AWS Certified Advanced Networking - Specialty.premium.76q - DEMO

Number: Advanced Networking
Passing Score: 800
Time Limit: 120 min

ANS-C00

AWS Certified Advanced Networking - Specialty Exam

Exam A

QUESTION 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 ELB. 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
References: https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/

QUESTION 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? (Select two.)

A. Internet gateway
B. VPC Flow Logs
C. AWS CloudTrail
D. Lambda
E. AWS Inspector

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
References: https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-specific-apis-are-called-by-using-aws-cloudtrail-amazon-sns-and-aws-lambda/

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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 from your 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

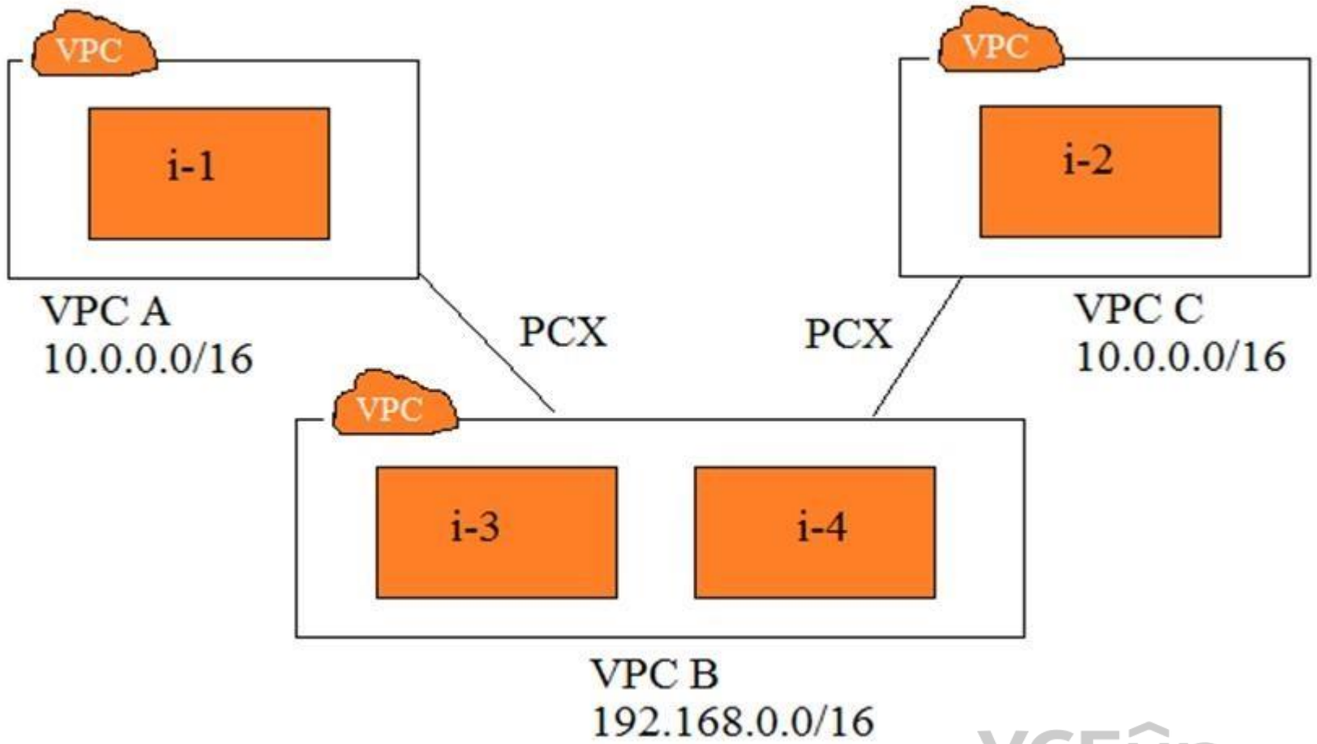
Which solution should you recommend so that the organization meets the requirements?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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? (Select 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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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 requirement? (Select 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

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
References: https://noise.getoto.net/tag/aws-kms/

QUESTION 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? (Select 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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
References: https://aws.amazon.com/premiumsupport/knowledge-center/internet-access-lambda-function/

QUESTION 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 URL, 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? (Select 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.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

QUESTION 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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? (Select 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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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 routers at your onpremises data center that can peer with the Direct Connect routers for redundancy.

Which two design methodologies, in combination, will achieve this connectivity? (Select 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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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? (Select 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 VPC.
D. ABC Telecom removes the other 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.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 An organization runs a consumer-facing website on AWS. The Amazon EC2-based web fleet is load balanced using the AWS Application Load Balancer, Amazon Route 53 is used to provide the public DNS services.

The following URLs need to server content to end users:

test.example.com
web.example.com
example.com

Based on this information, what combination of services must be used to meet the requirement? (Select two.)

A. Path condition in ALB listener to route example.com to appropriate target groups.
B. Host condition in ALB listener to route *.example.com to appropriate target groups.
C. Host condition a ALB listener to route example.com to appropriate target groups.
D. Path condition in ALB listener to route *.example.com to appropriate target groups.
E. Host condition in ALB listener to route $$$$.example.com to appropriate target groups.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Under increased cybersecurity concerns, a company is deploying a near real-time intrusion detection system (IDS) solution. A system must be put in place as soon as possible. The architecture consists of many AWS accounts, and all results must be delivered to a central location.

Which solution will meet this requirement, while minimizing downtime and costs?

