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.certbus.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 has deployed a new web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are inan Amazon EC2 Auto Scaling group. Enterprise customers from around the world will use the application. Employees of these enterprisecustomers will connect to the application over HTTPS from office locations.The company must configure firewalls to allow outbound traffic to only approved IP addresses. The employees of the enterprise customersmust be able to access the application with the least amount of latency.Which change should a network engineer make in the infrastructure to meet these requirements?

A. Create a new Network Load Balancer (NLB). Add the ALB as a target of the NLB.

B. Create a new Amazon CloudFront distribution. Set the ALB as the distribution\\'s origin.

C. Create a new accelerator in AWS Global Accelerator. Add the ALB as an accelerator endpoint.

D. Create a new Amazon Route 53 hosted zone. Create a new record to route traffic to the ALB.

Correct Answer: C

Global static IP - Simplify allowlisting in enterprise firewalling and IoT use cases https://aws.amazon.com/global-accelerator/

QUESTION 2

A banking company is successfully operating its public mobile banking stack on AWS. The mobile banking stack is deployed in a VPC thatincludes private subnets and public subnets. The company is using IPv4 networking and has not deployed or supported IPv6 in theenvironment. The company has decided to adopt a third-party service provider\\'s API and must integrate the API with the existing environment.The service provider\\'s API requires the use of IPv6.A network engineer must turn on IPv6 connectivity for the existing workload that is deployed in a private subnet. The company does not wantto permit IPv6 traffic from the public internet and mandates that the company\\'s servers must initiate all IPv6 connectivity. The networkengineer turns on IPv6 in the VPC and in the private subnets.Which solution will meet these requirements?

A. Create an internet gateway and a NAT gateway in the VPC. Add a route to the existing subnet route tables to point IPv6 traffic to theNAT gateway.

B. Create an internet gateway and a NAT instance in the VPC. Add a route to the existing subnet route tables to point IPv6 traffic to theNAT instance.

C. Create an egress-only Internet gateway in the VPAdd a route to the existing subnet route tables to point IPv6 traffic to the egress-onlyinternet gateway.

D. Create an egress-only internet gateway in the VPC. Configure a security group that denies all inbound traffic. Associate the securitygroup with the egress-only internet gateway.

Correct Answer: C

A. NAT Gateway does not support IPv6

B. NAT Instance will be on Public subnet where IPv6 is not enabled.

C. Works

D. You don\\'t to explicitly deny inbound access to EO GW. It is its default functionality.

QUESTION 3

A company has a transit gateway in AWS Account A. The company uses AWS Resource Access Manager (AWS RAM) to share the transit gateway so that users in other accounts can connect to multiple VPCs in the same AWS Region. AWS Account B contains a VPC (10.0.0.0/16) with subnet 10.0.0.0/24 in the us-west-2a Availability Zone and subnet 10.0.1.0/24 in the us-west-2b Availability Zone. Resources in these subnets can communicate with other VPCs.

A network engineer creates two new subnets: 10.0.2.0/24 in the us-west-2b Availability Zone and 10.0.3.0/24 in the us-west-2c Availability Zone. All the subnets share one route table. The default route 0.0.0.0/0 is pointing to the transit gateway. Resources in subnet 10.0.2.0/24 can communicate with other VPCs, but resources in subnet 10.0.3.0/24 cannot communicate with other VPCs.

What should the network engineer do so that resources in subnet 10.0.3.0/24 can communicate with other VPCs?

A. In Account B, add 10.0.2.0/24 and 10.0.3.0/24 as the destinations to the route table. Use the transit gateway as the target.

B. In Account B, update the transit gateway attachment. Attach the new subnet ID that is associated with us-west-2c to Account B\\'s VPC.

