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 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 2

An Australian ecommerce company hosts all of its services in the AWS Cloud and wants to expand its customer base to the United States (US).The company is targeting the western US for the expansion.The company\\'s existing AWS architecture consists of four AWS accounts with multiple VPCs deployed in the ap-southeast-2 Region. All VPCsare attached to a transit gateway in ap-southeast-2. There are dedicated VPCs for each application service. The company also has VPCs forcentralized security features such as proxies, firewalls, and logging.The company plans to duplicate the infrastructure from ap-southeast-2 to the us-west-1 Region. A network engineer must establishconnectivity between the various applications in the two Regions. The solution must maximize bandwidth, minimize latency and minimizeoperational overhead.Which solution will meet these requirements?

A. Create VPN attachments between the two transit gateways. Configure the VPN attachments to use BGP routing between the two transitgateways.

B. Peer the transit gateways in each Region. Configure routing between the two transit gateways for each Region\\'s IP addresses.

C. Create a VPN server in a VPC in each Region. Update the routing to point to the VPN servers for the IP addresses in alternate Regions.

D. Attach the VPCs in us-west-1 to the transit gateway in ap-southeast-2.

Correct Answer: B

Only possible solution here is TGW peering and adding static routes for peering connection.

QUESTION 3

An education agency is preparing for its annual competition between schools. In the competition, students at schools from around the country solve math problems, complete puzzles, and write essays.

The IP addressing plan of all the schools is well-known and is administered centrally. The competition is hosted in the AWS Cloud and is not publicly available. All competition traffic must be encrypted in transit. Only authorized endpoints can access the competition. All the schools have firewall policies that block ICMP traffic.

A network engineer builds a solution in which all the schools access the competition through AWS Site-to-Site VPN connections. The network engineer uses BGP as the routing protocol. The network engineer must implement a solution that notifies schools when they lose connectivity and need to take action on their premises to address the issue.

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

A. Monitor the state of the VPN tunnels by using Amazon CloudWatch. Create a CloudWatch alarm that uses Amazon Simple Notification Service (Amazon SNS) to notify people at the affected school if the tunnels are down.

B. Create a scheduled AWS Lambda function that pings each school\\'s on-premises customer gateway device. Configure the Lambda function to send an Amazon Simple Notification Service (Amazon SNS) notification to people at the affected school if the ping fails.

C. Create a scheduled AWS Lambda function that uses the VPC Reachability Analyzer API to verify the connectivity. Configure the Lambda function to send an Amazon Simple Notification Service (Amazon SNS) notification to people at the affected school if failure occurs.

D. Create an Amazon CloudWatch dashboard for each school to show all CloudWatch metrics for each school\\'s Site-to-Site VPN connection. Share each dashboard with the appropriate school.

E. Create a scheduled AWS Lambda function to monitor the existence of each school\\'s routes in the VPC route table where VPN routes are propagated. Configure the Lambda function to send an Amazon Simple Notification Service (Amazon SNS) notification to people at the affected school if failure occurs.

Correct Answer: AC

QUESTION 4

A company uses a hybrid architecture and has an AWS Direct Connect connection between its on-premises data center and AWS. The companyhas production applications that run in the on-premises data center. The company also has production applications that run in a VPC. Theapplications that run in the on-premises data center need to communicate with the applications that run in the VPC. The company is usingcorp.example.com as the domain name for the on-

premises resources and is using an Amazon Route 53 private hosted zone foraws.example.com to host the VPC resources.The company is using an open-source recursive DNS resolver in a VPC subnet and is using a DNS resolver in the on-premises data center. Thecompany\\'s on-premises DNS resolver has a forwarder that directs requests for the aws.example.com domain name to the DNS resolver in theVPC. The DNS resolver in the VPC has a forwarder that directs requests for the corp.example.com domain name to the DNS resolver in the on-premises data center. The company has deckled to replace the open-source recursive DNS resolver with Amazon Route 53 Resolver endpoints.Which combination of steps should a network engineer take to make this replacement? (Choose three.)

