# ANS-C01$^{\text{Q\&As}}$

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.passapply.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A company has been using an outdated application layer protocol for communication among applications. The company decides not to usethis protocol anymore and must migrate all applications to support a new protocol. The old protocol and the new protocol are TCP-based, butthe protocols use different port numbers.After several months of work, the company has migrated dozens of applications that run on Amazon EC2 instances and in containers. Thecompany believes that all the applications have been migrated, but the company wants to verify this belief. A network engineer needs toverify that no application is still using the old protocol.Which solution will meet these requirements without causing any downtime?

A. Use Amazon Inspector and its Network Reachability rules package. Wait until the analysis has finished running to find out which EC2instances are still listening to the old port.

B. Enable Amazon GuardDuty. Use the graphical visualizations to filter for traffic that uses the port of the old protocol. Exclude all internettraffic to filter out occasions when the same port is used as an ephemeral port.

C. Configure VPC flow logs to be delivered into an Amazon S3 bucket. Use Amazon Athena to query the data and to filter for the portnumber that is used by the old protocol.

D. Inspect all security groups that are assigned to the EC2 instances that host the applications. Remove the port of the old protocol if thatport is in the list of allowed ports. Verify that the applications are operating properly after the port is removed from the security groups.

Correct Answer: C

A requires agents to be installed while option C is agentless.

**QUESTION 2**

A company has deployed a web application on AWS. The web application uses an Application Load Balancer (ALB) across multiple AvailabilityZones. The targets of the ALB are AWS Lambda functions. The web application also uses Amazon CloudWatch metrics for monitoring.Users report that parts of the web application are not loading properly. A network engineer needs to troubleshoot the problem. The networkengineer enables access logging for the ALB.What should the network engineer do next to determine which errors the ALB is receiving?

A. Send the logs to Amazon CloudWatch Logs. Review the ALB logs in CloudWatch Insights to determine which error messages the ALB isreceiving.

B. Configure the Amazon S3 bucket destination. Use Amazon Athena to determine which error messages the ALB is receiving.

C. Configure the Amazon S3 bucket destination. After Amazon CloudWatch Logs pulls the ALB logs from the S3 bucket automatically,review the logs in CloudWatch Logs to determine which error messages the ALB is receiving.

D. Send the logs to Amazon CloudWatch Logs. Use the Amazon Athena CloudWatch Connector to determine which error messages the ALBis receiving.

Correct Answer: B

Access logs is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logs for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logs at any time.

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

**QUESTION 3**

A company\\'s application team is unable to launch new resources into its VPC. A network engineer discovers that the VPC has run out ofusable IP addresses. The VPC CIDR block is 172.16.0.0/16.Which additional CIDR block can the network engineer attach to the VPC?

A. 172.17.0.0/29

B. 10.0.0.0/16

C. 172.17.0.0/16

D. 192.168.0.0/16

Correct Answer: C

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html#add-cidr-block-restrictions Only it will also us to add 172.17.0.0/16

**QUESTION 4**

A company deploys an internal website behind an Application Load Balancer (ALB) in a VPC. The VPC has a CIDR block of 172.31.0.0/16. Thecompany creates a private hosted zone for the domain example.com for the website in Amazon Route 53. The company establishes an AWSSite-to-Site VPN connection between its office network and the VPC.A network engineer needs to set up a DNS solution so that employees can visit the internal webpage by accessing a private domain URL(https://example.com) from the office network.Which combination of steps will meet this requirement? (Choose two.)

A. Create an alias record that points to the ALB in the Route 53 private hosted zone.

B. Create a CNAME record that points to the ALB internal domain in the Route 53 private hosted zone.

C. Create a Route 53 Resolver inbound endpoint. On the office DNS server, configure a conditional forwarder to forward the DNS queries tothe Route 53 Resolver inbound endpoint.

D. Create a Route 53 Resolver outbound endpoint. On the office DNS server, configure a conditional forwarder to forward the DNS queriesto the Route 53 Resolver outbound endpoint.

E. On the office DNS server, configure a conditional forwarder for the private domain to the VPC DNS at 172.31.0.2.

Correct Answer: AC

Alias record in Route 53 and conditional forwarding from on premise DNS to INBOUND endpoint

**QUESTION 5**

An insurance company is planning the migration of workloads from its on-premises data center to the AWS Cloud. The company requires end-to-end domain name resolution. Bi-directional DNS resolution between AWS and the existing on-premises environments must be established.The workloads will be migrated into multiple VPCs. The workloads also have dependencies on each other, and not all the workloads will bemigrated at the same time.Which solution meets these requirements?

