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.leads4pass.com/ans-c01.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company plans to run a computationally intensive data processing application on AWS. The data is highly sensitive. The VPC must have nodirect internet access, and the company has applied strict network security to control access.Data scientists will transfer data from the company\\'s on-premises data center to the instances by using an AWS Site-to-Site VPN connection.The on-premises data center uses the network range 172.31.0.0/20 and will use the network range 172.31.16.0/20 in the application VPC.The data scientists report that they can start new instances of the application but that they cannot transfer any data from the on-premisesdata center. A network engineer enables VPC flow logs and sends a ping to one of the instances to test reachability. The flow logs show thefollowing:

```
2 123456789010 eni-1235b8ca123456789 172.31.8.29 172.31.18.139 0 0 1 4 336 1622433184 1622433194 ACCEPT OK
2 123456789010 eni-1235b8ca123456789 172.31.18.139 172.31.8.29 0 0 1 3 252 1622433216 1622433232 REJECT OK
```

The network engineer must recommend a solution that will give the data scientists the ability to transfer data from the on-premises datacenter.Which solution will meet these requirements?

A. Modify the security group for the application. Add an inbound rule to allow traffic from the on-premises data center network range tothe application.

B. Modify the network ACLs for the VPC subnet. Add an inbound rule to allow traffic from the on-premises data center network range to theVPC subnet range.

C. Modify the network ACLs for the VPC subnet. Add an outbound rule to allow traffic from the VPC subnet range to the on-premises datacenter network range.

D. Modify the security group for the application. Add an outbound rule to allow traffic from the application to the on-premises data centernetwork range.

Correct Answer: C

Return traffic was blocked by NACL, outbound should be allowed

QUESTION 2

A company\\'s network engineer is designing a hybrid DNS solution for an AWS Cloud workload. Individual teams want to manage their own DNShostnames for their applications in their development environment. The solution must integrate the application-specific hostnames with thecentrally managed DNS hostnames from the on-premises network and must provide bidirectional name resolution. The solution also mustminimize management overhead.Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Use an Amazon Route 53 Resolver inbound endpoint.

B. Modify the DHCP options set by setting a custom DNS server value.

C. Use an Amazon Route 53 Resolver outbound endpoint.

D. Create DNS proxy servers.

E. Create Amazon Route 53 private hosted zones.

F. Set up a zone transfer between Amazon Route 53 and the on-premises DNS.

Correct Answer: ACE

For bidirectional name resolution, both Route 53 Resolver inbound and outbound endpoint is required.

QUESTION 3

AnyCompany has acquired Example Corp. AnyCompany\\'s infrastructure is all on premises, and Example Corp\\'s infrastructure is completely inthe AWS Cloud. The companies are using AWS Direct Connect with AWS Transit Gateway to establish connectivity between each other.Example Corp has deployed a new application across two Availability Zones in a VPC with no internet gateway. The CIDR range for the VPC is10.0.0.0/16. Example Corp needs to access an application that is deployed on premises by AnyCompany. Because of compliancerequirements, Example Corp must access the application through a limited contiguous block of approved IP addresses (10.1.0.0/24).A network engineer needs to implement a highly available solution to achieve this goal. The network engineer starts by updating the VPC toadd a new CIDR range of 10.1.0.0/24.What should the network engineer do next to meet the requirements?

A. In each Availability Zone in the VPC, create a subnet that uses part of the allowed IP address range. Create a public NAT gateway ineach of the new subnets. Update the route tables that are associated with other subnets to route application traffic to the public NATgateway in the corresponding Availability Zone. Add a route to the route table that is associated with the subnets of the public NATgateways to send traffic destined for the application to the transit gateway.

B. In each Availability Zone in the VPC, create a subnet that uses part of the allowed IP address range. Create a private NAT gateway ineach of the new subnets. Update the route tables that are associated with other subnets to route application traffic to the private NATgateway in the corresponding Availability Zone. Add a route to the route table that is associated with the subnets of the private NATgateways to send traffic destined for the application to the transit gateway.

C. In the VPC, create a subnet that uses the allowed IP address range. Create a private NAT gateway in the new subnet. Update the routetables that are associated with other subnets to route application traffic to the private NAT gateway. Add a route to the route table that isassociated with the subnet of the private NAT gateway to send traffic destined for the application to the transit gateway.

D. In the VPC, create a subnet that uses the allowed IP address range. Create a public NAT gateway in the new subnet. Update the routetables that are associated with other subnets to route application traffic to the public NAT gateway. Add a route to the route table that isassociated with the subnet of the public NAT gateway to send traffic destined for the application to the transit gateway.