A. Create a Route 53 Resolver rule to forward aws.example.com domain queries to the IP addresses of the outbound endpoint.

B. Configure the on-premises DNS resolver to forward aws.example.com domain queries to the IP addresses of the inbound endpoint.

C. Create a Route 53 Resolver inbound endpoint and a Route 53 Resolver outbound endpoint.

D. Create a Route 53 Resolver rule to forward aws.example.com domain queries to the IP addresses of the inbound endpoint.

E. Create a Route 53 Resolver rule to forward corp.example.com domain queries to the IP address of the on-premises DNS resolver.

F. Configure the on-premises DNS resolver to forward aws.example.com queries to the IP addresses of the outbound endpoint.

Correct Answer: BCE

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

QUESTION 5

A company is using Amazon Route 53 Resolver DNS Firewall in a VPC to block all domains except domains that are on an approved list. Thecompany is concerned that if DNS Firewall is unresponsive, resources in the VPC might be affected if the network cannot resolve any DNSqueries. To maintain application service level agreements, the company needs DNS queries to continue to resolve even if Route 53 Resolverdoes not receive a response from DNS Firewall.Which change should a network engineer implement to meet these requirements?

A. Update the DNS Firewall VPC configuration to disable fail open for the VPC.

B. Update the DNS Firewall VPC configuration to enable fail open for the VPC.

C. Create a new DHCP options set with parameter dns_firewall_fail_open=false. Associate the new DHCP options set with the VPC.

D. Create a new DHCP options set with parameter dns_firewall_fail_open=true. Associate the new DHCP options set with the VPC.

Correct Answer: B

Enabling the "fail open" feature in the Route 53 Resolver DNS Firewall VPC configuration ensures that if DNS Firewall becomes unresponsive, DNS queries will still be resolved. This helps maintain application service level agreements by allowing resources in the VPC to continue operating even if Route 53 Resolver does not receive a response from DNS Firewall.

QUESTION 6

A company deploys a software solution on Amazon EC2 instances that are in a cluster placement group. The solution\\'s UI is a single HTMLpage. The HTML file size is 1,024 bytes. The software processes files that exceed 1,024 MB in size. The software shares files over the networkto clients upon request. The files are shared with the Don\\'t Fragment flag set. Elastic network interfaces of the EC2 instances are set up withjumbo frames.The UI is always accessible from all allowed source IP addresses, regardless of whether the source IP addresses are within a VPC, on theinternet, or on premises. However, clients sometimes do not receive files that they request because the files fail to travel successfully fromthe software to the clients.Which options provide a possible root cause of these failures? (Choose two.)

A. The source IP addresses are from on-premises hosts that are routed over AWS Direct Connect.

B. The source IP addresses are from on-premises hosts that are routed over AWS Site-to-Site VPN.

C. The source IP addresses are from hosts that connect over the public internet.

D. The security group of the EC2 instances does not allow ICMP traffic.

E. The operating system of the EC2 instances does not support jumbo frames.

Correct Answer: BC

Jumbo frames allow more than 1500 bytes of data by increasing the payload size per packet, and thus increasing the percentage of the packet that is not packet overhead. Fewer packets are needed to send the same amount of usable data. However, traffic is limited to a maximum MTU of 1500 in the following cases:

Traffic over an internet gateway

Traffic over an inter-region VPC peering connection

Traffic over VPN connections

Traffic outside of a given AWS Region for EC2-Classic

If packets are over 1500 bytes, they are fragmented, or they are dropped if the Don\\'t Fragment flag is set in the IP header.

regardless the security group allows icmp traffic to enable pmtud or not, the oversized packets will be dropped anyway due to don\\'t fragment flag set.