A. Deploy a third-party vendor solution to perform deep packet inspection in a transit VPC.
B. Enable VPC Flow Logs on each VPC. Set up a stream of the flow logs to a central Amazon Elasticsearch cluster.
C. Enable Amazon Macie on each AWS account and configure central reporting.
D. Enable Amazon GuardDuty on each account as members of a central account.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://aws.amazon.com/blogs/security/how-to-manage-amazon-guardduty-security-findings-across-multiple-accounts/

QUESTION 23
An organization delivers high-resolution, dynamic web content. Internet users access the content from a variety of platforms, including mobile, tablet and desktop. Each platform receives a customized experience to account for the differences in viewing modes. A dedicated, automatic-scaling fleet of Amazon EC2 instances is used for each platform to server content based on path-based headers. Which combination of services will MINIMIZE cost and MAXIMIZE performance? (Select two.)

A. Amazon CloudFront with Lambda@Edge
B. Network Load Balancer
C. Amazon S3 static websites
D. Amazon Route 53 with traffic flow policies
E. Application Load Balancer

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-at-the-edge.html

QUESTION 24
You need to set up a VPN between AWS VPC and your on-premises network. You create a VPN connection in the AWS Management Console, download the configuration file, and install it on your on-premises router. The tunnel is not coming up because of firewall restrictions on your router. Which two network traffic options should you allow through the firewall? (Select two.)

A. UDP port 500
B. IP protocol 50
C. IP protocol 5
D. TCP port 50
E. TCP port 500

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_VPN.html

QUESTION 25
You have been asked to monitor traffic flows on your Amazon EC2 instance. You will be performing deep packet inspection, looking for atypical patterns.

Which tool will enable you to look at this data?

A. Wireshark
B. VPC Flow Logs

C. AWS CLI
D. CloudWatch Logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://www.slideshare.net/TeriRadichel/packet-capture-on-aws

QUESTION 26
You ping an Amazon Elastic Compute Cloud (EC2) instance from an on-premises server. VPC Flow Logs record the following:

```
2 123456789010 eni-1235b8ca 10.123.234.78 172.11.22.33 0 0 1 8 672 1432917027
1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.11.22.33 10.123.234.78 0 0 1 4 336 1432917027
1432917082 ACCEPT OK
2 123456789010 eni-1235b8ca 172.11.22.33 10.123.234.78 0 0 1 4 336 1432917094
1432917142 REJECT OK
```

Why are ICMP responses not received by the on-premises system?

A. The inbound network access control list is blocking the traffic B.
The outbound network access control list is blocking the traffic
C. The inbound security group is blocking the traffic.
D. The outbound security group is blocking the traffic.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
You are moving a two-tier application into an Amazon VPC. An Elastic Load Balancing (ELB) load balancer is configured in front of the application tier. The application tier is driven through RESTful interfaces. The data tier uses relational database service (RDS) MySQL. Company policy requires end-to-end encryption of all data in transit.

What ELB configuration complies with the corporate encryption policy?

A. Configure the ELB load balancer protocol as HTTP. Configure the application instances for SSL termination. Configure Amazon RDS for SSL, and use REQUIRE SSL grants.
B. Configure the ELB protocols in TCP mode. Configure the application instances for SSL termination. Configure Amazon RDS for SSL, and use REQUIRE SSL grants.
C. Configure the ELB load balancer protocol as HTTPS. Offload application instance encryption to the load balancer. Install your SSL certificate on Amazon RDS, and configure SSL.
D. Configure the ELB protocols in SSL mode. Offload application instance encryption to the load balancer. Install your SSL/TLS certificate on Amazon RDS, and configure SSL.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Your application is hosted behind an Elastic Load Balancer (ELB) within an autoscaling group. The autoscaling group is configured with a minimum of 2, a maximum of 14, and a desired value of 2. The autoscaling cooldown and the termination policies are set to the default value.

CloudWatch reports that the site typically requires just two servers, but spikes at the start and end of the business day can require eight to ten servers. You receive intermittent reports of timeouts and partially loaded web pages.

Which configuration change should you make to address this issue?

A. Configure connection draining on the ELB.
B. Configure the autoscaling cooldown to 600 seconds.
C. Configure the termination policy to oldest instance.
D. Configure a Terminating: Wait lifecycle hook on a scale in event.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html

QUESTION 29
You are designing an AWS Direct Connect solution into your VPC. You need to consider requirements for the customer router to terminate the Direct Connect link at the Direct Connect location.
Which three factors that must be supported should you consider when choosing the customer router? (Select three.)

A. 802.1q trunking
B. 802.1ax or 802.3ad link aggregation
C. OSPF
D. BGP
E. single-mode optical fiber connectivity
F. 1-Gbps copper connectivity

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:
References: https://aws.amazon.com/directconnect/faqs/

QUESTION 30
Your company uses an NTP server to synchronize time across systems. The company runs multiple versions of Linux and Windows systems. You discover that the NTP server has failed, and you need to add an alternate NTP server to your instances.

Where should you apply the NTP server update to propagate information without rebooting your running instances?

A. DHCP Options Set
B. instance user-data
C. cfn-init scripts
D. instance meta-data

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Your company has set up AWS Direct Connect to connect on-premises to an Amazon VPC instance. Two Direct Connect connections terminate at two different Direct Connect locations. You are using two routers, R1 and R2, at your end (one of each Direct Connect connection). R1 and R2 do NOT have connectivity between them. Both routers advertise the same routers over BGP to the VGW. You have a stateful firewall on each router. The routers drop some of the traffic coming from the VPC.

