AWS Certified Advanced Networking - Specialty

1. Your organization’s corporate website must be available on www.acme.com and acme.com. How should you configure Amazon Route 53 to meet this requirement?

A. Configure acme.com with an ALIAS record targeting the ELB. www.acme.com with an ALIAS record targeting the ELB.

B. Configure acme.com with an A record targeting the EL www.acme.com with a CNAME record targeting the acme.com record.

C. Configure acme.com with a CNAME record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.

D. Configure acme.com using a second ALIAS record with the ELB target. www.acme.com using a PTR record with the acme.com record target.

Answer(s): A

---

2. You are building an application in AWS that requires Amazon Elastic MapReduce (Amazon EMR). The application needs to resolve hostnames in your internal, on-premises Active Directory domain. You update your DHCP Options Set in the VPC to point to a pair of Active Directory integrated DNS servers running in your VPC.
Which action is required to support a successful Amazon EMR cluster launch?

A. Add a conditional forwarder to the Amazon-provided DNS server.

B. Enable seamless domain join for the Amazon EMR cluster.

C. Launch an AD connector for the internal domain.

D. Configure an Amazon Route 53 private zone for the EMR cluster.

Answer(s): B

---

3. You have a three-tier web application with separate subnets for Web, Applications, and Database tiers. Your CISO suspects your application will be the target of malicious activity. You are tasked with notifying the security team in the event your application is port scanned by external systems.
Which two AWS Services cloud you leverage to build an automated notification system? (Choose two.)

☐ A. Internet gateway

□ B. VPC Flow Logs

□ C. AWS CloudTrail

□ D. Lambda

□ E. AWS Inspector

Answer(s): C D

---

4. You are designing the network infrastructure for an application server in Amazon VPC. Users will access all the application instances from the Internet and from an on-premises network. The on-premises network is connected to your VPC over an AWS Direct Connect link.
How should you design routing to meet these requirements?

A. Configure a single routing table with two default routes: one to the Internet via an IGW, the other to the on-premises network via the VGW. Use this routing table across all subnets in your VPC.

B. Configure two routing tables: one that has a default route via the IGW, and another that has a default route via the VGW. Associate both routing tables with each VPC subnet.

C. Configure a single routing table with a default route via the IGW. Propagate a default route via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnet.

D. Configure a single routing table with a default route via the IGW. Propagate specific routes for the on- premises networks via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnets.

Answer(s): D

---

5. Your company decides to use Amazon S3 to augment its on-premises data store. Instead of using the company's highly controlled, on-premises Internet gateway, a Direct Connect connection is ordered to provide high bandwidth, low latency access to S3. Since the company does not own a publically routable IPv4 address block, a request was made to AWS for an AWS-owned address for a Public Virtual Interface (VIF).
The security team is calling this new connection a "backdoor", and you have been asked to clarify the risk to the company.
Which concern from the security team is valid and should be addressed?

A. AWS advertises its aggregate routes to the Internet allowing anyone on the Internet to reach the router.

B. Direct Connect customers with a Public VIF in the same region could directly reach the router.

C. EC2 instances in the same region with access to the Internet could directly reach the router.

D. The S3 service could reach the router through a pre-configured VPC Endpoint.

Answer(s): A

---

6. Your organization uses a VPN to connect to your VPC but must upgrade to a 1-G AWS Direct Connect connection for stability and performance. Your telecommunications provider has provisioned the circuit fromyour data center to an AWS Direct Connect facility and needs information on how to cross-connect (e.g., which rack/port to connect).
What is the AWS-recommended procedure for providing this information?

A. Create a support ticket. Provide your AWS account number and telecommunications company's name and where you need the Direct Connect connection to terminate.

B. Create a new connection through your AWS Management Console and wait for an email from AWS with information.

C. Ask your telecommunications provider to contact AWS through an AWS Partner Channel. Provide your AWS account number.

D. Contact an AWS Account Manager and provide your AWS account number, telecommunications company's name, and where you need the Direct Connect connection to terminate.