QUESTION 7

A retail company is running its service on AWS. The company\\'s architecture includes Application Load Balancers (ALBs) in public subnets. TheALB target groups are configured to send traffic to backend Amazon EC2 instances in private subnets. These backend EC2 instances can callexternally hosted services over the internet by using a NAT gateway.The company has noticed in its billing that NAT gateway usage has increased significantly. A network engineer needs to find out the source ofthis increased usage.Which options can the network engineer use to investigate the traffic through the NAT gateway? (Choose two.)

A. Enable VPC flow logs on the NAT gateway\\'s elastic network interface. Publish the logs to a log group in Amazon CloudWatch Logs. UseCloudWatch Logs Insights to query and analyze the logs.

B. Enable NAT gateway access logs. Publish the logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to queryand analyze the logs.

C. Configure Traffic Mirroring on the NAT gateway\\'s elastic network interface. Send the traffic to an additional EC2 instance. Use tools suchas tcpdump and Wireshark to query and analyze the mirrored traffic.

D. Enable VPC flow logs on the NAT gateway\\'s elastic network interface. Publish the logs to an Amazon S3 bucket. Create a custom tablefor the S3 bucket in Amazon Athena to describe the log structure. Use Athena to query and analyze the logs.

E. Enable NAT gateway access logs. Publish the logs to an Amazon S3 bucket. Create a custom table for the S3 bucket in Amazon Athenato describe the log structure. Use Athena to query and analyze the logs.

Correct Answer: AD

A. Yes, this would work.

B. Not a real thing, wrong

C. We don\\'t need to do packet inspection to analyze costs. This won\\'t help with costs at all.

D. The most obvious right answer.

E. Like B, not a real thing.

QUESTION 8

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 9

A company has developed an application on AWS that will track inventory levels of vending machines and initiate the restocking processautomatically. The company plans to integrate this application with vending machines and deploy the vending machines in several marketsaround the world. The application resides in a VPC in the us-east-1 Region. The application consists of an Amazon Elastic Container Service(Amazon ECS) cluster behind an Application Load Balancer (ALB). The communication from the vending machines to the application happensover HTTPS.The company is planning to use an AWS Global Accelerator accelerator and configure static IP addresses of the accelerator in the vendingmachines for application endpoint access. The application must be accessible only through the accelerator and not through a directconnection over the internet to the ALB endpoint.Which solution will meet these requirements?

A. Configure the ALB in a private subnet of the VPC. Attach an internet gateway without adding routes in the subnet route tables to pointto the internet gateway. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB\\'s security groupto only allow inbound traffic from the internet on the ALB listener port.

B. Configure the ALB in a private subnet of the VPC. Configure the accelerator with endpoint groups that include the ALB endpoint.Configure the ALB\\'s security group to only allow inbound traffic from the internet on the ALB listener port.

C. Configure the ALB in a public subnet of the VPAttach an internet gateway. Add routes in the subnet route tables to point to the internetgateway. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB\\'s security group to only allowinbound traffic from the accelerator\\'s IP addresses on the ALB listener port.

D. Configure the ALB in a private subnet of the VPC. Attach an internet gateway. Add routes in the subnet route tables to point to theinternet gateway. Configure the accelerator with endpoint groups that include the ALB endpoint. Configure the ALB\\'s security group to onlyallow inbound traffic from the accelerator\\'s IP addresses on the ALB listener port.

Correct Answer: A

This is not a normal scenario of attaching IGW to EC2 instance by creating a route in subnet.

Please read the below link typically describing ELB integration with AWS Global accelator (and the last line of the extract)

https://docs.aws.amazon.com/global-accelerator/latest/dg/secure-vpc-connections.html

"When you add an internal Application Load Balancer or an Amazon EC2 instance endpoint in AWS Global Accelerator, you enable internet traffic to flow directly to and from the endpoint in Virtual Private Clouds (VPCs) by targeting it in a private subnet. The VPC that contains the load balancer or EC2 instance must have an internet gateway attached to it, to indicate that the VPC accepts internet traffic. However, you don\\'t need public IP addresses on the load balancer or EC2 instance. You also don\\'t need an associated internet gateway route for the subnet."

