So, option B) answers EFS resolution from VPC. Combination of Option B) and D) explains resolution from on-prem

QUESTION 8

A company is migrating critical applications to AWS. The company has multiple accounts and VPCs that are connected by a transit gateway.A network engineer must design a solution that performs deep packet inspection for any traffic that leaves a VPC network boundary. Allinspected traffic and the actions that are taken on the traffic must be logged in a central log account.Which solution will meet these requirements with the LEAST administrative overhead?

A. Create a central network VPC that includes an attachment to the transit gateway. Update the VPC and transit gateway route tables tosupport the new attachment. Deploy an AWS Gateway Load Balancer that is backed by third-party, next-generation firewall appliances tothe central network VPC. Create a policy that contains the rules for deep packet inspection. Attach the policy to the firewall appliances.Create an Amazon S3 bucket in the central log account. Configure the firewall appliances to capture and save the network flow logs to theS3 bucket.

B. Create a central network VPC that includes an attachment to the transit gateway. Update the VPC and transit gateway route tables tosupport the new attachment. Deploy an AWS Application Load Balancer that is backed by third-party, next-generation firewall appliancesto the central network VPC. Create a policy that contains the rules for deep packet inspection. Attach the policy to the firewall appliances.Create a syslog server in the central log account. Configure the firewall appliances to capture and save the network flow logs to the syslogserver.

C. Deploy network ACLs and security groups to each VPAttach the security groups to active network interfaces. Associate the networkACLs with VPC subnets. Create rules for the network ACLs and security groups to allow only the required traffic flows between subnets andnetwork interfaces. Create an Amazon S3 bucket in the central log account. Configure a VPC flow log that captures and saves all trafficflows to the S3 bucket.

D. Create a central log VPC and an attachment to the transit gateway. Update the VPC and transit gateway route tables to support the newattachment. Deploy an AWS Network Load Balancer (NLB) that is backed by third-party, next-generation intrusion detection system (IDS)security appliances to the central VPC. Activate rules on the security appliances to monitor for intrusion signatures. For each networkinterface, create a VPC Traffic Mirroring session that sends the traffic to the central VPC\\'s NLB.

Correct Answer: A

QUESTION 9

A company is running multiple workloads on Amazon EC2 instances in public subnets. In a recent incident, an attacker exploited anapplication vulnerability on one of the EC2 instances to gain access to the instance. The company fixed the application and launched areplacement EC2 instance that contains the updated application.The attacker used the compromised application to spread malware over the internet. The company became aware of the compromise througha notification from AWS. The company needs the ability to identify when an application that is deployed on an EC2 instance is spreadingmalware.Which solution will meet this requirement with the LEAST operational effort?

A. Use Amazon GuardDuty to analyze traffic patterns by inspecting DNS requests and VPC flow logs.

B. Use Amazon GuardDuty to deploy AWS managed decoy systems that are equipped with the most recent malware signatures.

C. Set up a Gateway Load Balancer. Run an intrusion detection system (IDS) appliance from AWS Marketplace on Amazon EC2 for trafficinspection.

D. Configure Amazon Inspector to perform deep packet inspection of outgoing traffic.

Correct Answer: A

This solution involves using Amazon GuardDuty to monitor network traffic and analyze DNS requests and VPC flow logs for suspicious activity. This will allow the company to identify when an application is spreading malware by monitoring the network traffic patterns associated with the instance. GuardDuty is a fully managed threat detection service that continuously monitors for malicious activity and unauthorized behavior in your AWS accounts and workloads. It requires minimal setup and configuration and can be integrated with other AWS services for automated remediation. This solution requires the least operational effort compared to the other options

QUESTION 10

An international company wants to implement a multi-site hybrid infrastructure. The company wants to deploy its cloud computing resources on AWS in the us-east-1 Region and in the eu-west-2 Region, and in on-premises data centers in the United States (US) and in the United Kingdom (UK). The data centers are connected to each other by a private WAN connection. IP routing information is exchanged dynamically through BGP. The company wants to have two AWS Direct Connect connections, one each in the US and the UK.

The company expects to have 15 VPCs in each Region with CIDR blocks that do not overlap with each other or with CIDR blocks of the on-premises environment. The VPC CIDR blocks are planned so that the prefix aggregation can be performed both on a Regional level and across the entire AWS environment. The company will deploy a transit gateway in each Region to connect the VPCs. A network engineer plans to use a Direct Connect gateway in each Region. A

transit VIF will attach the Direct Connect gateway in each Region to the transit gateway in that Region. The transit gateways will be peered with each other.

