Vendor: Amazon

Exam Code:ANS-C01

Exam Name:AWS Certified Advanced Networking Specialty Exam

Version: Demo

QUESTION 1

A company needs to transfer data between its VPC and its on-premises data center. The data must travel through a connection that hasdedicated bandwidth. The data also must be encrypted in transit. The company has been working with an AWS Partner Network (APN) Partnerto establish the connection.Which combination of steps will meet these requirements? (Choose three.)

A. Request a hosted connection from the APN Partner.

B. Request a hosted public VIF from the APN Partner.

C. Create an AWS Site-to-Site VPN connection.

D. Create an AWS Client VPN connection.

E. Create a private VIF.

F. Create a public VIF.

Correct Answer: ACF

You need public VIF in order to create a Site-to-Site VPN connection.

QUESTION 2

A company operates its IT services through a multi-site hybrid infrastructure. The company deploys resources on AWS in the us-east-1 Regionand in the eu-west-2 Region. The company also deploys resources in its own data centers that are located in the United States (US) and in theUnited Kingdom (UK). In both AWS Regions, the company uses a transit gateway to connect 15 VPCs to each other. The company has createda transit gateway peering connection between the two transit gateways. The VPC CIDR blocks do not overlap with each other or with IPaddresses used within the data centers. The VPC CIDR prefixes can also be aggregated either on a Regional level or for the company\\'s entireAWS environment.The data centers are connected to each other by a private WAN connection. IP routing information is exchanged dynamically through InteriorBGP (iBGP) sessions. The data centers maintain connectivity to AWS through one AWS Direct Connect connection in the US and one DirectConnect connection in the UK. Each Direct Connect connection is terminated on a Direct Connect gateway and is associated with a localtransit gateway through a transit VIF.Traffic follows the shortest geographical path from source to destination. For example, packets from the UK data center that are targeted toresources in eu-west-2 travel across the local Direct Connect connection. In cases of cross-Region data transfers, such as from the UK datacenter to VPCs in us-east-1, the private WAN connection must be used to minimize costs on AWS. A network engineer has configured eachtransit gateway association on the Direct Connect gateway to advertise VPC-specific CIDR IP prefixes only from the local Region. The routestoward the other Region must be learned through BGP from the routers in the other data center in the original, non-aggregated form.The company recently experienced a problem with cross-Region data transfers because of issues with its private WAN connection. Thenetwork engineer needs to modify the routing setup to prevent similar interruptions in the future. The solution cannot modify the originaltraffic routing goal when the network is operating normally.Which modifications will meet these requirements? (Choose two.)

A. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection. Add the company\\'sentire AWS environment aggregate route to the list of subnets advertised through the local Direct Connect connection.

B. Add the CIDR prefixes from the other Region VPCs and the local VPC CIDR blocks to the list of subnets advertised through the localDirect Connect connection. Configure data center routers to make routing decisions based on the BGP communities received.

C. Add the aggregate IP prefix for the other Region and the local VPC CIDR blocks to the list of subnets advertised through the local DirectConnect connection.

D. Add the aggregate IP prefix for the company\\'s entire AWS environment and the local VPC CIDR blocks to the list of subnets advertisedthrough the local Direct Connect connection.

E. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection. Add both Regionalaggregate IP prefixes to the list of subnets advertised through the Direct Connect connection on both sides of the network. Configure datacenter routers to make routing decisions based on the BGP communities received.

Correct Answer: CE

If the private WAN failed, the network engineer would swing the traffic to the other region through the local Direct Connect and the Transit Gateways. That is the requirement.

The solution is that the local DC has 2 kinds of route to the other region VPCs. One is the existing CIDR-based routes via the private WAN, another is the advertised aggregated routes from the local Direct Connect connection. CIDR-based

routes are prior to the aggregated routes advertised from Direct Connect connection due to the longest prefix match routing algorithm.

The options which match this solution are C and E.

QUESTION 3

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 4

An international company provides early warning about tsunamis. The company plans to use IoT devices to monitor sea waves around theworld. The data that is collected by the IoT devices must reach the company\\'s infrastructure on AWS as quickly as possible. The company isusing three operation centers around the world. Each operation center is connected to AWS through Its own AWS Direct Connect connection.Each operation center is connected to the internet through at least two upstream internet service providers.The company has its own provider-independent (PI) address space. The IoT devices use TCP protocols for reliable transmission of the datathey collect. The IoT devices have both landline and mobile internet connectivity. The infrastructure and the solution will be deployed inmultiple AWS Regions. The company will use Amazon Route 53 for DNS services.A network engineer needs to design connectivity between the IoT devices and the services that run in the AWS Cloud.Which solution will meet these requirements with the HIGHEST availability?

A. Set up an Amazon CloudFront distribution with origin failover. Create an origin group for each Region where the solution is deployed.

B. Set up Route 53 latency-based routing. Add latency alias records. For the latency alias records, set the value of Evaluate Target Healthto Yes.