A. Configure a private hosted zone for each application VPC, and create the requisite records. Create a set of Amazon Route 53 Resolverinbound and outbound endpoints in an egress VPC. Define Route 53 Resolver rules to forward requests for the on-premises domains to theon-premises DNS resolver. Associate the application VPC private hosted zones with the egress VPC, and share the Route 53 Resolver ruleswith the application accounts by using AWS Resource Access Manager. Configure the on-premises DNS servers to forward the clouddomains to the Route 53 inbound endpoints.

B. Configure a public hosted zone for each application VPC, and create the requisite records. Create a set of Amazon Route 53 Resolverinbound and outbound endpoints in an egress VPC. Define Route 53 Resolver rules to forward requests for the on-premises domains to theon-premises DNS resolver. Associate the application VPC private hosted zones with the egress VPC. and share the Route 53 Resolver ruleswith the application accounts by using AWS Resource Access Manager. Configure the on-premises DNS servers to forward the clouddomains to the Route 53 inbound endpoints.

C. Configure a private hosted zone for each application VPC, and create the requisite records. Create a set of Amazon Route 53 Resolverinbound and outbound endpoints in an egress VPDefine Route 53 Resolver rules to forward requests for the on-premises domains to theon-premises DNS resolver. Associate the application VPC private hosted zones with the egress VPand share the Route 53 Resolver ruleswith the application accounts by using AWS Resource Access Manager. Configure the on-premises DNS servers to forward the clouddomains to the Route 53 outbound endpoints.

D. Configure a private hosted zone for each application VPC, and create the requisite records. Create a set of Amazon Route 53 Resolverinbound and outbound endpoints in an egress VPC. Define Route 53 Resolver rules to forward requests for the on-premises domains to theon-premises DNS resolver. Associate the Route 53 outbound rules with the application VPCs, and share the private hosted zones with theapplication accounts by using AWS Resource Access Manager. Configure the on-premises DNS servers to forward the cloud domains to theRoute 53 inbound endpoints.

Correct Answer: A

PHZ cannot be shared, Route 53 resolver rules can be shared uusing AWS RAM.

**QUESTION 6**

A company recently migrated its Amazon EC2 instances to VPC private subnets to satisfy a security compliance requirement. The EC2instances now use a NAT gateway for internet access. After the migration, some long-running database queries from private EC2 instances toa publicly accessible third-party database no longer receive responses. The database query logs reveal that the queries successfullycompleted after 7 minutes but that the client EC2 instances never received the response.Which configuration change should a network engineer implement to resolve this issue?

A. Configure the NAT gateway timeout to allow connections for up to 600 seconds.

B. Enable enhanced networking on the client EC2 instances.

C. Enable TCP keepalive on the client EC2 instances with a value of less than 300 seconds.

D. Close idle TCP connections through the NAT gateway.

Correct Answer: C

https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-troubleshooting.html#nat- gateway- troubleshooting-timeout

**QUESTION 7**

A global delivery company is modernizing its fleet management system. The company has several business units. Each business unit designsand maintains applications that are hosted in its own AWS account in separate application VPCs in the same AWS Region. Each businessunit\\'s applications are designed to get data from a central shared services VPC.The company wants the network connectivity architecture to provide granular security controls. The architecture also must be able to scale asmore business units consume data from the central shared services VPC in the future.Which solution will meet these requirements in the MOST secure manner?

A. Create a central transit gateway. Create a VPC attachment to each application VPC. Provide full mesh connectivity between all theVPCs by using the transit gateway.

B. Create VPC peering connections between the central shared services VPC and each application VPC in each business unit\\'s AWSaccount.

C. Create VPC endpoint services powered by AWS PrivateLink in the central shared services VPCreate VPC endpoints in each applicationVPC.

D. Create a central transit VPC with a VPN appliance from AWS Marketplace. Create a VPN attachment from each VPC to the transit VPC.Provide full mesh connectivity among all the VPCs.

Correct Answer: C

VPC endpoint services powered by AWS PrivateLink will provide the highest level of security by keeping all network traffic within the AWS network. It allows for granular security controls by allowing only authorized traffic from the application VPC to the central shared services VPC, reducing the attack surface area.

**QUESTION 8**

A company has a new AWS Direct Connect connection between its on-premises data center and the AWS Cloud. The company has created anew private VIF on this connection. However, the VIF status is DOWN.A network engineer verifies that the physical connection status is UP and RUNNING based on information from the AWS Management Console.The network engineer checks the customer Direct Connect router and can see the ARP entry for the VLAN interface created for the private VIFat AWS.What could be causing the private VIF to have a DOWN status?

A. ICMP is blocked on the customer Direct Connect router.

B. TCP port 179 is blocked on the customer Direct Connect router.

C. The IEEE 802.1Q VLAN identifier is misconfigured on the customer Direct Connect router.

D. The company has configured IEEE 802.1ad instead of 802.1Q on the customer Direct Connect router.

Correct Answer: B

Changed to B as the entry is visible for the VLAN interface created for the private VIF at AWS, which means that the Layer 2 connectivity appears to be functioning correctly.