QUESTION 10

A company is deploying an application. The application is implemented in a series of containers in an Amazon Elastic Container Service(Amazon ECS) cluster. The company will use the Fargate launch type for its tasks. The containers will run workloads that require connectivityinitiated over an SSL connection. Traffic must be able to flow to the application from other AWS accounts over private connectivity. Theapplication must scale in a manageable way as more

consumers use the application.Which solution will meet these requirements?

A. Choose a Gateway Load Balancer (GLB) as the type of load balancer for the ECS service. Create a lifecycle hook to add new tasks to thetarget group from Amazon ECS as required to handle scaling. Specify the GLB in the service definition. Create a VPC peer for external AWSaccounts. Update the route tables so that the AWS accounts can reach the GLB.

B. Choose an Application Load Balancer (ALB) as the type of load balancer for the ECS service. Create path-based routing rules to allowthe application to target the containers that are registered in the target group. Specify the ALB in the service definition. Create a VPCendpoint service for the ALB Share the VPC endpoint service with other AWS accounts.

C. Choose an Application Load Balancer (ALB) as the type of load balancer for the ECS service. Create path-based routing rules to allowthe application to target the containers that are registered in the target group. Specify the ALB in the service definition. Create a VPCpeer for the external AWS accounts. Update the route tables so that the AWS accounts can reach the ALB.

D. Choose a Network Load Balancer (NLB) as the type of load balancer for the ECS service. Specify the NLB in the service definition.Create a VPC endpoint service for the NLB. Share the VPC endpoint service with other AWS accounts.

Correct Answer: D

Path based routing is not required here. Requirement is "Traffic must be able to flow to the application from other AWS accounts over private connectivity. " - which is a case for PrivateLink.

QUESTION 11

A financial company that is located in the us-east-1 Region needs to establish secure connectivity to AWS. The company has two on-premisesdata centers, each located within the same Region. The company\\'s network team needs to establish hybrid connectivity to its AWSenvironment with reliable and consistent connectivity.The connection must provide access to the company\\'s private resources inside its AWS environment. The resources are located in the us-east-1 and us-west-2 Regions. The connection must allow resources from the corporate networks to send large amounts of data to Amazon S3 overthe same connection. To meet compliance requirements, the connection must be highly available and must provide encryption for all packetsthat are sent between the on-premises location and any services on AWS.Which combination of steps should the network team take to meet these requirements? (Choose two.)

A. Set up a private VIF to send data to Amazon S3. Use an AWS Site-to-Site VPN connection over the private VIF to encrypt data in transitto the VPCs in us-east-1 and us-west-2.

B. Set up an AWS Direct Connect connection to each of the company\\'s data centers.

C. Set up an AWS Direct Connect connection from one of the company\\'s data centers to us-east-1 and us-west-2.

D. Set up a public VIF to send data to Amazon S3. Use an AWS Site-to-Site VPN connection over the public VIF to encrypt data in transit tothe VPCs in us-east-1 and us-west-2.

E. Set up a transit VIF for an AWS Direct Connect gateway to send data to Amazon S3. Create a transit gateway. Associate the transitgateway with the Direct Connect gateway to provide secure communications from the company\\'s data centers to the VPCs in us-east-1 andus-west-2.

Correct Answer: BD

Option B: Establishing an AWS Direct Connect connection to each of the company\\'s data centers ensures a reliable,

consistent connection. This setup also addresses the requirement for high availability. If there are problems with one connection, the other connection can maintain the data flow.

Option D: A public VIF can provide direct access to AWS services, including Amazon S3, across the Direct Connect link. By using an AWS Site-to-Site VPN connection over the public VIF, you can encrypt data in transit between the on-premises location and the VPCs in us-east-1 and us-west-2, thereby meeting the company\\'s compliance requirements.

QUESTION 12

A company has users who work from home. The company wants to move these users to Amazon WorkSpaces for additional security visibility.The company has deployed WorkSpaces in its own AWS account in VPC A. A network engineer decides to provide the security visibility byusing two firewall appliances behind a Gateway Load Balancer (GWLB). The network engineer provisions another VPC, VPC B, in a separateaccount and deploys the two firewall appliances in separate Availability Zones.What should the network engineer do to configure the network connectivity for this solution?

A. Create a GWLB in VPC A with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWSprincipal ARN of the WorkSpaces account to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPCendpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables ofVPC A to point the default route to the VPC endpoint.

B. Create a GWLB in VPC B with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWSprincipal ARN of the WorkSpaces account to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPCendpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables ofVPC A to point the default route to the GWLB endpoint.

C. Create a GWLB in VPC B with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWSprincipal ARN of the WorkSpaces account to the principal allow list of the GWLB endpoint. In the WorkSpaces account, create a VPCendpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modify the route tables ofVPC A to point the WorkSpaces subnet to the VPC endpoint.

D. Create a GWLB in VPC B with the firewall appliance instances as targets. Use the GWLB to create a GWLB endpoint. Add the AWSprincipal ARN of the account that contains the firewall appliances to the principal allow list of the GWLB endpoint. In the WorkSpacesaccount, create a VPC endpoint and specify the service name that the AWS Management Console provides for the GWLB endpoint. Modifythe route tables of VPC A to point the default route to the VPC endpoint.

Correct Answer: B

Using AWS PrivateLink, GWLB Endpoint routes traffic to GWLB. Traffic is routed securely over Amazon network without any additional configuration.

QUESTION 13

A company has a VPC in the AWS Cloud. The company recently acquired a competitor that also has a VPC the AWS Cloud. A network engineer discovers an IP address overlap between the two VPCs. Both VPCs require access to an AWS Marketplace partner service.

Which solution will ensure interoperability among the VPC hosted services and the AWS Markelplace partner service?

A. Configure VPC peering with static routing between the VPCs. Configure an AWS Site-to-Site VPN connection with

static routing to the partner service.

B. Configure a NAT gateway in the VPCs. Configure default routes in each VPC to point to the local NAT gateway. Attach each NAT gateway to a transit gateway. Configure an AWS Site-to-Site VPN connection with static routing to the partner service.

C. Configure AWS PrivateLink to facilitate connectivity between the VPCs and the partner service. Use the DNS name that is created with the associated interface endpoints to route traffic between the VPCs and the partner service.

D. Configure a NAT instance in the VPCs. Configure default routes in each VPC to point to the local NAT instance. Configure an interface endpoint in each VPC to connect to the partner service. Use the DNS name that is created with the associated interface endpoints to route traffic between the VPCs and the partner service.

Correct Answer: C

QUESTION 14

A company uses an AWS Direct Connect private VIF with a link aggregation group (LAG) that consists of two 10 Gbps connections. Thecompany\\'s security team has implemented a new requirement for external network connections to provide layer 2 encryption. The company\\'snetwork team plans to use MACsec support for Direct Connect to meet the new requirement.Which combination of steps should the network team take to implement this functionality? (Choose three.)

A. Create a new Direct Connect LAG with new circuits and ports that support MACsec.

B. Associate the MACsec Connectivity Association Key (CAK) and the Connection Key Name (CKN) with the new LAG.

C. Associate the Internet Key Exchange (IKE) with the existing LAG.

D. Configure the MACsec encryption mode on the existing LAG.

E. Configure the MACsec encryption mode on the new LAG.

F. Configure the MACsec encryption mode on each Direct Connect connection that makes up the existing LAG.

Correct Answer: ABE

To start using MACsec, you must turn the feature on when you create a dedicated connection
https://docs.aws.amazon.com/directconnect/latest/UserGuide/create-lag.html
https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-mac-sec-getting-started.html
https://docs.aws.amazon.com/directconnect/latest/UserGuide/associate-key-lag.html

QUESTION 15

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