Which two actions should you take to fix this problem? (Select two.)

A. Use BGP AS prepend attribute to prepend additional AS numbers while advertising routers from R1 to VGW.
B. Use BGP local preference attribute to assign R1 to a lower local preference number than R2.

C. Use BGP local preference attribute to assign R1 a higher local preference number than R2.
D. Use BGP MED attribute to assign a higher MED value to the routes advertised R1 to VGW.
E. Use BGP MED attribute to assign a higher MED value to the routes advertised from R2 to VGW.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
An organization will be expanding its current network design. When fully built out, there will be 99 VPCs spread across 11 AWS accounts (9 VPCs per account). There is currently an AWS Direct Connect connection into one account with 9 VPCs, each with a virtual network interface (VIF) per VPC.

Which of the following designs will minimize cost while allowing the organization to expand?

A. Order 10 new Direct Connect connections, one from each of the accounts that will be provisioned. Create private VIFs in each account. Attach one private VIF per VPC.
B. Create a public VIF on the Direct Connect connection. Leverage the public VIF to create a VPN connection to each VPC.
C. Create hosted private VIFs in the existing account. Connect a private VIF to an AWS Direct Connect gateway in each account. Connect the gateway in each account to the VPCs.
D. Create a transit VPC in the existing account that consists of two routers in separate Availability Zones. Connect each VPC to the two routers in the transit VPC by using VPN.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
An organization with a growing e-commerce presence uses the AWS CloudHSM to offload the SSL/TLS processing of its web server fleet. The company leverages Amazon EC2 Auto Scaling for web servers to handle the growth. What architectural approach is optimal to scale the encryption operation?

A. Use multiple CloudHSM instances, and load balance them using a Network Load Balancer.
B. Use multiple CloudHSM instances to the cluster;request to it will automatically load balance.
C. Enable Auto Scaling on the CloudHSM instance, with similar configuration to the web tier Auto Scaling group.
D. Use multiple CloudHSM instances, and load balance them using an Application Load Balancer.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A company has 225 mobile and desktop devices and 300 partner VPNs that need access to an AWS VPC. VPN users should not be able to reach one another. Which approach will meet the technical and security requirements while minimizing costs?

A. Use the AWS IPsec VPN for the mobile, desktop, and partner VPN connections. Use network access control lists (Network ACLs) and security groups to maintain routing separation.
B. Use the AWS IPsec VPN for the partner VPN connections. Use an Amazon EC2 instance VPN for the mobile and desktop devices. Use Network ACLs and security groups to maintain routing separation.
C. Create an AWS Direct Connect connection between on-premises and AWS Use a public virtual interface to connect to the AWS IPsec VPN for the mobile, desktop, and partner VPN connections.
D. Use an Amazon EC2 instance VPN for the desktop, mobile, and partner VPN connections. Use features of the VPN instance to limit routing and connectivity.

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 35
Your company needs to leverage Amazon Simple Storage Solution (S3) for backup and archiving. According to company policy, data should not flow on the public Internet even if data is encrypted. You have set up two S3 buckets in useast-1 and us-west-2. Your company data center is located on the West Coast of the United States. The design must be cost-effective and enable minimal latency.

Which design should you set up?

A. An AWS Direct Connect connection to us-east-1 and a Direct Connect connection to us-west-2.
B. An AWS Direct Connect connection to us-east-1.
C. An AWS Direct Connect connection to us-west-2.
D. An AWS Direct Connect connection to us-west-2 and a VPN connection to us-east-1.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Your organization runs a popular e-commerce application deployed on AWS that uses autoscaling in conjunction with an Elastic Load balancing (ELB) service with an HTTPS listener. Your security team reports that an exploitable vulnerability has been discovered in the encryption protocol and cipher that your site uses.

Which step should you take to fix this problem?

A. Generate new SSL certificates for all web servers and replace current certificates.
B. Change the security policy on the ELB to disable vulnerable protocols and ciphers.
C. Generate new SSL certificates and use ELB to front-end the encrypted traffic for all web servers.
D. Leverage your current configuration management system to update SSL policy on all web servers.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Your organization leverages an IP Address Management (IPAM) product to manage IP address distribution. The IPAM exposes an API. Development teams use CloudFormation to provision approved reference architectures. At deployment time, IP addresses must be allocated to the VPC. When the VPC is deleted, the IPAM must reclaim the VPC's IP allocation.

Which method allows for efficient, automated integration of the IPAM with CloudFormation?

A. AWS CloudFormation parameters using the "Ref::" intrinsic function
B. AWS CloudFormation custom resource using an AWS Lambda invocation.
C. CloudFormation::OpsWorks::Stack with custom Chef configuration.
D. AWS CloudFormation parameters using the "Fn::FindInMap" intrinsic function.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
You need to set up an Amazon Elastic Compute Cloud (EC2) instance for an application that requires the lowest latency and the highest packet-per-second network performance. The application will talk to other servers in a peered VPC. Which two of the following components should be part of the design? (Select two.)

A. Select an instance with support for single root I/O virtualization.
B. Select an instance that has support for multiple ENIs.
C. Ensure that the instance supports jumbo frames and set 9001 MTU.
D. Select an instance with Amazon Elastic Block Store (EBS)-optimization.
E. Ensure that proper OS drivers are installed.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

QUESTION 39 You are configuring a virtual interface for access to your VPC on a newly provisioned 1-Gbps AWS Direct Connect connection. Which two configuration values do you need to provide? (Select two.)