**QUESTION 9**

A network engineer needs to standardize a company\\'s approach to centralizing and managing interface VPC endpoints for privatecommunication with AWS services. The company uses AWS Transit Gateway for inter-VPC connectivity between AWS accounts through a hub-and-spoke model. The company\\'s network services team must manage all Amazon Route 53 zones and interface endpoints within a sharedservices AWS account. The company wants to use this centralized model to provide AWS resources with access to AWS Key ManagementService (AWS KMS) without sending traffic over the public internet.What should the network engineer do to meet these requirements?

A. In the shared services account, create an interface endpoint for AWS KMS. Modify the interface endpoint by disabling the private DNSname. Create a private hosted zone in the shared services account with an alias record that points to the interface endpoint. Associatethe private hosted zone with the spoke VPCs in each AWS account.

B. In the shared services account, create an interface endpoint for AWS KMS. Modify the interface endpoint by disabling the private DNSname. Create a private hosted zone in each spoke AWS account with an alias record that points to the interface endpoint. Associate eachprivate hosted zone with the shared services AWS account.

C. In each spoke AWS account, create an interface endpoint for AWS KMS. Modify each interface endpoint by disabling the private DNSname. Create a private hosted zone in each spoke AWS account with an alias record that points to each interface endpoint. Associateeach private hosted zone with the shared services AWS account.

D. In each spoke AWS account, create an interface endpoint for AWS KMS. Modify each interface endpoint by disabling the private DNSname. Create a private hosted zone in the shared services account with an alias record that points to each interface endpoint. Associatethe private hosted zone with the spoke VPCs in each AWS account.

Correct Answer: A

Option A is the correct answer because it creates a private hosted zone in the shared services account with an alias record that points to the interface endpoint, and associates the private hosted zone with the spoke VPCs in each AWS account. Disabling the private DNS name of the interface endpoint ensures that DNS resolution of the endpoint is restricted to the Amazon Route 53 private hosted zone. This option creates a centralized model for managing interface endpoints and Route 53 zones in a shared services AWS account, which simplifies administration and reduces complexity.

**QUESTION 10**

A company runs an application on Amazon EC2 instances. A network engineer implements a NAT gateway in the application\\'s VPC to replaceself-managed NAT instances. After the network engineer shifts traffic from the self-managed NAT instances to the NAT gateway, users begin toreport issues.During troubleshooting, the network engineer discovers that the connection to the application is closing after approximately 6 minutes ofinactivity.What should the network engineer do to resolve this issue?

A. Check for increases in the IdleTimeoutCount Amazon CloudWatch metric for the NAT gateway. Configure TCP keepalive on theapplication EC2 instances.

B. Check for increases in the ErrorPortAllocation Amazon CloudWatch metric for the NAT gateway. Configure an HTTP timeout value on theapplication EC2 instances.

C. Check for increases in the PacketsDropCount Amazon CloudWatch metric for the NAT gateway. Configure an HTTPS timeout value onthe application EC2 instances.

D. Check for decreases in the ActiveConnectionCount Amazon CloudWatch metric for the NAT gateway. Configure UDP keepalive on theapplication EC2 instances.

Correct Answer: A

Internet connection drops after 350 seconds

Problem

Your instances can access the internet, but the connection drops after 350 seconds.

Cause

If a connection that\\'s using a NAT gateway is idle for 350 seconds or more, the connection times out.

When a connection times out, a NAT gateway returns an RST packet to any resources behind the NAT gateway that attempt to continue the connection (it does not send a FIN packet).

Solution

To prevent the connection from being dropped, you can initiate more traffic over the connection. Alternatively, you can enable TCP keepalive on the instance with a value less than 350 seconds.

**QUESTION 11**

A network engineer needs to build an encrypted connection between an on-premises data center and a VPC. The network engineer attachesthe VPC to a virtual private gateway and sets up an AWS Site-to-Site VPN connection. The VPN tunnel is UP after configuration and is working.However, during rekey for phase 2 of the VPN negotiation, the customer gateway device is receiving different parameters than the parametersthat the device is configured to support.The network engineer checks the IPsec configuration of the VPN tunnel. The network engineer notices that the customer gateway device isconfigured with the most secure encryption algorithms that the AWS Site-to-Site VPN configuration file provides.What should the network engineer do to troubleshoot and correct the issue?

A. Check the native virtual private gateway logs. Restrict the VPN tunnel options to the specific VPN parameters that the virtual privategateway requires.

B. Check the native customer gateway logs. Restrict the VPN tunnel options to the specific VPN parameters that the customer gatewayrequires.

C. Check Amazon CloudWatch logs of the virtual private gateway. Restrict the VPN tunnel options to the specific VPN parameters that thevirtual private gateway requires.

D. Check Amazon CloudWatch logs of the customer gateway. Restrict the VPN tunnel options to the specific VPN parameters that thecustomer gateway requires.

Correct Answer: B

You check Cloudwatch for AWS resources or your native/on-prem logs for your on prem resource. AandD is out.

The problem statement indicates that customer gateway is misconfigured. So you need to work on Customer gateway.

**QUESTION 12**

A company is planning to use Amazon S3 to archive financial data. The data is currently stored in an on-premises data center. The companyuses AWS Direct Connect with a Direct Connect gateway and a transit gateway to connect to the on-premises data center. The data cannot betransported over the public internet and must be encrypted in transit.Which solution will meet these requirements?

A. Create a Direct Connect public VIF. Set up an IPsec VPN connection over the public VIF to access Amazon S3. Use HTTPS forcommunication.

B. Create an IPsec VPN connection over the transit VIF. Create a VPC and attach the VPC to the transit gateway. In the

VPC, provision aninterface VPC endpoint for Amazon S3. Use HTTPS for communication.

C. Create a VPC and attach the VPC to the transit gateway. In the VPC, provision an interface VPC endpoint for Amazon S3. Use HTTPS forcommunication.

D. Create a Direct Connect public VIF. Set up an IPsec VPN connection over the public VIF to the transit gateway. Create an attachment forAmazon S3. Use HTTPS for communication.

Correct Answer: B

Technically both B and C are possible, but with B encryption is enforced. You can prevent unencrypted S3 actions via bucket policies, but not mentioned in the question, see: https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html#example-bucket-policies-HTTP-HTTPS

In this case interface vpc endpoint for S3 is also correct, see: https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html > "You can use two types of VPC endpoints to access Amazon S3: gateway endpoints and interface endpoints (by using AWS PrivateLink). A gateway endpoint is a gateway that you specify in your route table to access Amazon S3 from your VPC over the AWS network. Interface endpoints extend the functionality of gateway endpoints by using private IP addresses to route requests to Amazon S3 from within your VPC, on premises, or from a VPC in another AWS Region by using VPC peering or AWS Transit Gateway."

**QUESTION 13**

A company has an on-premises data center in the United States. The data center is connected to AWS by an AWS Direct Connect connection.The data center has a private VIF that is connected to a Direct Connect gateway.Recently, the company opened a new data center in Europe and established a new Direct Connect connection between the Europe data centerand AWS. A new private VIF connects to the existing Direct Connect gateway.The company wants to use Direct Connect SiteLink to set up a private network between the data center in the United States and the datacenter in Europe.Which solution will meet these requirements in the MOST operationally efficient manner?

A. Create a new public VIF from each data center. Enable SiteLink on the new public VIFs.

B. Create a new transit VIF from each data center. Enable SiteLink on the new transit VIFs.

C. Use the existing VIF from each data center. Enable SiteLink on the existing private VIFs.

D. Create a new AWS Site-to-Site VPN connection between the data centers. Configure the new connection to use SiteLink.

Correct Answer: C

https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-direct-connect-sitelink/

**QUESTION 14**

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 15**

A company plans to deploy a two-tier web application to a new VPC in a single AWS Region. The company has configured the VPC with aninternet gateway and four subnets. Two of the subnets are public and have default routes that point to the internet gateway. Two of thesubnets are private and share a route table that does not have a default route.The application will run on a set of Amazon EC2 instances that will be deployed behind an external Application Load Balancer. The EC2instances must not be directly accessible from the internet. The application will use an Amazon S3 bucket in the same Region to store data.The application will invoke S3 GET API operations and S3 PUT API operations from the EC2 instances. A network engineer must design a VPCarchitecture that minimizes data transfer cost.Which solution will meet these requirements?

A. Deploy the EC2 instances in the public subnets. Create an S3 interface endpoint in the VPC. Modify the application configuration to usethe S3 endpoint-specific DNS hostname.

B. Deploy the EC2 instances in the private subnets. Create a NAT gateway in the VPC. Create default routes in the private subnets to theNAT gateway. Connect to Amazon S3 by using the NAT gateway.

C. Deploy the EC2 instances in the private subnets. Create an S3 gateway endpoint in the VPSpecify die route table of the private subnetsduring endpoint creation to create routes to Amazon S3.

D. Deploy the EC2 instances in the private subnets. Create an S3 interface endpoint in the VPC. Modify the application configuration touse the S3 endpoint-specific DNS hostname.

Correct Answer: C

Recurring questions about gateway VPC endpoints https://repost.aws/knowledge-center/vpc-reduce-nat-gateway-transfer-costs