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.geekcert.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 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 2

A marketing company is using hybrid infrastructure through AWS Direct Connect links and a software-defined wide area network (SD-WAN)overlay to connect its branch offices. The company connects multiple VPCs to a third-party SD-WAN appliance transit VPC within the sameaccount by using AWS Site-to-Site VPNs.The company is planning to connect more VPCs to the SD-WAN appliance transit VPC. However, the company faces challenges of scalability,route table limitations, and higher costs with the existing architecture. A network engineer must design a solution to resolve these issues andremove dependencies.Which solution will meet these requirements with the LEAST amount of operational overhead?

A. Configure a transit gateway to attach the VPCs. Configure a Site-to-Site VPN connection between the transit gateway and the third-partySD-WAN appliance transit VPC. Use the SD-WAN overlay links to connect to the branch offices.

B. Configure a transit gateway to attach the VPCs. Configure a transit gateway Connect attachment for the third-party SD-WAN appliancetransit VPC. Use transit gateway Connect native integration of SD-WAN virtual hubs with AWS Transit Gateway.

C. Configure a transit gateway to attach the VPCs. Configure VPC peering between the VPCs and the third-party SD-WAN appliance transitVPUse the SD-WAN overlay links to connect to the branch offices.

D. Configure VPC peering between the VPCs and the third-party SD-WAN appliance transit VPC. Use transit gateway Connect nativeintegration of SD-WAN virtual hubs with AWS Transit Gateway.

Correct Answer: B

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-sd-wan.html

QUESTION 3

A company has a public application. The application uses an Application Load Balancer (ALB) that has a target group of Amazon EC2 instances.

The company wants to protect the application from security issues in web requests. The traffic to the application must have end-to-end encryption. Which solution will meet these requirements?

A. Configure a Network Load Balancer (NLB) that has a target group of the existing EC2 instances. Configure TLS connections to terminate on the EC2 instances that use a public certificate. Configure an AWS WAF web ACL. Associate the web ACL with the NLB.

B. Configure TLS connections to terminate at the ALB that uses a public certificate. Configure AWS Certificate Manager (ACM) certificates for the communication between the ALB and the EC2 instances. Configure an AWS WAF web ACL. Associate the web ACL with the ALB.

C. Configure a Network Load Balancer (NLB) that has a target group of the existing EC2 instances. Configure TLS connections to terminate at the EC2 instances by creating a TLS listener. Configure self-signed certificates on the EC2 instances for the communication between the NLB and the EC2 instances. Configure an AWS WAF web ACL. Associate the web ACL with the NLB.

D. Configure a third-party certificate on the EC2 instances for the communication between the ALB and the EC2 instances. Import the third-party certificate into AWS Certificate Manager (ACM). Associate the imported certificate with the ALB. Configure TLS connections to terminate at the ALB. Configure an AWS WAF web ACL. Associate the web ACL with the ALB.

Correct Answer: B

QUESTION 4

An ecommerce company is hosting a web application on Amazon EC2 instances to handle continuously changing customer demand. The EC2instances are part of an Auto Scaling group. The company wants to implement a solution to distribute traffic from customers to the EC2instances. The company must encrypt all traffic at all stages between the customers and the application servers. No decryption atintermediate points is allowed.Which solution will meet these requirements?

A. Create an Application Load Balancer (ALB). Add an HTTPS listener to the ALB. Configure the Auto Scaling group to register instanceswith the ALB\\'s target group.

B. Create an Amazon CloudFront distribution. Configure the distribution with a custom SSL/TLS certificate. Set the Auto Scaling group asthe distribution\\'s origin.

C. Create a Network Load Balancer (NLB). Add a TCP listener to the NLB. Configure the Auto Scaling group to register instances with theNLB\\'s target group.

D. Create a Gateway Load Balancer (GLB). Configure the Auto Scaling group to register instances with the GLB\\'s

target group.

Correct Answer: C

If you need to pass encrypted traffic to the targets without the load balancer decrypting it, create a TCP listener on port 443 instead of creating a TLS listener. https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html

QUESTION 5

A company is moving its record-keeping application to the AWS Cloud. All traffic between the company\\'s on-premises data center and AWSmust be encrypted at all times and at every transit device during the migration.The application will reside across multiple Availability Zones in a single AWS Region. The application will use existing 10 Gbps AWS DirectConnect dedicated connections with a MACsec capable port. A network engineer must ensure that the Direct Connect connection is securedaccordingly at every transit device.The network engineer creates a Connection Key Name and Connectivity Association Key (CKN/CAK) pair for the MACsec secret key.Which combination of additional steps should the network engineer take to meet the requirements? (Choose two.)

A. Configure the on-premises router with the MACsec secret key.

B. Update the connection\\'s MACsec encryption mode to must_encrypt. Then associate the CKN/CAK pair with the connection.

C. Update the connection\\'s MACsec encryption mode to should encrypt. Then associate the CKN/CAK pair with the connection.

D. Associate the CKN/CAK pair with the connection. Then update the connection\\'s MACsec encryption mode to must_encrypt.

E. Associate the CKN/CAK pair with the connection. Then update the connection\\'s MACsec encryption mode to should_encrypt.

Correct Answer: AD

According to AWS, you need to do the following 4 steps in order.

1.

Create a new connection with MACsec support

2.

Associate the CKN/CAK with the connection

3.

Verify the connection status

4.

Migrate traffic to new connection as appropriate

When you first create the DX connection, the default encryption mode is should encrypt. You need to update it to must

encrypt in step 3. There\\'s no way to specify that during the creation of DX.

https://aws.amazon.com/blogs/networking-and-content-delivery/adding-macsec-security-to-aws-direct-connect-connections/

ANS-C01 VCE Dumps ANS-C01 Practice Test ANS-C01 Study Guide