A. Public AS number
B. VLAN ID
C. IP prefixes to advertise
D. Direct Connect location
E. Virtual private gateway

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
References: https://aws.amazon.com/directconnect/faqs/

QUESTION 40
A corporate network routing table contains 624 individual RFC 1918 and public IP prefixes. You have two AWS Direct Connect connectors. You configure a private virtual interface on both connections to a virtual private gateway. The virtual private gateway is not currently attached to a VPC. Neither BGP session will maintain the *Established* state on the customer router. The AWS Management Console reports the private virtual interfaces as *Down.*

What could you do to address the problem so that the AWS Management Console reports the private virtual interface as *Available*?

A. Attach the virtual private gateway to a VPC and enable route propagation.
B. Filter the public IP pre?xes on the corporate network from the private virtual interface.
C. Change the BGP advertisements from the corporate network to only be a default route.
D. Attach the second virtual interface to an alternative virtual private gateway.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Your company maintains an Amazon Route 53 private hosted zone. DNS resolution is restricted to a single, pre-existing VPC. For a new application deployment, you create an additional VPC in the same AWS account. Both this new VPC and your on-premises DNS infrastructure must resolve records in the existing private hosted zone.

Which two activities are required to enable DNS resolution both within the new VPC and from the on-premises infrastructure? (Select two.)

A. Update the DHCP options set for the new VPC with the Route 53 nameserver IP addresses.
B. Update the Route 53 private hosted zone's VPC associations to include the new VPC.
C. Launch Amazon EC2-based DNS proxies in the new VPC. Specify the proxies as forwarders in the on-premises DNS.
D. Update the on-premises DNS to include forwarders to the Route 53 nameserver IP addresses.

E. Launch Amazon EC2-based DNS proxies in the new VPC. Specify the proxies in the DHCP options set.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
A department in your company has created a new account that is not part of the organization's consolidated billing family. The department has also created a VPC for its workload. Access is restricted by network access control lists to the department's on-premises private IP allocation. An AWS Direct Connect private virtual interface for this VPC advertises a default route to the company network. When the department downloads data from an Amazon Elastic Compute Cloud (EC2) instance in its new VPC, what are the associated charges?

A. The company pays Internet Data Out charges.
B. The company pays AWS Direct Connect Data Out charges.
C. The department pays Internet Data Out charges.
D. The department pays AWS Direct Connect Data Out charges.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
An organization will be extending its existing on-premises infrastructure into the cloud. The design consists of a transit VPC that contains stateful firewalls that will be deployed in a highly available configuration across two Availability Zones for automatic failover.

What MUST be configured for this design to work? (Select two.)

A. A different Autonomous System Number (ASN) for each firewall.
B. Border Gateway Protocol (BGP) routing
C. Autonomous system (AS) path prepending
D. Static routing
E. Equal-cost multi-path routing (ECMP)

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
A company is about to migrate an application from its on-premises data center to AWS. As part of the planning process, the following requirements involving DNS have been identified.

- On-premises systems must be able to resolve the entries in an Amazon Route 53 private hosted zone.
- Amazon EC2 instances running in the organization's VPC must be able to resolve the DNS names of on-premises systems

The organization's VPC uses the CIDR block 172.16.0.0/16.

Assuming that there is no DNS namespace overlap, how can these requirements be met?

A. Change the DHCP options set for the VPC to use both the Amazon-provided DNS server and the on-premises DNS systems. Configure the on-premises DNS systems with a stub-zone, delegating the name server 172.16.0.2 asauthoritative for the Route 53 private hosted zone.
B. Deploy and configure a set of EC2 instances into the company VPC to act as DNS proxies. Configure the proxies to forward queries for the on-premises domain to the on-premises DNS systems, and forward all other queries to 172.16.0.2. Change the DHCP options set for the VPC to use the new DNS proxies. Configure the on-premises DNS systems with a stub-zone, delegating the name server 172.16.0.2 as authoritative for the Route 53 private hosted zone.

C. Deploy and configure a set of EC2 instances into the company VPC to act as DNS proxies. Configure the proxies to forward queries for the on-premises domain to the on-premises DNS systems, and forward all other queries to theAmazon-provided DNS server (172.16.0.2). Change the DHCP options set for the VPC to use the new DNS proxies. Configure the on-premises DNS systems with a stub-zone, delegating the proxies as authoritative for the Route 53 private hosted zone.
D. Change the DHCP options set for the VPC to use both the on-premises DNS systems. Configure the on-premises DNS systems with a stub-zone, delegating the Route 53 private hosted zone's name servers as authoritative for the Route53 private hosted zone.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
The Web Application Development team is worried about malicious activity from 200 random IP addresses. Which action will ensure security and scalability from this type of threat?

A. Use inbound security group rules to block the IP addresses.
B. Use inbound network ACL rules to block the IP addresses.
C. Use AWS WAF to block the IP addresses.
D. Write iptables rules on the instance to block the IP addresses.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
You operate a production VPC with both a public and a private subnet. Your organization maintains a restricted Amazon S3 bucket to support this production workload. Only Amazon EC2 instances in the private subnet should access the bucket. You implement VPC endpoints(VPC-E) for Amazon S3 and remove the NAT that previously provided a network path to Amazon S3. The default VPC-E policy is applied. Neither EC2 instances in the public or private subnets are able to access the S3 bucket.

What should you do to enable Amazon S3 access from EC2 instances in the private subnet?