C. Set up an accelerator in AWS Global Accelerator. Configure Regional endpoint groups and health checks.

D. Set up Bring Your Own IP (BYOIP) addresses. Use the same PI addresses for each Region where the solution is deployed.

Correct Answer: C

https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html
https://docs.aws.amazon.com/global-accelerator/latest/dg/using-byoip.html

---

QUESTION 5

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 6

A company is using a shared services VPC with two domain controllers. The domain controllers are deployed in the company\\'s privatesubnets. The company is deploying a new application into a new VPC in the account. The application will be deployed onto an Amazon EC2 forWindows Server instance in the new VPC. The instance must join the existing Windows domain that is supported by the domain controllers inthe shared services VPC.A transit gateway is attached to both the shared services VPC and the new VPC. The company has updated the route tables for the transitgateway, the shared services VPC, and the new VPC. The security groups for the domain controllers and the instance are updated and allowtraffic only on the ports that are necessary for domain operations. The instance is unable to join the domain that is hosted on the domaincontrollers.Which combination of actions will help identify the cause of this issue with the LEAST operational overhead? (Choose two.)

A. Use AWS Network Manager to perform a route analysis for the transit gateway network. Specify the existing EC2 instance as the source.Specify the first domain controller as the destination. Repeat the route analysis for the second domain controller.

B. Use port mirroring with the existing EC2 instance as the source and another EC2 instance as the target to obtain packet captures of theconnection attempts.

C. Review the VPC flow logs on the shared services VPC and the new VPC.

D. Issue a ping command from one of the domain controllers to the existing EC2 instance.

E. Ensure that route propagation is turned off on the shared services VPC.

Correct Answer: AC

To identify the cause of this issue with the least operational overhead, you can use AWS Network Manager to perform a route analysis for the transit gateway network. You can specify the existing EC2 instance as the source and one of the domain controllers as the destination. You can repeat the route analysis for the second domain controller. This will help you verify if there is any routing issue between the EC2 instance and the domain controllers through the transit gateway.

You can also review the VPC flow logs on the shared services VPC and the new VPC. VPC flow logs capture information about accepted and rejected IP traffic in your VPCs. You can use VPC flow logs to troubleshoot connectivity issues or monitor network traffic in your VPCs. You can view VPC flow logs in Amazon CloudWatch Logs or Amazon S3.

QUESTION 7

A company has two AWS Direct Connect links. One Direct Connect link terminates in the us-east-1 Region, and the other Direct Connect linkterminates in the af-south-1 Region. The company is using BGP to exchange routes with AWS.How should a network engineer configure BGP to ensure that af-south-1 is used as a secondary link to AWS?

A. . On the Direct Connect link to us-east-1, configure BGP peering to use community tag 7224:7100. On the Direct Connect link to af-south-1, configure BGP peering to use community tag 7224:7300. On the Direct Connect BGP peer to useast-1, set the local preference value to 200. On the Direct Connect BGP peer to af-south-1, set the local preference value to 50

B. . On the Direct Connect link to us-east-1, configure BGP peering to use community tag 7224:7300. On the Direct

Connect link to af-south-1, configure BGP peering to use community tag 7224:7100. On the Direct Connect BGP peer to useast-1, set the local preference value to 200. On the Direct Connect BGP peer to af-south-1, set the local preference value to 50

C. . On the Direct Connect link to us-east-1, configure BGP peering to use community tag 7224:7100. On the Direct Connect link to af-south-1, configure BGP peering to use community tag 7224:7300. On the Direct Connect BGP peer to useast-1, set the local preference value to 50. On the Direct Connect BGP peer to af-south-1, set the local preference value to 200

D. . On the Direct Connect link to us-east-1, configure BGP peering to use community tag 7224:7300. On the Direct Connect link to af-south-1, configure BGP peering to use community tag 7224:7100. On the Direct Connect BGP peer to useast-1, set the local preference value to 50. On the Direct Connect BGP peer to af-south-1, set the local preference value to 200

Correct Answer: B

The higher the LOCAL_PREF value, the more preferred the route is.

QUESTION 8

A company\\'s development team has created a new product recommendation web service. The web service is hosted in a VPC with a CIDRblock of 192.168.224.0/19. The company has deployed the web service on Amazon EC2 instances and has configured an Auto Scaling group asthe target of a Network Load Balancer (NLB).The company wants to perform testing to determine whether users who receive product recommendations spend more money than users whodo not receive product recommendations. The company has a big sales event in 5 days and needs to integrate its existing productionenvironment with the recommendation engine by then. The existing production environment is hosted in a VPC with a CIDR block of192.168.128 0/17.A network engineer must integrate the systems by designing a solution that results in the least possible disruption to the existingenvironments.Which solution will meet these requirements?

A. Create a VPC peering connection between the web service VPC and the existing production VPC. Add a routing rule to the appropriateroute table to allow data to flow to 192.168.224.0/19 from the existing production environment and to flow to 192.168.128.0/17 from theweb service environment. Configure the relevant security groups and ACLs to allow the systems to communicate.

B. Ask the development team of the web service to redeploy the web service into the production VPC and integrate the systems there.