The network engineer wants to ensure that traffic follows the shortest geographical path from source to destination. Traffic between the on-premises data centers and AWS must travel across a local Direct Connect connection. Traffic between the US data center and eu-west-2 and traffic between the UK data center and us-east-1 must use the private WAN connection to reach the Direct Connect connection to the appropriate Region when the Direct Connect connection is available. The network must be resilient to failures in either the private WAN connection or with the Direct Connect connections. The network also must reroute traffic automatically in the event of any failure.

How should the network engineer configure the transit VIF associations on the Direct Connect gateways to meet these requirements?

A. Advertise only the aggregate route for the company\\'s entire AWS environment.

B. Advertise VPC-specific CIDR prefixes from only the local Region. Additionally, advertise the aggregate route for the company\\'s entire AWS environment.

C. Advertise all the specific VPC CIDR blocks from both Regions.

D. Advertise both Regional aggregate prefixes. Configure custom BGP communities on the routes advertised toward the data center.

Correct Answer: B

QUESTION 11

A security team is performing an audit of a company\\'s AWS deployment. The security team is concerned that two applications might beaccessing resources that should be blocked by network ACLs and security groups. The applications are deployed across two Amazon ElasticKubernetes Service (Amazon EKS) clusters that use the Amazon VPC Container Network Interface (CNI) plugin for Kubernetes. The clustersare in separate subnets within the same VPC and have a Cluster Autoscaler configured.The security team needs to determine which POD IP addresses are communicating with which services throughout the VPC. The security teamwants to limit the number of flow logs and wants to examine the traffic from only the two applications.Which solution will meet these requirements with the LEAST operational overhead?

A. Create VPC flow logs in the default format. Create a filter to gather flow logs only from the EKS nodes. Include the srcaddr field and thedstaddr field in the flow logs.

B. Create VPC flow logs in a custom format. Set the EKS nodes as the resource Include the pkt-srcaddr field and the pkt-dstaddr field in theflow logs.

C. Create VPC flow logs in a custom format. Set the application subnets as resources. Include the pkt-srcaddr field and the pkt-dstaddrfield in the flow logs.

D. Create VPC flow logs in a custom format. Create a filter to gather flow logs only from the EKS nodes. Include the pkt-srcaddr field andthe pkt-dstaddr field in the flow logs.

Correct Answer: C

Eks Node can\\'t be specified in VPC log filter

QUESTION 12

A company has two on-premises data center locations. There is a company-managed router at each data center. Each data center has adedicated AWS Direct Connect connection to a Direct Connect gateway through a private virtual interface. The router for the first location isadvertising 110 routes to the Direct Connect gateway by using BGP, and the router for the second location is advertising 60 routes to theDirect Connect gateway by using BGP. The Direct Connect gateway is attached to a company VPC through a virtual private gateway.A network engineer receives reports that resources in the VPC are not reachable from various locations in either data center. The networkengineer checks the VPC route table and sees that the routes from the first data center location are not being populated into the route table.The network engineer must resolve this issue in the most operationally efficient manner.What should the network engineer do to meet these requirements?

A. Remove the Direct Connect gateway, and create a new private virtual interface from each company router to the virtual private gatewayof the VPC.

B. Change the router configurations to summarize the advertised routes.

C. Open a support ticket to increase the quota on advertised routes to the VPC route table.

D. Create an AWS Transit Gateway. Attach the transit gateway to the VPC, and connect the Direct Connect gateway to the transit gateway.

Correct Answer: B

You can announce a maximum of 100 prefixes to AWS.These routes can be automatically be propagated into subnet route tables In order to advertise more than 100 prefixes, you should summarize the prefixes into larger range to reduce number of prefixes

QUESTION 13

A company has two AWS accounts one for Production and one for Connectivity. A network engineer needs to connect the Production accountVPC to a transit gateway in the Connectivity account. The feature to auto accept shared attachments is not enabled on the transit gateway.Which set of steps should the network engineer follow in each AWS account to meet these requirements?

A. 1. In the Production account: Create a resource share in AWS Resource Access Manager for the transit gateway. Provide theConnectivity account ID. Enable the feature to allow external accounts2. In the Connectivity account: Accept the resource.3. In the Connectivity account: Create an attachment to the VPC subnets.4. In the Production account: Accept the attachment. Associate a route table with the attachment.

B. 1. In the Production account: Create a resource share in AWS Resource Access Manager for the VPC subnets. Provide the Connectivityaccount ID. Enable the feature to allow external accounts.2. In the Connectivity account: Accept the resource.3. In the Production account: Create an attachment on the transit gateway to the VPC subnets.4. In the Connectivity account: Accept the attachment. Associate a route table with the attachment.

C. 1. In the Connectivity account: Create a resource share in AWS Resource Access Manager for the VPC subnets. Provide the Productionaccount ID. Enable the feature to allow external accounts.2. In the Production account: Accept the resource.3. In the Connectivity account: Create an attachment on the transit gateway to the VPC subnets.4. In the Production account: Accept the attachment. Associate a route table with the attachment.

D. 1. In the Connectivity account: Create a resource share in AWS Resource Access Manager for the transit gateway. Provide theProduction account ID Enable the feature to allow external accounts.2. In the Production account: Accept the resource.3. In the Production account: Create an attachment to the VPC subnets.4. In the Connectivity account: Accept the attachment. Associate a route table with the attachment.

Correct Answer: D

D is correct, the first step is to share the TGW From the Connectivity account to the Production account, making all the other options incorrect.

QUESTION 14

A company has a highly available application that is hosted in multiple VPCs and in two on-premises data centers. All the VPCs reside in the same AWS Region. All the VPCs require access to each other and to the on-premises data centers for the transfer of files that are multiple gigabytes in size.

A network engineer is designing an AWS Direct Connect solution to connect the on-premises data centers to each VPC.

Which architecture will meet the company\\'s requirements with the LEAST operational overhead?

A. Configure a virtual private gateway and a private VIF in each VPC in the Region. Configure a Direct Connect gateway. Associate the VIF of every VPC with the Direct Connect gateway. Create a new private VIF that connects the Direct Connect gateway to each on-premises data center. Configure the new private VIF to exchange BGP routes with the on-premises data centers and to have an MTU of 9001. Use VPC peering between each VPC. Configure static routing in each VPC to provide inter-VPC routing.

B. Configure a virtual private gateway and a private VIF in each VPC in the Region. Configure a Direct Connect gateway. Associate the VIF of every VPC with the Direct Connect gateway. Create a new private VIF that connects the Direct Connect gateway to each on-premises data center. Configure the new private VIF to exchange BGP routes with the on-premises data centers and to have an MTU of 8500. Use VPC peering between each VPC. Configure static routing in each VPC to provide inter-VPC routing.

C. Configure a transit gateway in the same Region of each VPAttach each VPC to the transit gateway. Configure a Direct Connect gateway. Associate the Direct Connect gateway with the transit gateway. Associate a new transit VIF with each Direct Connect connection. Configure the new transit VIF to exchange BGP routes and to have an MTU of 9001. Configure route propagation between each VPC and the transit gateway.

D. Configure a transit gateway in the same Region of each VPC. Attach each VPC to the transit gateway. Configure a Direct Connect gateway. Associate the Direct Connect gateway with the transit gateway. Associate a new transit VIF with each Direct Connect connection. Configure the new transit VIF to exchange BGP routes and to have an MTU of 8500. Configure route propagation between each VPC and the transit gateway.

Correct Answer: D

QUESTION 15

A company is migrating its containerized application to AWS. For the architecture the company will have an ingress VPC with a Network LoadBalancer (NLB) to distribute the traffic to front-end pods in an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The front end of theapplication will determine which user is requesting access and will send traffic to 1 of 10 services VPCs. Each services VPC will include anNLB that distributes traffic to the services pods in an EKS cluster.The company is concerned about overall cost. User traffic will be responsible for more than 10 TB of data transfer from the ingress VPC toservices VPCs every month. A network engineer needs to recommend how to design the communication between the VPCs.Which solution will meet these requirements at the LOWEST cost?

A. Create a transit gateway. Peer each VPC to the transit gateway. Use zonal DNS names for the NLB in the services VPCs to minimizecross-AZ traffic from the ingress VPC to the services VPCs.

B. Create an AWS PrivateLink endpoint in every Availability Zone in the ingress VPC. Each PrivateLink endpoint will point to the zonal DNSentry of the NLB in the services VPCs.

C. Create a VPC peering connection between the ingress VPC and each of the 10 services VPCs. Use zonal DNS names for the NLB in theservices VPCs to minimize cross-AZ traffic from the ingress VPC to the services VPCs.

D. Create a transit gateway. Peer each VPC to the transit gateway. Turn off cross-AZ load balancing on the transit gateway. Use RegionalDNS names for the NLB in the services VPCs.

Correct Answer: C

VPC peering offers the lowest overall cost when compared to other options for inter-VPC connectivity. https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/vpc-to-vpc-connectivity.html

There is no such thing as "TG peering"; there are VPC peering and TG attachments.