A. Add the CIDR address range of the private subnet to the S3 bucket policy.
B. Add the VPC-E identified to the S3 bucket policy.
C. Add the VPC identifier for the production VPC to the S3 bucket policy.
D. Add the VPC-E identifier for the production VPC to endpoint policy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Your hybrid networking environment consists of two application VPCs, a shared services VPC, and your corporate network. The corporate network is connected to the shared services VPC via an IPsec VPN with dynamic (BGP) routing enabled.

The applications require access to a common authentication service in the shared services VPC. You need to enable native network access from the corporate network to both application VPCs.

Which step should you take to meet the requirements?

A. Use VPC peering to peer the application VPCs with the shared services VPC, and enable associated routing in the shared services VPC via the corporate VPN.
B. Configure an IPsec VPN between the virtual private gateway in each application VPC to the virtual private gateway in the shared services VPC.
C. Configure additional IPsec VPNs for each application VPC back to the corporate network, and enable VPC peering to the shared services VPC.

D. Enable CloudHub functionality to route traffic between the three VPCs and the corporate network using dynamic BGP routing.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
You use a VPN to extend your corporate network into a VPC. Instances in the VPC are able to resolve resource records in an Amazon Route 53 private hosted zone. Your on-premises DNS server is configured with a forwarder to the VPC DNS server IP address. On-premises users are unable to resolve names in the private hosted zone, although instances in a peered VPC can.

What should you do to provide on-premises users with access to the private hosted zone?

A. Create a proxy resolver within the VPC. Point the on-premises forwarder to the proxy resolver.
B. Modify the network access control list on the VPC to allow DNS queries from on-premises systems.
C. Configure the on-premises server as a secondary DNS for the private zone. Update the NS records.
D. Update the on-premises forwarders with the four name servers assigned to the private hosted zone.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
References: https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-by-using-unbound/

QUESTION 49
Your organization has a newly installed 1-Gbps AWS Direct Connect connection. You order the cross-connect from the Direct Connect location provider to the port on your router in the same facility. To enable the use of your first virtual interface, your router must be configured appropriately.

What are the minimum requirements for your router?

A. 1-Gbps Multi Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
B. 1-Gbps Single Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
C. IPsec Parameters, Pre-Shared key, Peer IP Address, BGP Session with MD5
D. BGP Session with MD5, 802.1Q VLAN, Route-Map, Prefix List, IPsec encrypted GRE Tunnel

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Your security team implements a host-based firewall on all of your Amazon Elastic Compute Cloud (EC2) instances to block all outgoing traffic. Exceptions must be requested for each specific requirement. Until you request a new rule, you cannot access the instance metadata service. Which firewall rule should you request to be added to your instances to allow instance metadata access?

A. Inbound; Protocol tcp; Source [Instance's EIP]; Destination 169.254.169.254
B. Inbound; Protocol tcp; Destination 169.254.169.254; Destination port 80
C. Outbound; Protocol tcp; Destination 169.254.169.254; Destination port 80
D. Outbound; Protocol tcp; Destination 169 .254.169.254; Destination port 443

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 51
A customer has set up multiple VPCs for Dev, Test, Prod, and Management. You need to set up AWS Direct Connect to enable data flow from on-premises to each VPC. The customer has monitoring software running in the Management VPC that collects metrics from the instances in all the other VPCs. Due to budget requirements, data transfer charges should be kept at minimum. Which design should be recommended?

A. Create a total of four private VIFs, one for each VPC owned by the customer, and route traffic between VPCs using the Direct Connect link.
B. Create a private VIF to the Management VPC, and peer this VPC to all other VPCs.
C. Create a private VIF to the Management VPC, and peer this VPC to all other VPCs, enable source/destination NAT in the Management VPC.
D. Create a total of four private VIFs, and enable VPC peering between all VPCs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Your company runs an application for the US market in the us-east-1 AWS region. This application uses proprietary TCP and UDP protocols on Amazon Elastic Compute Cloud (EC2) instances. End users run a real-time, front-end application on their local PCs. This front-end application knows the DNS hostname of the service.

You must prepare the system for global expansion. The end users must access the application with lowest latency.

How should you use AWS services to meet these requirements?

A. Register the IP addresses of the service hosts as “A” records with latency-based routing policy in Amazon Route 53, and set a Route 53 health check for these hosts.
B. Set the Elastic Load Balancing (ELB) load balancer in front of the hosts of the service, and register the ELB name of the main service host as an ALIAS record with a latency-based routing policy in Route 53.
C. Set Amazon CloudFront in front of the host of the service, and register the CloudFront name of the main service as an ALIAS record in Route 53.
D. Set the Amazon API gateway in front of the service, and register the API gateway name of the main service as an ALIAS record in Route 53.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 You deploy an Amazon EC2 instance that runs a web server into a subnet in a VPC. An Internet gateway is attached, and the main route table has a default route (0.0.0.0/0) configured with a target of the Internet gateway.

The instance has a security group configured to allow as follows:

- Protocol: TCP
- Port: 80 inbound, nothing outbound

The Network ACL for the subnet is configured to allow as follows:

- Protocol: TCP
- Port: 80 inbound, nothing outbound

When you try to browse to the web server, you receive no response.

Which additional step should you take to receive a successful response?

A. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 80
B. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 1024-65535
C. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 80
D. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 1024-65535

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
An organization launched an IPv6-only web portal to support IPv6-native mobile clients. Front-end instances launch in an Amazon VPC associated with an appropriate IPv6 CIDR. The VPC IPv4 CIDR is fully utilized. A single subnet exists in each of two Availability Zones with appropriately configured IPv6 CIDR associations. Auto Scaling is properly configured, and no Elastic Load Balancing is used.