Answer(s): A

---

7. You manage a web service that is used by client applications deployed in 300 offices worldwide. The web service architecture is an Elastic Load balancer (ELB) distributing traffic across four application servers deployed in an autoscaling group across two availability zones.
The ELB is configured to use round robin, and sticky sessions are disabled. You have configured the NACLs and Security Groups to allow port 22 from your bastion host, and port 80 from 0.0.0.0/0. The client configuration is managed by each regional IT team.
Upon inspection you find that a large amount of requests from incorrectly configured sites are causing a single application server to degrade. The remainder of the requests are equally distributed across all servers with no negative effects.
What should you do to remedy the situation and prevent future occurrences?

A. Mark the affected instance as degraded in the ELB and raise it with the client application team.

B. Update the NACL to only allow port 80 to the application servers from the ELB servers.

C. Update the Security Groups to only allow port 80 to the application servers from the ELB.

D. Terminate the affected instance and allow Auto Scaling to create a new instance.

Answer(s): D

---

8. A multinational organization has applications deployed in three different AWS regions. These applications must securely communicate with each other by VPN. According to the organization's security team, the VPN must meet the following requirements:
-AES 128-bit encryption

-SHA-1 hashing
-User access via SSL VPN
-PFS using DH Group 2
-Ability to maintain/rotate keys and passwords
-Certificate-based authentication
Which solution should you recommend so that the organization meets the requirements?

A. AWS hardware VPN between the virtual private gateway and customer gateway

B. A third-party VPN solution deployed from AWS Marketplace

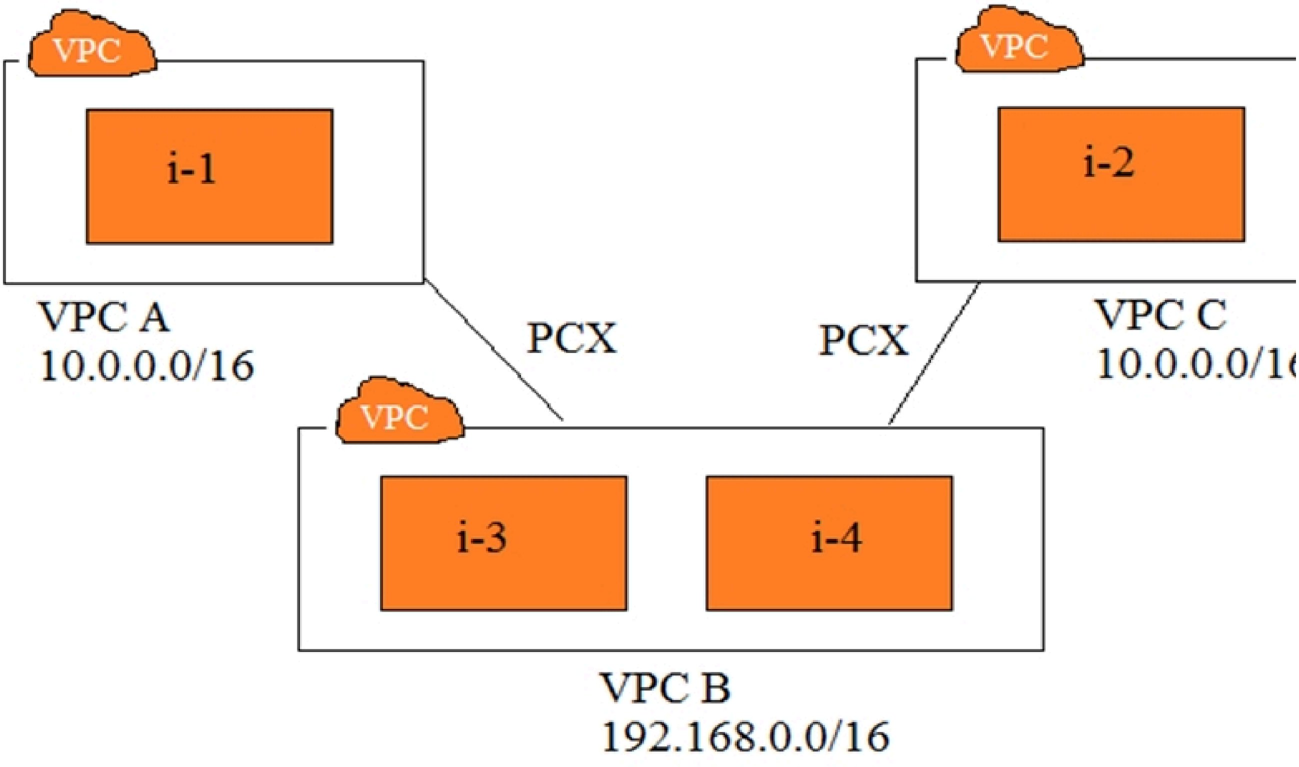
C. A private MPLS solution from an international carrier

D. AWS hardware VPN between the virtual private gateways in each region

Answer(s): D

---

9. Refer to the image.



You have three VPCs: A, B, and C. VPCs A and C are both peered with VPC B. The IP address ranges are as follows:
-VPC A: 10.0.0.0/16
-VPC B: 192.168.0.0/16
-VPC C: 10.0.0.0/16
Instance i-1 in VPC A has the IP address 10.0.0.10. Instance i-2 in VPC C has the IP address 10.0.0.10. Instances i-3 and i-4 in VPC B have the IP addresses 192.168.1.10 and 192.168.1.20, respectively, i-3 and i-4 are in the subnet 192.168.1.0/24.
-i-3 must be able to communicate with i-1
-i-4 must be able to communicate with i-2

-i-3 and i-4 are able to communicate with i-1, but not with i-2.
Which two steps will fix this problem? (Choose two.)

□ A. Create subnets 192.168.1.0/28 and 192.168.1.16/28. Move i-3 and i-4 to these subnets, respectively.

□ B. Create subnets 192.168.1.0/27 and 192.168.1.16/27. Move i-3 and i-4 to these subnets, respectively.

□ C. Change the IP address of i-2 to 10.0.0.100. Assign it an elastic IP address.

□ D. Create a new route table for VPC B, with unique route entries for destination VPC A and destination VPC C.

□ E. Create two route tables: one with a route for destination VPC A, and another for destination VPC C.

Answer(s): A E

---

10. A legacy, on-premises web application cannot be load balances effectively. There are both planned and unplanned events that cause usage spikes to millions of concurrent users. The existing infrastructure cannot handle the usage spikes. The CIO has mandated that the application be moved to the cloud to avoid further disruptions, with the additional requirement that source IP addresses be unaltered to support network traffic-monitoring needs. Which of the following designs will meet these requirements?

A. Use an Auto Scaling group of Amazon EC2 instances behind a Classic Load Balancer.

B. Use an Auto Scaling group of EC2 instances in a target group behind an Application Load Balancer.

C. Use an Auto Scaling group of EC2 instances in a target group behind a Classic Load Balancer.

D. Use an Auto Scaling group of EC2 instances in a target group behind a Network Load Balancer.

Answer(s): D

---

11. An organization processes consumer information submitted through its website. The organization’s security policy requires that personally identifiable information (PII) elements are specifically encrypted at all times and as soon as feasible when received. The front-end Amazon EC2 instances should not have access to decrypted PII. A single service within the production VPC must decrypt the PII by leveraging an IAM role.Which combination of services will support these requirements? (Choose two.)

□ A. Amazon Aurora in a private subnet

□ B. Amazon CloudFront using AWS Lambda@Edge

□ C. Customer-managed MySQL with Transparent Data Encryption

□ D. Application Load Balancer using HTTPS listeners and targets

□ E. AWS Key Management Services

Answer(s): C E

---

12. A Lambda function needs to access the private address of an Amazon ElastiCache cluster in a VPC. The Lambda function also needs to write messages to Amazon SQS. The Lambda function has been configured to run in a subnet in the VPC.
Which of the following actions meet the requirements? (Choose two.)

□ A. The Lambda function needs an IAM role to access Amazon SQS

□ B. The Lambda function must route through a NAT gateway or NAT instance in another subnet to access the public SQS API.

□ C. The Lambda function must be assigned a public IP address to access the public Amazon SQS API.

□ D. The ElastiCache server outbound security group rules must be configured to permit the Lambda function's security group.

□ E. The Lambda function must consume auto-assigned public IP addresses but not elastic IP addresses.

Answer(s): A C

---

13. You are deploying an EC2 instance in a private subnet that requires access to the Internet. One of the requirements for this solution is to restrict access to only particular URLs on a whitelist. In addition to the whitelisted URLs, the instances should be able to access any Amazon S3 bucket in the same region via any URL.Which of the following solutions should you deploy? (Choose two.)

□ A. Include s3.amazonaws.com in the whitelist.

□ B. Create a VPC endpoint for S3.

□ C. Run Squid proxy on a NAT instance.

□ D. Deploy a NAT gateway into your VPC.

□ E. Utilize a security group to restrict access.

Answer(s): C D

---

14. Your company runs an HTTPS application using an Elastic Load Balancing (ELB) load balancer/PHP on nginx server/RDS in multiple Availability Zones. You need to apply Geographic Restriction and identify the client's IP address in your application to generate dynamic content.
How should you utilize AWS services in a scalable fashion to perform this task?

A. Modify the nginx log configuration to record value in X-Forwarded-For and use CloudFront to apply the Geographic Restriction.

B. Enable ELB access logs to store the client IP address and parse these to dynamically modify a blacklist.

C. Use X-Forwarded-For with security groups to apply the Geographic Restriction

D. Modify the application code to use value of X-Forwarded-For and CloudFront to apply the Geographic Restriction.

Answer(s): A

---

15. You run a well-architected, multi-AZ application in the eu-central-1 (Frankfurt) AWS region. The application is hosted in a VPC and is only accessed from the corporate network. To support large volumes of data transfer and administration of the application, you use a single 10-Gbps AWS Direct Connect connection with multiple private virtual interfaces. As part of a review, you decide to improve the resilience of your connection to AWS and make sure that any additional connectivity does not share the same Direct Connect routers at AWS. You need to provide the best levels of resilience to meet the application's needs.Which two options should you consider? (Choose two.)

□ A. Install a second 10-Gbps Direct Connect connection to the same Direct Connection location.

□ B. Deploy an IPsec VPN over a public virtual interface on a new 10-Gbps Direct Connect connection.

□ C. Install a second 10-Gbps Direct Connect connection to a Direct Connect location in eu-west-1.

□ D. Deploy an IPsec VPN over the Internet to the eu-west-1 region for diversity.

□ E. Install a second 10-Gbps Direct Connect connection to a second Direct Connect location for eu-central-1.

Answer(s): B C

---

16. You currently use a single security group assigned to all nodes in a clustered NoSQL database. Only your cluster members in one region must be able to connect to each other. This security group uses a self-referencing rule using the cluster security group's group-id to make it easier to add or remove nodes from the cluster. You need to make this database comply with out-of-region disaster recovery requirements and ensure that the network traffic between the nodes is encrypted when travelling between regions. How should you enable secure cluster communication while deploying additional cluster members in another AWS region?

A. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group rules that reference each other's security group-id in each region.

B. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.

C. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.

D. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group rules that reference each other’s security group-id in each region.