C. In Account A, create a static route for 10.0.3.0/24 in the transit gateway route tables.

D. In Account A, recreate propagation for 10.0.0.0/16 in the transit gateway route tables.

Correct Answer: C

QUESTION 4

A company uses a 1 Gbps AWS Direct Connect connection to connect its AWS environment to its on-premises data center. The connectionprovides employees with access to an application VPC that is hosted on AWS. Many remote employees use a company-provided VPN toconnect to the data center. These employees are reporting slowness when they access the application during business hours. On-premisesusers have started to report similar slowness while they are in the office.The company plans to build an additional application on AWS. On-site and remote employees will use the additional application. After thedeployment of this additional application, the company will need 20% more bandwidth than the company currently uses. With the increasedusage, the company wants to add resiliency to the AWS connectivity. A network engineer must review the current implementation and mustmake improvements within a limited budget.What should the network engineer do to meet these requirements MOST cost-effectively?

A. Set up a new 1 Gbps Direct Connect dedicated connection to accommodate the additional traffic load from remote employees and theadditional application. Create a link aggregation group (LAG).

B. Deploy an AWS Site-to-Site VPN connection to the application VPC. Configure the on-premises routing for the remote employees toconnect to the Site-to-Site VPN connection.

C. Deploy Amazon Workspaces into the application VPInstruct the remote employees to connect to Workspaces.

D. Replace the existing 1 Gbps Direct Connect connection with two new 2 Gbps Direct Connect hosted connections. Create an AWS ClientVPN endpoint in the application VPC. Instruct the remote employees to connect to the Client VPN endpoint.

Correct Answer: D

A) If current 1 Gbps Direct Connect is not enough for on-premises users adding another 1 Gbps Direct Connect will not add resiliency. In case of one Direct Connect link failure there will be not enough bandwidth. Especially with new app and

increased by 20% usage.

B) No resiliency. In case of VPN S2S failure 1 Gbps Direct connect won\\'t be sufficient for on-premises and remote users.

C) Very expensive

D) Should work. In case of one link failure single 2 Gbps Direct Connect hosted connection will be sufficient to handle all the traffic for on-premises users. Remote users will connect by AWS client VPN directly to VPC.

QUESTION 5

A company has a total of 30 VPCs. Three AWS Regions each contain 10 VPCs. The company has attached the VPCs in each Region to a transit gateway in that Region. The company also has set up inter-Region peering connections between the transit gateways.

The company wants to use AWS Direct Connect to provide access from its on-premises location for only four VPCs across the three Regions. The company has provisioned four Direct Connect connections at two Direct Connect locations.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

A. Create four virtual private gateways. Attach the virtual private gateways to the four VPCs.

B. Create a Direct Connect gateway. Associate the four virtual private gateways with the Direct Connect gateway.

C. Create four transit VIFs on each Direct Connect connection. Associate the transit VIFs with the Direct Connect gateway.

D. Create four transit VIFs on each Direct Connect connection. Associate the transit VIFs with the four virtual private gateways.

E. Create four private VIFs on each Direct Connect connection to the Direct Connect gateway.

F. Create an association between the Direct Connect gateway and the transit gateways.

Correct Answer: ABE

QUESTION 6

A company is migrating an application to the AWS Cloud. The company has successfully provisioned and tested connectivity between AWS Direct Connect and the company\\'s on-premises data center. The application runs on Amazon EC2 instances across multiple Availability Zones. The instances are in an Auto Scaling group.

The application communicates through HTTPS to a third-party vendor\\'s data service that is hosted at the company\\'s data center. The data service implements a static ACL through explicit allow listing of client IP addresses.

A network engineer must design a network solution so that the migrated application can continue to access the vendor\\'s data service as the application scales.

Which solution will meet these requirements with the LEAST amount of ongoing change to the vendor\\'s allow list?

A. Configure a private NAT gateway in the subnets for each Availability Zone that the application runs in. Configure the application to target the NAT gateways instead of the data service directly. Update the data service\\'s allow list to include the IP addresses of the NAT gateways.

B. Configure an elastic network interface in the subnets for each Availability Zone that the application runs in. Associate the elastic network interfaces with the Auto Scaling group for the application. Update the data service\\'s allow list to include the IP addresses of the elastic network interfaces.

C. Configure an elastic network interface in the subnets for each Availability Zone that the application runs in. Launch an EC2 instance into each subnet. Attach the respective elastic network interfaces to the new EC2 instances. In the application subnet route tables, configure the new EC2 instances as the next destination for the data service. Update the data service\\'s allow list to include the IP addresses of the elastic network interfaces.

D. Configure an Application Load Balancer (ALB) in the subnets for each Availability Zone that the application runs in. Configure an ALB-associated target group that contains a target that uses the IP address for the data service. Configure the application to target the ALB instead of the data service directly. Update the data service\\'s allow list to include the IP addresses of the ALBs.

Correct Answer: D

QUESTION 7

A company has deployed a multi-VPC environment in the AWS Cloud. The company uses a transit gateway to connect all the VPCs together. Inthe past, the company has experienced a loss of connectivity between applications after changes to security groups, network ACLs, and routetables in a VPC. When these changes occur, the company wants to automatically verify that connectivity still exists between differentresources in a single VPC.

A. Create a list of paths between different resources to check in VPC Reachability Analyzer. Create an Amazon EventBridge rule to monitorwhen a change is made and logged in Amazon CloudWatch. Configure the rule to invoke an AWS Lambda function to test the differentpaths in Reachability Analyzer.

B. Create a list of paths between different resources to check in VPC Reachability Analyzer. Create an Amazon EventBridge rule to monitorwhen a change is made and logged in AWS. CloudTrail. Configure the rule to invoke an AWS Lambda function to test the different paths inReachability Analyzer.

C. Create a list of paths to check in AWS Transit Gateway Network Manager Route Analyzer. Create an Amazon EventBridge rule to monitorwhen a change is made and logged in Amazon CloudWatch. Configure the rule to invoke an AWS Lambda function to test the diffidentpaths in Route Analyzer.

D. Create a list of paths to check in AWS Transit Gateway Network Manager Route Analyzer. Create an Amazon EventBridge rule to monitorwhen a change is made and logged in AWS CloudTrail. Configure the rule to invoke an AWS Lambda function to test the different paths inRoute Analyzer.

Correct Answer: B

https://docs.aws.amazon.com/vpc/latest/reachability/what-is-reachability-analyzer.html

QUESTION 8

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 9

A data analytics company has a 100-node high performance computing (HPC) cluster. The HPC cluster is for parallel data processing and ishosted in a VPC in the AWS Cloud. As part of the data processing workflow, the HPC cluster needs to perform several DNS queries to resolveand connect to Amazon RDS databases, Amazon S3 buckets, and on-premises data stores that are accessible through AWS Direct Connect. TheHPC cluster can increase in size by five to seven times during the company\\'s peak event at the end of the year.The company is using two Amazon EC2 instances as primary DNS servers for the VPC. The EC2 instances are configured to forward queries tothe default VPC resolver for Amazon Route 53 hosted domains and to the on-premises DNS servers for other on-premises hosted domainnames. The company notices job failures and finds that DNS queries from the HPC cluster nodes failed when the nodes tried to resolve RDSand S3 bucket endpoints.Which architectural change should a network engineer implement to provide the DNS service in the MOST scalable way?

A. Scale out the DNS service by adding two additional EC2 instances in the VPC. Reconfigure half of the HPC cluster nodes to use thesenew DNS servers. Plan to scale out by adding additional EC2 instance-based DNS servers in the future as the HPC cluster size grows.

B. Scale up the existing EC2 instances that the company is using as DNS servers. Change the instance size to the largest possibleinstance size to accommodate the current DNS load and the anticipated load in the future.

C. Create Route 53 Resolver outbound endpoints. Create Route 53 Resolver rules to forward queries to on-premises DNS servers for onpremises hosted domain names. Reconfigure the HPC cluster nodes to use the default VPC resolver instead of the EC2 instance-basedDNS servers. Terminate the EC2 instances.

D. Create Route 53 Resolver inbound endpoints. Create rules on the on-premises DNS servers to forward queries to the default VPCresolver. Reconfigure the HPC cluster nodes to forward all DNS queries to the on-premises DNS servers. Terminate the EC2 instances.

Correct Answer: C

The VPC+2 addresses that those two EC2-based DNS use have a limit of 1024 queries per second. So we must get rid of them. We use the route 53 resolver, and for that we need an outgoing endpoint that can forwards queries to the ompprem zones.

QUESTION 10

A software-as-a-service (SaaS) company is migrating its private SaaS application to AWS. The company has hundreds of customers thatconnect to multiple data centers by using VPN tunnels. As the number of customers has grown, the company has experienced more difficultyin its effort to manage routing and segmentation of customers with complex NAT rules.After the migration to AWS is complete, the company\\'s AWS customers must be able to access the SaaS application directly from their VPCs.Meanwhile, the company\\'s on-premises customers still must be able to connect through IPsec encrypted tunnels.Which solution will meet these requirements?

A. Connect the AWS customer VPCs to a shared transit gateway. Use AWS Site-to-Site VPN connections to the transit gateway for the on-premises customers

B. Use AWS PrivateLink to connect the AWS customers. Use a third-party routing appliance in the SaaS application VPC to terminateonpremises Site-to-Site VPN connections.

C. Peer each AWS customer\\'s VPCs to the VPC that hosts the SaaS application. Create AWS Site-to-Site VPN connections on the SaaS VPCvirtual private gateway.

D. Use Site-to-Site VPN tunnels to connect each AWS customer\\'s VPCs to the VPC that hosts the SaaS application. Use AWS Site-to-SiteVPN to connect the on-premises customers.

Correct Answer: B

The is an adjustable limit of 50 with s2s vpn connections and customer gateways per Region. https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-limits.html Private link for connecting from customer\\'s vpc and third party appliances for multiple s2s vpn connections with customers data centers seems to be the best solution

QUESTION 11

A company\\'s network engineer must implement a cloud-based networking environment for a network operations team to centrally manage. Other Teams will use the environment. Each team must be able to deploy infrastructure to the environment and must be able to manage its own resources. The environment must feature IPv4 and IPv6 support and must provide internet connectivity in a dual-stack configuration.

The company has an organization in AWS Organizations that contains a workload account for the teams. The network engineer creates a new networking account in the organization.

Which combination of steps should the network engineer take next to meet the requirements? (Choose three.)

A. Create a new VPC. Associate an IPv4 CIDR block of 10.0.0.0/16 and specify an IPv6 block of 2001:db8:c5a:6000::/56. Provision subnets by assigning /24 IPv4 CIDR blocks and /64 IPv6 CIDR blocks.

B. Create a new VPC. Associate an IPv4 CIDR block of 10.0.0.0/16 and use an Amazon-provided IPV6 CIDR block. Provision subnets by assigning /24 IPv4 CIDR blocks and /64 IPV6 CIDR blocks.

C. Enable sharing of resources within the organization by using AWS Resource Access Manager (AWS RAM). Create a resource share in the networking account, select the provisioned subnets, and share the provisioned subnets with the target workload account. Use the workload account to accept the resource share through AWS RAM.

D. Enable sharing of resources within the organization by using AWS Resource Access Manager (AWS RAM). Create a resource share in the networking account, select the new VPC, and share the new VPC with the target workload account. Use the workload account to accept the resource share through AWS RAM.

E. Create an internet gateway and an egress-only internal gateway. Deploy NAT gateways to the public subnets. Associate the internet gateway with the new VPC. Update the route tables. Associate the route tables with the relevant subnets.

F. Create an internet gateway. Deploy NAT instances to public subnets. Update the route tables. Associate the route tables with the relevant subnets.

Correct Answer: ACE

QUESTION 12

A company has an AWS Site-to-Site VPN connection between its office and its VPC. Users report occasional failure of the connection to theapplication that is hosted inside the VPC. A network engineer discovers in the customer gateway logs that the Internet Key Exchange (IKE)session ends when the connection to the application fails.What should the network engineer do to bring up the IKE session if the IKE session goes down?

A. Set the dead peer detection (DPD) timeout action to Clear. Initiate traffic from the VPC to on premises.

B. Set the dead peer detection (DPD) timeout action to Restart. Initiate traffic from on premises to the VPC.

C. Set the dead peer detection (DPD) timeout action to None. Initiate traffic from the VPC to on premises.

D. Set the dead peer detection (DPD) timeout action to Cancel. Initiate traffic from on premises to the VPC.

Correct Answer: B

https://docs.aws.amazon.com/vpn/latest/s2svpn/initiate-vpn-tunnels.html

QUESTION 13

A company wants to use an AWS Network Firewall firewall to secure its workloads in the cloud through network traffic inspection. The company must record complete metadata information, such as source/destination IP addresses and protocol type. The company must also record all network traffic flows and any DROP or ALERT actions that the firewall takes for traffic that the firewall processes. The Network Firewall endpoints are placed in the correct subnets, and the VPC route tables direct traffic to the Network Firewall endpoints on the path to and from the internet.

How should a network engineer configure the firewall to meet these requirements?

A. Create a firewall policy to ensure that traffic is processed by stateless or stateful rules according to needs. Select Amazon CloudWatch Logs as the destination for the flow logs.

B. Create a firewall policy to ensure that traffic is processed by stateless or stateful rules according to needs. Configure Network Firewall logging for alert logs and flow logs.

Select a destination for logs separately for stateful and stateless engines.

C. Create a firewall policy to ensure that a stateful engine processes all the traffic. Configure Network Firewall logging for alert logs and flow logs. Select a destination for alert logs and flow logs.

D. Create a firewall policy to ensure that a stateful engine processes all the traffic. Configure VPC flow logs for the subnets that the firewall protects. Select a destination for the flow logs.

Correct Answer: B

QUESTION 14

A government contractor is designing a multi-account environment with multiple VPCs for a customer. A network security policy requires alltraffic between any two VPCs to be transparently inspected by a third-party appliance.The customer wants a solution that features AWS Transit Gateway. The setup must be highly available across multiple Availability Zones, andthe solution needs to support automated failover. Furthermore, asymmetric routing is not supported by the inspection appliances.Which combination of steps is part of a solution that meets these requirements? (Choose two.)

A. Deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection VPC. Connect theinspection VPC to the transit gateway by using a VPC attachment. Create a target group, and register the appliances with the targetgroup. Create a Network Load Balancer (NLB), and set it up to forward to the newly created target group. Configure a default route in theinspection VPCs transit gateway subnet toward the NLB.

B. Deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection VPC. Connect theinspection VPC to the transit gateway by using a VPC attachment. Create a target group, and register the appliances with the targetgroup. Create a Gateway Load Balancer, and set it up to forward to the newly created target group. Configure a default route in theinspection VPC\\'s transit gateway subnet toward the Gateway Load Balancer endpoint.

C. Configure two route tables on the transit gateway. Associate one route table with all the attachments of the application VPCs.Associate the other route table with the inspection VPC\\'s attachment. Propagate all VPC attachments into the inspection route table.Define a static default route in the application route table. Enable appliance mode on the attachment that connects the inspection VPC.

D. Configure two route tables on the transit gateway. Associate one route table with all the attachments of the application VPCs.Associate the other route table with the inspection VPCs attachment. Propagate all VPC attachments into the application route table.Define a static default route in the inspection route table. Enable appliance mode on the attachment that connects the inspection VPC.

E. Configure one route table on the transit gateway. Associate the route table with all the VPCs. Propagate all VPC attachments into theroute table. Define a static default route in the route table.

Correct Answer: BC

B and C, GLB better for 3rd party appliance, TGW RT associated to APP VPCs has a single route to the Inspection VPC and second TGW RT for the inspection VPC has all APP VPC CIDRs propagated to it.

QUESTION 15

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.