Customers say the service is unavailable during peak load times. The network engineer attempts to launch an instance manually and receives the following message: "There are not enough free addresses in subnet 'subnet-12345677' to satisfy the requested number of instances."

What action will resolve the availability problem?

A. Create a new subnet using a VPC secondary IPv6 CIDR, and associate an IPv6 CIDR. Include the new subnet in the Auto Scaling group.
B. Create a new subnet using a VPC secondary IPv4 CIDR, and associate an IPv6 CIDR. Include the new subnet in the Auto Scaling group.
C. Resize the IPv6 CIDR on each of the existing subnets. Modify the Auto Scaling group maximum number of instances.
D. Add a secondary IPv4 CIDR to the Amazon VPC. Assign secondary IPv4 address space to each of the existing subnets.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A Network Engineer is designing a new system on AWS that will take advantage of Amazon CloudFront for both content caching and for protecting the underlying origin. There is concern that an external agency might be able to access the IP addresses for the application's origin and then attack the origin despite it being served by CloudFront. Which of the following solutions provides the strongest level of protection to the origin?

A. Use an IP whitelist rule in AWS WAF within CloudFront to ensure that only known-client IPs are able to access the application.
B. Configure CloudFront to use a custom header and configure an AWS WAF rule on the origin's Application Load Balancer to accept only traffic that contains that header.
C. Configure an AWS Lambda@Edge function to validate that the traffic to the Application Load Balancer originates from CloudFront.
D. Attach an origin access identity to the CloudFront origin that allows traffic to the origin that originates from only CloudFront.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A network engineer is managing two AWS Direct Connect connections. Each connection has a public virtual interface configured with a private ASN. The engineer wants to configure active/passive routing between the Direct Connect connections to access Amazon public endpoints. What BGP configuration is required for the on-premises equipment? (Select two.)

A. Use Local Pref to control outbound traffic.
B. Use AS Prepending to control inbound traffic.
C. Use eBGP multi-hop between loopback interfaces.
D. Use BGP Communities to control outbound traffic.
E. Advertise more specific prefixes over one Direct Connect connection.

Correct Answer: CE
Section: (none)
Explanation
Explanation/Reference:

QUESTION 57
You are preparing to launch Amazon WorkSpaces and need to configure the appropriate networking resources. What must be configured to meet this requirement?

A. At least two subnets in different Availability Zones.
B. A dedicated VPC with Active Directory Services.
C. An IPsec VPN to on-premises Active DirectoryD. Network address translation for outbound traffic.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
References: https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-vpc.html

QUESTION 58
You have multiple Amazon Elastic Compute Cloud (EC2) instances running a web server in a VPC configured with security groups and NACL. You need to ensure layer 7 protocol level logging of all network traffic (ACCEPT/REJECT) on the instances. What should be enabled to complete this task?

A. CloudWatch Logs at the VPC level
B. Packet sniffing at the instance level
C. VPC flow logs at the subnet level
D. Packet sniffing at the VPC level

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Your company operates a single AWS account. A common services VPC is deployed to provide shared services, such as network scanning and compliance tools. Each AWS workload uses its own VPC, and each VPC must peer with the common services VPC. You must choose the most efficient and cost effective approach.

Which approach should be used to automate the required VPC peering?

A. AWS CloudTrail integration with Amazon CloudWatch Logs to trigger a Lambda function.
B. An OpsWorks Chef recipe to execute a command-line peering request.
C. Cfn-init with AWS CloudFormation to execute a command-line peering request.
D. An AWS CloudFormation template that includes a peering request.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Your organization requires strict adherence to a change control process for its Amazon Elastic Compute Cloud (EC2) and VPC environments. The organization uses AWS CloudFormation as the AWS service to control and implement changes. Which combination of three services provides an alert for changes made outside of AWS CloudFormation? (Select three.)

A. AWS Config
B. AWS Simple Notification Service
C. AWS CloudWatch metrics
D. AWS Lambda
E. AWS CloudFormation

F. AWS Identify and Access Management

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
You have a global corporate network with 153 individual IP prefixes in your internal routing table. You establish a private virtual interface over AWS Direct Connect to a VPC that has an Internet gateway (IGW). All instances in the VPC must be able to route to the Internet via an IGW and route to the global corporate network via the VGW.

How should you configure your on-premises BGP peer to meet these requirements?

A. Configure AS-Prepending on your BGP session
B. Summarize your prefix announcement to less than 100
C. Announce a default route to the VPC over the BGP session
D. Enable route propagation on the VPC route table

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62 You are building an application that provides real-time audio and video services to customers on the Internet. The application requires high throughput. To ensure proper audio and video transmission, minimal latency is required.

Which of the following will improve transmission quality?

A. Enable enhanced networking
B. Select G2 instance types
C. Enable jumbo frames
D. Use multiple elastic network interfaces

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
The Payment Card Industry Data Security Standard (PCI DSS) merchants that handle credit card data must use strong cryptography. These merchants must also use security protocols to protect sensitive data during transmission over public networks.

You are migrating your PCI DSS application from on-premises SSL appliance and Apache to a VPC behind Amazon CloudFront.

How should you configure CloudFront to meet this requirement?