Correct Answer: B

B is correct - Needs to be highly available so multiple AZ\\'s required one in each of the 2 AZ\\'s

"Example Corp has deployed a new application across two Availability Zones in a VPC with no internet gateway"

QUESTION 4

A company hosts its IT infrastructure in an on-premises data center. The company wants to migrate the infrastructure to the AWS Cloud inphases. A network engineer wants to set up a 10 Gbps AWS Direct Connect dedicated connection between the on-premises data center andVPCs. The company\\'s network provider needs 3 months to provision the Direct Connect connection.In the meantime, the network engineer implements a temporary solution by deploying an AWS Siteto-Site VPN connection that terminates toa virtual private gateway. The network engineer observes that the bandwidth of the Site-to-Site VPN connection is capped at 1.25 Gbpsdespite a powerful customer gateway device.What should the network engineer do to improve the VPN connection bandwidth before the implementation of the Direct Connect connection?

A. Contact AWS Support to request a bandwidth quota increase for the existing Site-to-Site VPN connection.

B. Discuss the issue with the hardware vendor. Buy a bigger and more powerful customer gateway device that has faster encryption anddecryption capabilities.

C. Create several additional Site-to-Site VPN connections that terminate on the same virtual gateway. Configure equal-cost multi-path(ECMP) routing to use all the VPN connections simultaneously.

D. Create a transit gateway. Attach the VPCs to the transit gateway. Create several additional Site-to-Site VPN connections that terminateon the transit gateway. Configure equal-cost multi-path (ECMP) routing to use all the VPN connections simultaneously.

Correct Answer: D

ECMP is not supported for Site-to-Site VPN connections on a virtual private gateway.

You can check this document: https://docs.aws.amazon.com/vpn/latest/s2svpn/VPNRoutingTypes.html

QUESTION 5

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 6

A company has developed a new web application on AWS. The application runs on Amazon Elastic Container Service (Amazon ECS) on AWSFargate behind an Application Load Balancer (ALB) in the us-east-1 Region. The application uses Amazon Route 53 to host the DNS recordsfor the domain. The content that is served from the website is mostly static images and files that are not updated frequently. Most of thetraffic to the website from end users will originate from the United States. Some traffic will originate from Canada and Europe.A network engineer needs to design a solution that will reduce latency for end users at the lowest cost. The solution also must ensure that alltraffic is encrypted in transit until the traffic reaches the ALB.Which solution will meet these requirements?

A. Configure the ALB to use an AWS Global Accelerator accelerator in us-east-1. Create a secure HTTPS listener. Create an alias record inAmazon Route 53 for the custom domain name. Configure the alias record to route to the DNS name that is assigned to the accelerator forthe ALB.

B. Configure the ALB to use a secure HTTPS listener. Create an Amazon CloudFront distribution. Set the origin domain name to point tothe DNS record that is assigned to the ALConfigure the CloudFront distribution to use an SSL certificate. Set all behaviors to force HTTPS.Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to route to the DNS name that isassigned to the ALB.

C. Configure the ALB to use a secure HTTPS listener. Create an Amazon CloudFront distribution. Set the origin domain name to point tothe DNS record that is assigned to the ALB. Configure the CloudFront distribution to use an SSL certificate and redirect HTTP to HTTPS.Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to route to the CloudFront distribution.

D. Configure the ALB to use an AWS Global Accelerator accelerator in us-east-1. Create a secure HTTPS listener. Create a secondapplication stack on Amazon ECS on Fargate in the eu-west-1 Region. Create another secure HTTPS listener. Create an alias record inAmazon Route 53 for the custom domain name. Configure the alias record to use a latency-based routing policy to route to the DNS namethat is assigned to the accelerator for the ALBs.

Correct Answer: C

Route 53 record points to Cloudfront default DNS name.

QUESTION 7

A company uses Amazon Route 53 to register a public domain, example.com, in an AWS account. A central services group manages theaccount. The company wants to create a subdomain, test.example.com, in another AWS account to offer name services for Amazon EC2instances that are hosted in the account. The company does not want to migrate the parent domain to the subdomain account.A network engineer creates a new Route 53 hosted zone for the subdomain in the second account.Which combination of steps must the network engineer take to complete the task? (Choose two.)