C. Create a VPC endpoint service. Associate the VPC endpoint service with the NLB for the web service. Create an interface VPC endpointfor the web service in the existing production VPC.

D. Create a transit gateway in the existing production environment. Create attachments to the production VPC and the web service VPC.Configure appropriate routing rules in the transit gateway and VPC route tables for 192.168.224.0/19 and 192.168.128.0/17. Configure therelevant security groups and ACLs to allow the systems to communicate.

Correct Answer: C

The CIDR ranges are overlapping, hence VPC peering or Transit Gateway will not work in this scenario.

QUESTION 9

A global company runs business applications in the us-east-1 Region inside a VPC. One of the company\\'s regional offices in London uses avirtual private gateway for an AWS Site-to-Site VPN connection tom the VPC. The company has configured a transit gateway and has set uppeering between the VPC and other VPCs that various departments in the company use.Employees at the London office are experiencing latency issues when they connect to the business applications.What should a network engineer do to reduce this latency?

A. Create a new Site-to-Site VPN connection. Set the transit gateway as the target gateway. Enable acceleration on the new Site-to-SiteVPN connection. Update the VPN device in the London office with the new connection details.

B. Modify the existing Site-to-Site VPN connection by setting the transit gateway as the target gateway. Enable acceleration on theexisting Site-to-Site VPN connection.

C. Create a new transit gateway in the eu-west-2 (London) Region. Peer the new transit gateway with the existing transit gateway. Modifythe existing Site-to-Site VPN connection by setting the new transit gateway as the target gateway.

D. Create a new AWS Global Accelerator standard accelerator that has an endpoint of the Site-to-Site VPN connection. Update the VPNdevice in the London office with the new connection details.

Correct Answer: A

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

---

QUESTION 10

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 11

A company wants to analyze TCP traffic to the internet. The traffic originates from Amazon EC2 instances in the company\\'s VPC. The EC2instances initiate connections through a NAT gateway. The required information includes source and destination IP addresses, ports, and thefirst 8 bytes of payload of TCP segments. The company needs to collect, store, and analyze all the required data points.Which solution will meet these requirements?

A. Set up the EC2 instances as VPC traffic mirror sources. Deploy software on the traffic mirror target to forward the data to AmazonCloudWatch Logs. Analyze the data by using CloudWatch Logs Insights.

B. Set up the NAT gateway as a VPC traffic mirror source. Deploy software on the traffic mirror target to forward the data to an AmazonOpenSearch Service cluster. Analyze the data by using OpenSearch Dashboards.

C. Turn on VPC Flow Logs on the EC2 instances. Specify the default format and a log destination of Amazon CloudWatch Logs. Analyzethe flow log data by using CloudWatch Logs Insights.

D. Turn on VPC Flow Logs on the EC2 instances. Specify a custom format and a log destination of Amazon S3. Analyze the flow log data byusing Amazon Athena.

Correct Answer: A

VPC Flow Logs capture metadata about the network traffic, such as source and destination IP addresses, source and destination ports, protocol, packet and byte counts, start and end times of the flow, and more. This information is useful for monitoring and troubleshooting network traffic patterns, but it does not include the payload content of TCP segments.

If you need to capture and analyze the payload data of TCP segments, you would need to use other monitoring and logging solutions, such as tapping into the network traffic with tools like Traffic Mirroring or using other packet capture mechanisms. These solutions can capture the actual data content for analysis, but they might require more advanced setup and configuration compared to VPC Flow Logs.

QUESTION 12

A company has deployed a critical application on a fleet of Amazon EC2 instances behind an Application Load Balancer. The application mustalways be reachable on port 443 from the public internet. The application recently had an outage that resulted from an incorrect change tothe EC2 security group.A network engineer needs to automate a way to verify the network connectivity between the public internet and the EC2 instances whenever achange is made to the security group. The solution also must notify the network engineer when the change affects the connection.Which solution will meet these requirements?

A. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture REJECT traffic on port 443. Publish the flow logrecords to a log group in Amazon CloudWatch Logs. Create a CloudWatch Logs metric filter for the log group for rejected traffic. Create analarm to notify the network engineer.

B. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture all traffic on port 443. Publish the flow logrecords to a log group in Amazon CloudWatch Logs. Create a CloudWatch Logs metric filter for the log group for all traffic. Create an alarmto notify the network engineer

C. Create a VPC Reachability Analyzer path on port 443. Specify the security group as the source. Specify the EC2 instances as thedestination. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change to thesecurity group affects the connection. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to the SNStopic in case the analyses fail Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function when achange to the security group occurs.

D. Create a VPC Reachability Analyzer path on port 443. Specify the internet gateway of the VPC as the source. Specify the EC2 instancesas the destination. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change tothe security group affects the connection. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to theSNS topic in case the analyses fail. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function whena change to the security group occurs.

Correct Answer: D

https://aws.amazon.com/blogs/networking-and-content-delivery/automating-connectivity-assessments-with-vpc-reachability-analyzer/