A. Configure the CloudFront Cache Behavior to require HTTPS and the CloudFront Origin's Protocol Policy to 'Match Viewer'.
B. Configure the CloudFront Cache Behavior to allow TCP connections and to forward all requests to the origin without TLS termination at the edge.
C. Configure the CloudFront Cache Behavior to require HTTPS and to forward requests to the origin via AWS Direct Connect.
D. Configure the CloudFront Cache Behavior to redirect HTTP requests to HTTPS and to forward request to the origin via the Amazon private network.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
You deploy your Internet-facing application is the us-west-2(Oregon) region. To manage this application and upload content from your corporate network, you have a 1–Gbps AWS Direct Connect connection with a private virtual interface via one of the associated Direct Connect locations. In normal operation, you use approximately 300 Mbps of the available bandwidth, which is more than your Internet connection from the corporate network.

You need to deploy another identical instance of the application is us-east-1(N Virginia) as soon as possible. You need to use the benefits of Direct Connect. Your design must be the most effective solution regarding cost, performance, and time to deploy.

Which design should you choose?

A. Use the inter-region capabilities of Direct Connect to establish a private virtual interface from us-west-2 Direct Connect location to the new VPC in us-east-1.
B. Deploy an IPsec VPN over your corporate Internet connection to us-east-1 to provide access to the new VPC.
C. Use the inter-region capabilities of Direct Connect to deploy an IPsec VPN over a public virtual interface to the new VPC in us-east-1.
D. Use VPC peering to connect the existing VPC in us-west-2 to the new VPC in us-east-1, and then route traffic over Direct Connect and transit the peering connection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65 Your company has a 1-Gbps AWS Direct Connect connection to AWS. Your company needs to send traffic from on-premises to a VPC owned by a partner company. The connectivity must have minimal latency at the lowest price.
Which of the following connectivity options should you choose?

A. Create a new Direct Connect connection, and set up a new circuit to connect to the partner VPC using a private virtual interface.
B. Create a new Direct Connect connection, and leverage the existing circuit to connect to the partner VPC.
C. Create a new private virtual interface, and leverage the existing connection to connect to the partner VPC.
D. Enable VPC peering and use your VPC as a transitive point to reach the partner VPC.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
An organization wants to process sensitive information using the Amazon EMR service. The information is stored in on-premises databases. The output of processing will be encrypted using AWS KMS before it is uploaded to a customerowned Amazon S3 bucket. The current configuration includes a VPS with public and private subnets, with VPN connectivity to the on-premises network. The security organization does not allow Amazon EC2 instances to run in the public subnet.

What is the MOST simple and secure architecture that will achieve the organization's goal?

A. Use the existing VPC and configure Amazon EMR in a private subnet with an Amazon S3 endpoint.
B. use the existing VPS and a NAT gateway, and configure Amazon EMR in a private subnet with an Amazon S3 endpoint.
C. Create a new VPS without an IGW and configure the VPN and Amazon EMR in a private subnet with an Amazon S3 endpoint.
D. Create a new VPS without an IGW and configure the VPN and Amazon EMR in a private subnet with an Amazon S3 endpoint and a NAT gateway.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
An organization has three AWS accounts with each containing VPCs in Virginia, Canada and the Sydney regions. The organization wants to determine whether all available Elastic IP addresses (EIPs) in these accounts are attached to Amazon EC2 instances or in use elastic network interfaces (ENIs) in all of the specified regions for compliance and cost-optimization purposes.

Which of the following meets the requirements with the LEAST management overhead?

A. use an Amazon CloudWatch Events rule to schedule an AWS Lambda function in each account in all three regions to find the unattached and unused EIPs.
B. Use a CloudWatch event bus to schedule Lambda functions in each account in all three regions to find the unattached and unused EIPs.
C. Add an AWS managed, EIP-attached AWS Config rule in each region in all three accounts to find unattached and unused EIPs.
D. Use AWS CloudFormation StackSets to deploy an AWS Config EIP-attached rule in all accounts and regions to find the unattached and unused EIPs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
A Systems Administrator is designing a hybrid DNS solution with spilt-view. The apex-domain “example.com” should be served through name servers across multiple top-level domains (TLDs). The name server for subdomain “dev.example.com” should reside on-premises. The administrator has decided to use Amazon Route 53 to achieve this scenario.

What procedurals steps must be taken to implement the solution?

A. Use a Route 53 public hosted zone for example.com and a private hosted zone for dev.example.com
B. Use a Route 53 public and private hosted zone for example.com and perform subdomain delegation for dev.example.com
C. Use a Route 53 public hosted zone for example.com and perform subdomain delegation for dev.example.com
D. Use a Route 53 private hosted zone for example.com and perform subdomain delegation for dev.example.com

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69 DNS name resolution must be provided for services in the following four zones:

```
company.private.
emea.company.private.
apac.company.private.
amer.company.private.
```

The contents of these zones is not considered sensitive, however, the zones only need to be used by services hosted in these VPCs, one per geographic region. Each VPC should resolve the names in all zones.

How can you use Amazon route 53 to meet these requirements?

A. Create a Route 53 Private Hosted Zone for each of the four zones and associate them with the three VPCs.
B. Create a single Route 53 Private Hosted Zone for the zone `company.private` and associate it with the three VPCs.
C. Create a Route Public Hosted Zone for each of the four zones and configure the VPS DNS Resolver to forward
D. Create a single Route 53 Public Hosted Zone for the zone `company.private` and configure the VPS DNS Resolver to forward

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
An organization is replacing a tape backup system with a storage gateway. there is currently no connectivity to AWS. Initial testing is needed.