A. Add records for the hosts of the new subdomain to the new Route 53 hosted zone.

B. Update the DNS service for the parent domain by adding name server (NS) records for the subdomain.

C. Update the DNS service for the subdomain by adding name server (NS) records for the parent domain.

D. Create an alias record from the parent domain that points to the hosted zone for the subdomain in the second account.

E. Add a start of authority (SOA) record in the parent domain for the subdomain.

Correct Answer: AB

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/CreatingNewSubdomain.html

QUESTION 8

A company has an AWS Site-to-Site VPN connection between its existing VPC and on-premises network. The default DHCP options set isassociated with the VPC. The company has an application that is running on an Amazon Linux 2 Amazon EC2 instance in the VPC. Theapplication must retrieve an Amazon RDS database secret that is stored in AWS Secrets Manager through a private VPC endpoint. An on-premises application provides internal RESTful API service that can be reached by URL (https://api.example.internal). Two on-premisesWindows DNS servers provide internal DNS resolution.The application on the EC2 instance needs to call the internal API service that is deployed in the on-premises environment. When theapplication on the EC2 instance attempts to call the internal API service by referring to the hostname that is assigned to the service, the callfails. When a network engineer tests the API service call from the same EC2 instance by using the API service\\'s IP address, the call issuccessful.What should the network engineer do to resolve this issue and prevent the same problem from affecting other resources in the VPC?

A. Create a new DHCP options set that specifies the on-premises Windows DNS servers. Associate the new DHCP options set with theexisting VPC. Reboot the Amazon Linux 2 EC2 instance.

B. Create an Amazon Route 53 Resolver rule. Associate the rule with the VPC. Configure the rule to forward DNS queries to the on-premises Windows DNS servers if the domain name matches example.internal.

C. Modify the local host file in the Amazon Linux 2 EC2 instance in the VPMap the service domain name (api.example.internal) to the IPaddress of the internal API service.

D. Modify the local /etc/resolv.conf file in the Amazon Linux 2 EC2 instance in the VPC. Change the IP addresses of the name servers inthe file to the IP addresses of the company\\'s on-premises Windows DNS servers.

Correct Answer: B

QUESTION 9

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 10

An IoT company collects data from thousands of sensors that are deployed in the Unites States and South Asia. The sensors use a proprietarycommunication protocol that is built on UDP to send the data to a fleet of Amazon EC2 instances. The instances are in an Auto Scaling groupand run behind a Network Load Balancer (NLB). The instances, Auto Scaling group, and NLB are deployed in the us-west-2 Region.Occasionally, the data from the sensors in South Asia gets lost in transit over the internet and does not reach the EC2 instances.Which solutions will resolve this issue? (Choose two.)

A. Use AWS Global Accelerator with the existing NLB.

B. Create an Amazon CloudFront distribution. Specify the existing NLB as the origin.

C. Create a second deployment of the EC2 instances and the NLB in the ap-south-1 Region. Use an Amazon Route 53 latency routingpolicy to resolve to the Region that provides the least latency.

D. Create a second deployment of the EC2 instances and the NLB in the ap-south-1 Region. Use an Amazon Route 53 failover routingpolicy to resolve to an alternate Region in case packets are dropped.

E. Turn on enhanced networking on the EC2 instances by using the most recent Elastic Network Adapter (ENA) drivers.

Correct Answer: AC

Global Accelerator is one option Another option is to have a second fleet of ec2 instances deployed in South Asia region and then have Route 53 latency based routing policy enabled

---

QUESTION 11

A company uses multiple AWS accounts and VPCs in a single AWS Region. The company must log all network traffic for Amazon EC2 instancesand Amazon RDS databases. The company will use the log information to monitor and identify traffic flows in the event of a security incident.The information must be retained for 12 months but will be accessed infrequently after the first 90 days. The company must be able to viewmetadata that includes the vpc-id, subnet-id: and tcpflags fields.Which solution will meet these requirements at the LOWEST cost?

A. Configure VPC flow logs with the default fields Store the logs in Amazon CloudWatch Logs.

B. Configure Traffic Mirroring on all AWS resources to point to a Network Load Balancer that will send the mirrored traffic to monitoringinstances.

C. Configure VPC flow logs with additional custom format fields Store the logs in Amazon S3.

D. Configure VPC flow logs with additional custom format fields Store the logs in Amazon CloudWatch Logs.

Correct Answer: C

The other options are less cost-effective:

Option A does not allow you to capture the custom fields you need (vpc-id, subnet-id, and tcp-flags).

Option B, Traffic Mirroring, would involve a considerable overhead in terms of infrastructure and cost. Traffic Mirroring copies all traffic (not just metadata), which can be massive, and it requires additional resources to capture and process that

traffic.

Option D is less cost-effective for long-term, infrequently accessed storage because Amazon CloudWatch Logs is more expensive than Amazon S3 for these use cases.

QUESTION 12

A global company is designing a hybrid architecture to privately access AWS resources in the us-west-2 Region. The company\\'s existingarchitecture includes a VPC that uses RFC 1918 IP address space. The VPC is connected to an on-premises data center over AWS DirectConnect Amazon Route 53 provides name resolution within the VPC. Locally managed DNS servers in the data center provide DNS services tothe on-premises hosts.The company has applications in the data center that need to download objects from an Amazon S3 bucket in us-west-2.Which solution can the company use to access Amazon S3 without using the public IP address space?

A. Create an S3 interface endpoint in the VPC. Update the on-premises application configuration to use the Regional VPC endpoint DNShostname that is mapped to the S3 interface endpoint.

B. Create an S3 interface endpoint in the VPC. Configure a Route 53 Resolver inbound endpoint in the VPC. Set up the data center DNSservers to forward DNS queries for the S3 domain from on premises to the inbound endpoint.

C. Create an S3 gateway endpoint in the VPUpdate the on-premises application configuration to use the hostname that is mapped to theS3 gateway endpoint.

D. Create an S3 gateway endpoint in the VPC. Configure a Route 53 Resolver inbound endpoint in the VPC. Set up the data center DNSservers to forward DNS queries for the S3 domain from on premises to the inbound endpoint.

Correct Answer: B

https://aws.amazon.com/blogs/networking-and-content-delivery/secure-hybrid-access-to-amazon-s3-using-aws-privatelink/

QUESTION 13

A network engineer is designing a hybrid networking environment that will connect a company\\'s corporate network to the company\\'s AWSenvironment. The AWS environment consists of 30 VPCs in 3 AWS Regions.The network engineer needs to implement a solution to centrally filter traffic by using a firewall that the company\\'s security team hasapproved. The solution must give all the VPCs the ability to connect to each other. Connectivity between AWS and the corporate network mustmeet a minimum bandwidth requirement of 2 Gbps.Which solution will meet these requirements?

A. Deploy an IPsec VPN connection between the corporate network and a new transit gateway. Connect all VPCs to the transit gateway.Associate the approved firewall with the transit gateway.

B. Deploy a single 10 Gbps AWS Direct Connect connection between the corporate network and virtual private gateway of each VPC.Connect the virtual private gateways to a Direct Connect gateway. Build an IPsec tunnel to a new transit VPC. Deploy the approved firewallto the transit VPC.

C. Deploy two 1 Gbps AWS Direct Connect connections in different Direct Connect locations to connect to the corporate network. Build atransit VIF on each connection to a Direct Connect gateway. Associate the Direct Connect gateway with a new transit gateway for eachRegion. Configure the VIFs to use equal-cost multipath (ECMP) routing. Connect all the VPCs in the three Regions to the transit gateway.Configure the transit gateway route table to route traffic to an inspection VPDeploy the approved firewall to the inspection VPC.

D. Deploy four 1 Gbps AWS Direct Connect connections in different Direct Connect locations to connect to the corporate network. Build atransit VIF on each connection to a Direct Connect gateway. Associate the Direct Connect gateway with a new transit gateway for eachRegion. Connect the transit gateways by using a transit gateway peering attachment. Configure the VIFs to use equal-cost multipath(ECMP) routing. Configure transit gateway route tables to route traffic to an inspection VPC. Deploy the approved firewall to the inspectionVPC.

Correct Answer: D

This solution meets the requirements because:

- It uses AWS Direct Connect, which provides a dedicated and private connection between the corporate network and AWS, with a minimum bandwidth of 2 Gbps (4 x 1 Gbps).
- It uses a Direct Connect gateway, which allows multiple VPCs in different Regions to share the same Direct Connect connection.
- It uses a transit gateway, which acts as a network hub that connects multiple VPCs and other networks, such as the corporate network and the inspection VPC.
- It uses a transit gateway peering attachment, which enables routing between transit gateways in different Regions.

- It uses ECMP routing, which allows traffic to be distributed across multiple paths for higher throughput and redundancy.

- It uses an inspection VPC, which hosts the approved firewall and filters traffic between the corporate network and the AWS environment.

QUESTION 14

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 15

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