Answer(s): D

---

17. You have to set up an AWS Direct Connect connection to connect your on-premises to an AWS VPC. Due to budget requirements, you can only provision a single Direct Connect port. You have two border gateway routersat your on-premises data center that can peer with the Direct Connect routers for redundancy. Which two design methodologies, in combination, will achieve this connectivity? (Choose two.)

☐ A. Terminate the Direct Connect circuit on a L2 border switch, which in turn has trunk connections to the two routers.

☐ B. Create two Direct Connect private VIFs for the same VPC, each with a different peer IP.

☐ C. Terminate the Direct Connect circuit on any of the one routers, which in turn will have an IBGP session with the other router.

☐ D. Create one Direct Connect private VIF for the VPC with two customer peer IPs.

☐ E. Provision two VGWs for the VPC and create one Direct Connect private VIF per VGW.

Answer(s): A D

---

18. Your organization needs to resolve DNS entries stored in an Amazon Route 53 private zone “awscloud:internal” from the corporate network. An AWS Direct Connect connection with a private virtual interface is configured to provide access to a VPC with the CIDR block 192.168.0.0/16. A DNS Resolver (BIND) is configured on an Amazon Elastic Compute Cloud (EC2) instance with the IP address 192.168.10.5 within the VPC. The DNS Resolver has standard root server hints configured and conditional forwarding for “awscloud.internal” to the IP address 192.168.0.2.
From your PC on the corporate network, you query the DNS server at 192.168.10.5 for www.amazon.com. The query is successful and returns the appropriate response. When you query for “server.awscloud.internal”, the query times out. You receive no response.
How should you enable successful queries for “server.awscloud.internal”?

A. Attach an internet gateway to the VPC and create a default route.

B. Configure the VPC settings for enableDnsHostnames and enableDnsSupport as True

C. Relocate the BIND DNS Resolver to the corporate network.

D. Update the security group for the EC2 instance at 192.168.10.5 to allow UDP Port 53 outbound.

Answer(s): B

---

19. Your company's policy requires that all VPCs peer with a "common services: VPC. This VPC contains a fleet of layer 7 proxies and an Internet gateway. No other VPC is allowed to provision an Internet gateway. You configure a new VPC and peer with the common service VPC as required by policy. You launch an Amazon EC2. Windows instance configured to forward all traffic to the layer 7 proxies in the common services VPC. The application on this server should successfully interact with Amazon S3 using its properly configured AWS Identity and Access Management (IAM) role. However, Amazon S3 is returning 403 errors to the application.
Which step should you take to enable access to Amazon S3?

A. Update the S3 bucket policy with the private IP address of the instance.

B. Exclude 169.254.169.0/24 from the instance's proxy configuration.

C. Configure a VPC endpoint for Amazon S3 in the same subnet as the instance.

D. Update the CORS configuration for Amazon S3 to allow traffic from the proxy.

Answer(s): D

---

20. A customer is using ABC Telecom as a network provider. The customer has 10 different offices connected to ABC Telecom's MPLS backbone. The customer is setting up an AWS Direct Connect connection to AWS and has provided the LOA-CFA to ABC Telecom. ABC Telecom has terminated the Direct Connect circuit into their MPLS backbone. To uniquely identify the customer's traffic over the MPLS backbone, the customer must encapsulate all traffic with VLAN tag 100. The customer wants to send traffic to multiple VPCs.
Which two steps should be taken to meet the customer's requirement? (Choose two.)

☐ A. The customer performs Q-in-Q tunneling, with the AWS-required VLAN tag in the inside and VLAN 100 as the outside tag.

☐ B. Create a support ticket with AWS to request the removal of the outer VLAN tag 100 as the traffic reaches AWS routers.

☐ C. Send the traffic for all VPCs with the same VLAN tag 100 and use BGP to ensure that proper routing takes place to the appropriate VP

☐ D. ABC Telecom removes the outer tag before sending the packet to AWS.

☐ E. ABC Telecom creates a support ticket with AWS to exchange MPLS labels and include the AWS port as part of their MPLS network.

Answer(s): C E