What connection option should the organization use to get up and running at minimal cost?

A. Use an internet connection.
B. Set up an AWS VPN connection.
C. Provision an AWS Direct Connection private virtual interface.
D. Provision a Direct Connect public virtual interface.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
All IP addresses within a 10.0.0.0/16 VPC are fully utilized with application servers across two Availability Zones. The application servers need to send frequent UDP probes to a single central authentication server on the Internet to confirm that is running up-to-date packages. The network is designed for application servers to use a single NAT gateway for internal access. Testing reveals that a few of the servers are unable to communicate with the authentication server.

A. The NAT gateway does not support UDP traffic.
B. The authentication server is not accepting traffic.
C. The NAT gateway cannot allocate more ports.
D. The NAT gateway is launched in a private subnet.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
An organization is using a VPC endpoint for Amazon S3. When the security group rules for a set of instances were initially configured, access was restricted to allow traffic only to the IP addresses of the Amazon S3 API endpoints in the region from the published JSON file. The application was working properly, but now is logging a growing number of timeouts when connecting with Amazon S3. No internet gateway is configured for the VPC.

Which solution will fix the connectivity failures with the LEAST amount of effort?

A. Create a Lambda function to update the security group based on AmazonIPSpaceChanged notifications.
B. Update the VPC routing to direct Amazon S3 prefix-list traffic to the VPC endpoint using the route table APIs.
C. Update the application server's outbound security group to use the prefix-list for Amazon S3 in the same region.
D. Create an additional VPC endpoint for Amazon S3 in the same route table to scale the concurrent connections to Amazon.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 73
A bank built a new version of its banking application in AWS using containers that content to an on-premises database over VPN connection. This application version requires users to also update their client application. The bank plans to deprecate the earlier client version. However, the company wants to keep supporting earlier clients through their on-premises version of the application to serve a small portion of the customers who haven't yet upgraded.

What design will allow the company to serve both newer and earlier clients in the MOST efficient way?

A. Use an Amazon Route 53 multivalue answer routing policy to route older client traffic to the on-premises application version and the rest of the traffic to the new AWS based version.
B. Use a Classic Load Balancer for the new application. Route all traffic to the new application by using an Elastic Load Balancing (ELB) load balancer DNS. Define a user-agent-based rule on the backend servers to redirect earlier clients tothe on-premises application.
C. Use an Application Load Balancer for the new application. Register both the new and earlier applications as separate target groups and use path-based routing to route traffic based on the application version.
D. Use an Application Load Balancer for the new application. Register both the new and earlier application backends as separate target groups. Use header-based routing to route traffic based on the application version.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A company is deploying a non-web application on an AWS load balancer. All targets are servers located on-premises that can be accessed by using AWS Direct Connect. The company wants to ensure that the source IP addresses of clients connecting to the application are passed all the way to the end server.

How can this requirement be achieved?

A. Use a Network Load Balancer to automatically preserve the source IP address.
B. Use a Network Load Balancer and enable the `X-Forwarded-For` attribute.
C. Use a Network Load Balancer and enable the `ProxyProtocol` v2 attribute.
D. Use an Application Load Balancer to automatically preserve the source IP address in the `X-Forwarded-For` header.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
An AWS CloudFormation template is being used to create a VPC peering connection between two existing operational VPCs, each belonging to a different AWS account. All necessary components in the **'Remote'** (receiving) account are already in place.

The template below creates the VPC peering connection in the Originating account. It contains these components:

```
AWSTemplateFormation Version: 2010-09-09
Parameters:
    Originating VCId:
Type: String
    RemoteVPCId:
        Type: String
    RemoteVPCAccountId:
Type: String
Resources:
    newVPCPeeringConnection:
        Type: 'AWS::EC2::VPCPeeringConnection'
        Properties:
            VpcdId: !Ref OriginatingVPCId
            PeerVpcId: !Ref RemoteVPCId
            PeerOwnerId: !Ref RemoteVPCAccountId
```

Which additional AWS CloudFormation components are necessary in **the Originating** account to create an operational cross-account VPC peering connection with AWS CloudFormation? (Select two.)

A.
```
Resources:
      NewEC2SecurityGroup:
          Type: AWS::EC2::SecurityGroup
```

B.
```
Resources:
```

```
        NetworkInterfaceToRemoteVPC:
            Type: "AWS::EC2NetworkInterface"
```

C.
```
Resources:
        newEC2Route:
            Type: AWS::EC2::Route
```

D.
```
Resources:
        VPCGatewayToRemoteVPC:
            Type: "AWS::EC2::VPCGatewayAttachment"
```

E.
```
Resources:
        newVPCPeeringConnection:
            Type: 'AWS::EC2VPCPeeringConnection'
                PeerRoleArn: !Ref PeerRoleArn
```

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A Network Engineer is provisioning a subnet for a load balancer that will sit in front of a fleet of application servers in a private subnet. There is limited IP space left in the VPC CIDR. The application has few users now but is expected to grow quickly to millions of users.

What design will use the LEAST amount of IP space, while allowing for this growth?

A. Use two /29 subnets for an Application Load Balancer in different Availability Zones.
B. Use one /29 subnet for the Network Load Balancer. Add another VPC CIDR to the VPC to allow for future growth.
C. Use two /28 subnets for a Network Load Balancer in different Availability Zones.
D. Use one /28 subnet for an Application Load Balancer. Add another VPC CIDR to the VPC to allow for future growth.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference: