Amazon AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Exam

Version: 6.0

QUESTION NO: 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.

Answer: A
Explanation:

QUESTION NO: 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: B

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

QUESTION NO: 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: C,D

Explanation:
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 NO: 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: D
Explanation:

QUESTION NO: 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: A

Explanation:

QUESTION NO: 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.

Answer: A

Explanation:

QUESTION NO: 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: D
Explanation:

QUESTION NO: 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

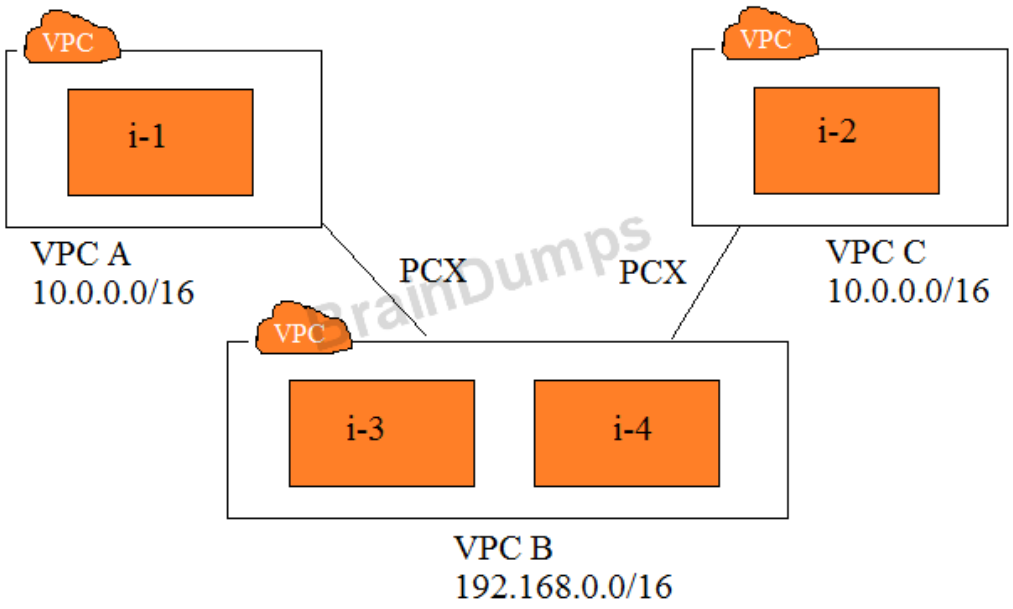
C.
A private MPLS solution from an international carrier

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

Answer: D
Explanation:

QUESTION NO: 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: A,E

Explanation:

QUESTION NO: 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: D
Explanation:

QUESTION NO: 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: C,E

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

QUESTION NO: 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: A,C

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

QUESTION NO: 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: C,D
Explanation:

QUESTION NO: 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: A

Explanation:

QUESTION NO: 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: B,C

Explanation:

QUESTION NO: 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: D
Explanation:

QUESTION NO: 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 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: A,D
Explanation:

QUESTION NO: 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: B
Explanation:

QUESTION NO: 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: D
Explanation:

QUESTION NO: 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 VPC.

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: C,E
Explanation:

QUESTION NO: 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? (Choose 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 in 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.

Answer: A,C
Explanation:

QUESTION NO: 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.

Answer: D

Explanation:

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

QUESTION NO: 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? (Choose 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

Answer: A,E

Explanation:

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

QUESTION NO: 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? (Choose two.)

A.
UDP port 500

B.
IP protocol 50

C.
IP protocol 5

D.
TCP port 50

E.
TCP port 500

Answer: A,B

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

QUESTION NO: 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

Answer: A

Explanation:

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

QUESTION NO: 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.

Answer: B

Explanation:

QUESTION NO: 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.

Answer: C
Explanation:

QUESTION NO: 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.

Answer: A

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

QUESTION NO: 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? (Choose 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

Answer: A,D,E

Explanation:

QUESTION NO: 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

Answer: C
Explanation:

QUESTION NO: 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? (Choose 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.

Answer: A,C

Explanation:

QUESTION NO: 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.

Answer: D

Explanation:

QUESTION NO: 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.

Answer: A
Explanation:

QUESTION NO: 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.

Answer: B
Explanation:

QUESTION NO: 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 us-east-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.

Answer: A
Explanation:

QUESTION NO: 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.

Answer: D
Explanation:

QUESTION NO: 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.

Answer: A

Explanation:

QUESTION NO: 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? (Choose 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.

Answer: A,B

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

QUESTION NO: 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? (Choose two.)

A.
Public AS number

B.
VLAN ID

C.
IP prefixes to advertise

D.
Direct Connect location

E.
Virtual private gateway

Answer: A,E

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

QUESTION NO: 40

A corporate network routing table contains 624 individual RFC 1918 and public IP prefixes. You have two AWS Direct Connect connectors. You congure 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 prexes 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.

Answer: D

Explanation:

QUESTION NO: 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? (Choose 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.

Answer: A,B
Explanation:

QUESTION NO: 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.

Answer: D
Explanation:

QUESTION NO: 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? (Choose 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)

Answer: B,E
Explanation:

QUESTION NO: 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 as authoritative 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 the Amazon-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 Route 53 private hosted zone.

Answer: C

Explanation:

QUESTION NO: 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.

Answer: B
Explanation:

QUESTION NO: 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.

Answer: A

Explanation:

QUESTION NO: 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.

Answer: C

Explanation:

QUESTION NO: 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.

Answer: D

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

QUESTION NO: 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

Answer: B

Explanation:

QUESTION NO: 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

Answer: C

Explanation:

QUESTION NO: 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.

Answer: A
Explanation:

QUESTION NO: 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.

Answer: B

Explanation:

QUESTION NO: 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

Answer: C
Explanation:

QUESTION NO: 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-12345678’ 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.

Answer: B
Explanation:

QUESTION NO: 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.

Answer: A

Explanation:

QUESTION NO: 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? (Choose 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.

Answer: C,E

Explanation:

QUESTION NO: 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 Directory

D.
Network address translation for outbound traffic.

Answer: A,D

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

QUESTION NO: 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

Answer: A
Explanation:

QUESTION NO: 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.

Answer: A
Explanation:

QUESTION NO: 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? (Choose 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

Answer: B,C,D
Explanation:

QUESTION NO: 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

Answer: D
Explanation:

QUESTION NO: 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

Answer: D
Explanation:

QUESTION NO: 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.

Answer: C
Explanation:

QUESTION NO: 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.

Answer: A
Explanation:

QUESTION NO: 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.

Answer: D
Explanation:

QUESTION NO: 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 customer-owned 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.

Answer: B
Explanation:

QUESTION NO: 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.

Answer: C

Explanation:

QUESTION NO: 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

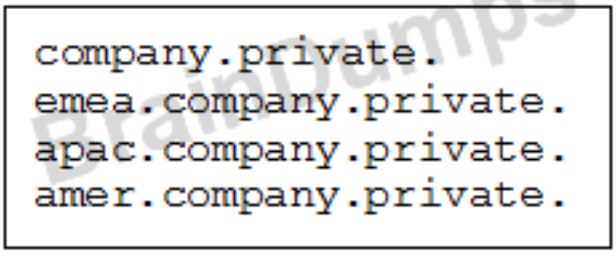
C.
Use a Route 53 public hosted zone for example.com and perform subdomain delegation for dev.example.com

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

Answer: A
Explanation:

QUESTION NO: 69

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



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 53 Public Hosted Zone for each of the four zones and configure the VPC DNS Resolver to forward

D.
Create a single Route 53 Public Hosted Zone for the zone company.private. and configure the VPC DNS Resolver to forward

Answer: D
Explanation:

QUESTION NO: 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.

Answer: A
Explanation:

QUESTION NO: 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 it 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.

What is the reason for this failure?

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.

Answer: C
Explanation:

QUESTION NO: 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 S3.

Answer: C
Explanation:

QUESTION NO: 73

A bank built a new version of its banking application in AWS using containers that connect to an on-premises database over a 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 to the 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 host header-based routing to route traffic based on the application version.

Answer: B
Explanation:

QUESTION NO: 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.

Answer: D
Explanation:

QUESTION NO: 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:

```
AWSTemplateFormatVersion: 2010-09-09
Parameters:
     Originating VPCId:
          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? (Choose two.)

A.

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

B.

```
Resources:
   NetworkInterfaceToRemoteVPC:
        Type: "AWS::EC2::NetworkInterface"
```

C.

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

D.

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

E.

```
Resources:
   newVPCPeeringConnection:
        Type: 'AWS::EC2::VPCPeeringConnection'
             PeerRoleArn:!Ref PeerRoleArn
```

Answer: D,E

Explanation:

QUESTION NO: 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.

Answer: D

Explanation:

QUESTION NO: 77

A network engineer is deploying an application on an Amazon EC2 instance. The instance is reachable within the VPC through its private IP address and from the internet using an elastic IP address. Clients are connecting to the instance over the Internet and within the VPC, and the application needs to be identified by a single custom Fully Qualified Domain Name that is publicly resolvable –'app.example.com'.

Instances within the VPC should always connect to the private IP to minimize data transfer costs.

How should the engineer configure DNS to support these requirements?

A.
Use Amazon Route 53 to create a geo-based routing entry for the hostname 'app' in the DNS zone 'example.com'.

B.
Create two A record entries for 'app' in the DNS zone 'example.com' – one for the public IP and one for the private IP.

C.
Use Route 53 to create an ALIAS record to the public DNS name for the instance.

D.
Create a CNAME for 'app' in the DNS zone 'example.com' to the public DNS name for the Amazon EC2 instance.

Answer: D

Explanation:

QUESTION NO: 78

A Network Engineer is troubleshooting a network connectivity issue for an instance within a public subnet that cannot connect to the internet. The first step the Engineer takes is to SSH to the instance via a local bastion within the VPC and runs an ifconfig command to inspect the IP addresses configured on the instance. The output is as follows:

```
[ec2-user@ip-172-31-8-24 ~]$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 0A:A9:4A:21:41:BE
          inet addr:172.31.8.24  Bcast:172.31.15.255  Mask:255.255.240.0
          inet6 addr: fe80::8a9:4aff:fe21:41be/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:557703 errors:0 dropped:0 overruns:0 frame:0
          TX packets:542300 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:59639585 (56.8 MiB)  TX bytes:101633146 (96.9 MiB)
```

The Engineer notices that the command output does not contain a public IP address. In the AWS Management Console, the public subnet has a route to the internet gateway. The instance also has a public IP address associated with it.

What should the Engineer do next to troubleshoot this situation?

A.
Configure the public IP on the interface.

B.
Disable source/destination checking for the instance.

C.
Associate an Elastic IP address to the interface.

D.
Evaluate the security groups and the network access control list.

Answer: B

Explanation:

QUESTION NO: 79

A company uses a single connection to the internet when connecting its on-premises location to AWS. It has selected an AWS Partner Network (APN) Partner to provide a point-to-point circuit for its first-ever 10 Gbps AWS Direct Connect connection.

What steps must be taken to order the cross-connect at the Direct Connect location?

A.
Obtain the LOA/CFA from the APN Partner when ordering connectivity. Upload it to the AWS Management Console when creating a new Direct Connect connection. AWS will ensure that the cross-connect is installed.

B.

Obtain the LOA/CFA from the AWS Management Console when ordering the Direct Connect connection. Provide it to the APN Partner when ordering connectivity. The Direct Connect partner will ensure that the cross-connect is installed.

C.
Obtain one LOA/CFA each from the AWS Management Console and the APN Partner. Provide both to the Facility Operator of the Direct Connect location. The Facility Operator will ensure that the cross-connect is installed.

D.
Identify the APN Partner in the AWS Management Console when creating the Direct Connect connection. Provide the resulting Connection ID to the APN Partner, who will ensure that the cross-connect is installed.

Answer: C
Explanation:

QUESTION NO: 80

An organization's Security team has a requirement that all data leaving its on-premises data center be encrypted at the network layer and use dedicated connectivity. There is also a requirement to centrally log all traffic flow in Amazon VPC environments. An AWS Direct Connect connection has been ordered to build out this design.

What steps should be taken to ensure that connectivity to AWS meets these security requirements? (Choose two.)

A.
Provision a public virtual interface on AWS Direct Connect and set up a VPN to each VPC.

B.
Provision a private virtual interface for each VPC connection.

C.
Enable VPC Flow Logs for each VPC.

D.
Use AWS KMS to encrypt traffic between on-premises and AWS.

E.
Provision a VPN connection to each VPC over the internet.

Answer: B,E

Reference: https://d1.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf

QUESTION NO: 81

A company has an application running on Amazon EC2 instances in a private subnet that connects to a third-party service provider's public HTTP endpoint through a NAT gateway. As request rates increase, new connections are starting to fail. At the same time, the ErrorPortAllocation Amazon CloudWatch metric count for the NAT gateway is increasing.

Which of the following actions should improve the connectivity issues? (Choose two.)

A.
Allocate additional elastic IP addresses to the NAT gateway.

B.
Request that the third-party service provider implement HTTP keepalive.

C.
Implement TCP keepalive on the client instances.

D.
Create additional NAT gateways and update the private subnet route table to introduce the new NAT gateways.

E.
Create additional NAT gateways in the public subnet and split client instances into multiple private subnets, each with a route to a different NAT gateway.

Answer: C,D
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/vpc-resolve-port-allocation-errors/

QUESTION NO: 82

An application runs on a fleet of Amazon EC2 instances in a VPC. All instances can reach one another using private IP addresses. The application owner has a new requirement that the domain name received via DHCP should be different for a particular set of instances that are currently in one particular subnet.

What changes should be made to meet this requirement while continuing to support the existing application requirements?

A.
Modify the existing DHCP option set and specify the different domain name for the specified subnet.

B.
Create a new DHCP option set with the different domain name, associate it with the specified subnet, and re-launch the Amazon EC2 instances.

C.
Create a new subnet, configure the DHCP option set with the different domain name, and re-launch the required instances there.

D.
Create a new peered VPC, configure the DHCP option set with the different domain name, and re-launch the required instances there.

Answer: B

Explanation:

QUESTION NO: 83

A Network Engineer has enabled VPC Flow Logs to troubleshoot an ICMP reachability issue for an echo reply from an Amazon EC2 instance. The flow logs reveal an ACCEPT record for the request from the client to the EC2 instance, and a REJECT record for the response from the EC2 instance to the client.

What is the MOST likely reason for there to be a REJECT record?

A.
The security group is denying inbound ICMP.

B.
The network ACL is denying inbound ICMP.

C.
The security group is denying outbound ICMP.

D.
The network ACL is denying outbound ICMP.

Answer: B

Explanation:

QUESTION NO: 84

An organization has multiple applications running in VPCs across multiple AWS accounts. The network engineer has deployed a central VPC with a pair of software VPN instances that run IPSec tunnels with dynamic routing to VGWs of all application VPCs. This central VPC is connected to on-premises resources via a Direct Connect connection using a private VIF.

What additional configuration is required to enable the applications in VPCs to communicate with each other and access on-premises resources?

A.
Configure each application VPC with a static route entry pointing the on-premises CIDR block to the software VPN instances.

B.
Configure the central VPC with a static route entry pointing the on-premises CIDR block to local VGWs.

C.
Advertise all application VPC CIDR blocks to on-premises resources via the VGW in the central VPC.

D.
Configure IPSec tunnels from the on-premises router into the software VPN instances with dynamic routing.

Answer: B

Explanation:

QUESTION NO: 85

A Network Engineer needs to create a public virtual interface on the company's AWS Direct Connect connection and only import routes which originated from the same region as the Direct Connect location.

What action should accomplish this?

A.
Configure a prefix list on the customer router containing the AWS IP address ranges for the specific region.

B.
Configure a filter on the company's router to only import routes with the 7224:8100 BGP community attribute.

C.
Configure a filter on the company's router to only import routes without a BGP community attribute and a maximum path length of 3.

D.
Configure a filter in the console and only allow routes advertised by AWS without a BGP community attribute and a maximum path length of 3.

Answer: A
Explanation:

QUESTION NO: 86

A network engineer has configured a private hosted zone using Amazon Route 53. The engineer needs to configure health checks for record sets within the zone that are associated with instances.

How can the engineer meet the requirements?

A.
Configure a Route 53 health check to a private IP associated with the instances inside the VPC to be checked.

B.
Configure a Route 53 health check pointing to an Amazon SNS topic that notifies an Amazon CloudWatch alarm when the Amazon EC2 StatusCheckFailed metric fails.

C.
Create a CloudWatch metric that checks the status of the EC2 StatusCheckFailed metric, add an alarm to the metric, and then create a health check that is based on the state of the alarm.

D.
Create a CloudWatch alarm for the StatusCheckFailed metric and choose Recover this instance, selecting a threshold value of 1.

Answer: A
Explanation:

QUESTION NO: 87

An architecture is being designed to support an Amazon WorkSpaces deployment of 1,000 desktops.

Which architecture will support this deployment while allowing for future expansion?

A.
A VPC with a /16 CIDR and one /21 subnet

B.
A VPC with a /20 CIDR and two /21 subnets

C.
A VPC with a /16 CIDR and one /22 subnet

D.
A VPC with a /20 CIDR and two /23 subnets

Answer: C
Explanation:

QUESTION NO: 88

An organization is deploying an application in a VPC that requires SSL mutual authentication with a client-side certificate, as that is the primary method of identifying clients. The Network Engineer has been tasked with defining the mechanism used within AWS to provide the SSL mutual authentication.

Which of the following options meets the organization's requirements?

A.
Use a Classic Load Balancer and upload the client certificate private keys to it. Perform SSL mutual authentication of the client-side certificate there.

B.

Use a Network Load Balancer with a TCP listener on port 443, and pass the request through for the SSL mutual authentication to be handled by a backend instance.

C.
Use an Application Load Balancer and upload the client certificate private keys to it by using the native server name indication (SNI) features with smart certificate selection to handle multiple calling applications.

D.
Front the application with Amazon API Gateway, and use its client-side SSL mutual authentication feature that uses the backend instances to verify the source of the request.

Answer: C
Reference: https://aws.amazon.com/about-aws/whats-new/2017/10/elastic-load-balancing-application-load-balancers-now-support-multiple-ssl-certificates-and-smart-certificate-selection-using-server-name-indication-sni/

QUESTION NO: 89

A network architect is designing an internet website. It has web, application, and database tiers that will run in AWS. The website uses Amazon DynamoDB.

Which architecture will minimize public exposure of the back-end instances?

A.
A VPC with public subnets for the NLB, public subnets for the web tier, private subnets for the application tier, and private subnets for DynamoDB.

B.
A VPC with public subnets for the ALB, private subnets for the web tier, and private subnets for the application tier. The application tier connects DynamoDB through a VPC endpoint.

C.
A VPC with public subnets for the ALB, public subnets for the web tier, private subnets for the application tier, and private subnets for DynamoDB.

D.
A VPC with public subnets for the NLB, private subnets for the web tier, and public subnets for the application tier. The application tier connects DynamoDB through a VPC endpoint.

Answer: D

Explanation:

QUESTION NO: 90

A company is connecting to a VPC over an AWS Direct Connect using a private VIF, and a dynamic VPN connection as a backup. The company's Reliability Engineering team has been running failover and resiliency tests on the network and the existing VPC by simulating an outage situation on the Direct Connect connection. During the resiliency tests, traffic failed to switch over to the backup VPN connection.

How can this failure be troubleshot?

A.
Ensure that Bidirectional Forwarding Detection is enabled on the Direct Connect connection

B.
Confirm that the same routes are being advertised over both the VPN and Direct Connect.

C.
Reconfigure the Direct Connect session from static routes to Border Gateway Protocol (BGP) peering.

D.
Configure a virtual private gateway for the VPN and another virtual private gateway for Direct Connect.

Answer: C
Reference: https://aws.amazon.com/answers/networking/aws-single-data-center-ha-network-connectivity/

QUESTION NO: 91

An organization is migrating its on-premises applications to AWS by using a lift-and-shift approach, taking advantage of managed AWS services wherever possible. The company must be able to edit the application code during the migration phase. One application is a traditional three-tier application, consisting of a web presentation tier, an application tier, and a database tier. The external calling client applications need their sessions to remain sticky to both the web and application nodes that they initially connect to.

Which load balancing solution would allow the web and application tiers to scale horizontally independent from one another other?

A.
Use an Application Load Balancer at the web tier and a Classic Load Balancer at the application tier. Set session stickiness on both, but update the application code to create an application-controlled cookie on the Classic Load Balancer.

B.
Use an Application Load Balancer at both the web and application tiers, setting session stickiness at the target group level for both tiers.

C.
Deploy a web node and an application node as separate containers on the same host, using task linking to create a relationship between the pair. Add an Application Load Balancer with session stickiness in front of all web node containers.

D.
Use a Network Load Balancer at the web tier, and an Application Load Balancer at the application tier. Enable session stickiness on the Application Load Balancer, but take advantage of the native WebSockets protocols available to the Network Load Balancer.

Answer: B
Explanation:

QUESTION NO: 92

A team implements a highly available solution using Amazon AppStream 2.0. The AppStream 2.0 fleet needs to communicate with resources both in an existing VPC and on-premises. The VPC is connected to the on-premises environment using an AWS Direct Connect private virtual interface.

What implementation enables on-premises users to connect to AppStream and existing VPC resources?

A.
Deploy two subnets into the existing VPC. Add a public virtual interface to the Direct Connect connection for users to access the AppStream endpoint

B.
Deploy two subnets into the existing VPC. Add a private virtual interface on the Direct Connect connection for users to access the AppStream endpoint.

C.

Deploy a new VPC with two subnets. Create a VPC peering connection between the two VPCs for users to access the AppStream endpoint.

D.
Deploy one subnet into the existing VPC. Add a private virtual interface on the Direct Connect connection for users to access the AppStream endpoint.

Answer: A
Explanation:

QUESTION NO: 93

An organization has ordered a new AWS Direct Connect connection. The AWS Management Console reports that the connection is available and BGP status is up. However, the networking team is not able to reach instances in the VPC using ping on the organization's private IP address

What could cause this connectivity issue? (Choose two.)

A.
The VGW is not advertising the correct CIDR range back on-premises.

B.
The instance security group does not allow ICMP traffic.

C.
A public virtual interface must be configured for Amazon EC2 connectivity.

D.
The on-premises router is not advertising the correct CIDR range to AWS.

E.
There is a misconfiguration of the bi-directional forwarding detection.

Answer: C,D
Explanation:

QUESTION NO: 94

A company has a hybrid IT architecture with two AWS Direct Connect connections to provide high

availability. The services hosted on-premises are accessible using public IPs, and are also on the 172.16.0.0/16 range. The AWS resources are on the 192.168.0.0/18 range. The company wants to use Amazon Elastic Load Balancing for SSL offloading, health checks, and sticky sessions.

What should be done to meet these requirements?

A.
Create a Network Load Balancer pointing to the on-premises server's private IP address.

B.
Create an Amazon CloudFront distribution for the on-premises service and use the public IPs of the on-premises servers as the origin.

C.
Create a Network Load Balancer pointing to the on-premises server's public IP address.

D.
Create an Application Load Balancer pointing to the on-premises server's private IP address.

Answer: A
Explanation:

QUESTION NO: 95

A company deployed its production Amazon VPC using CIDR block 33.16.0.0/16. The company has nearly depleted its addresses and now needs to extend the VPC network.

Which CIDR blocks meet the company’s requirement to extend the VPC network with a secondary CIDR? (Choose two.)

A.
33.17.0.0/16

B.
172.16.0.0/18

C.
100.70.0.0/17

D.
192.168.1.0/24

E.

10.0.0.0/8

Answer: A,C
Explanation:

QUESTION NO: 96

A company is deploying a new web application that uses a three-tier model with a public-facing Network Load Balancer and web servers in an Amazon VPC. The application servers are hosted in the company's data center. There is an AWS Direct Connect connection between the VPC and the company’s data center. Load testing results indicate that up to 100 servers, equally distributed across multiple Availability Zones, are required to handle peak loads.

The Network Engineer needs to design a VPC that has a /24 CIDR assigned to it.

How should the Engineer allocate subnets across three Availability Zones for each tier?

A.
Network Load Balancer: /29 per subnet

Web: /26 per subnet

B.
Network Load Balancer: /28 per subnet

Web: /25 per subnet

C.
Network Load Balancer: /28 per subnet

Web: /27 per subnet

D.
Network Load Balancer: /28 per subnet

Web: /26 per subnet

Answer: D
Explanation:

QUESTION NO: 97

Changes made to a security group attached to an Application Load Balancer resulted in connectivity issues for a company's production web application. The Network Engineer needs to lock down permissions for the company's AWS account, automate auditing for any changes, and set up notifications.

What actions should accomplish this?

A.
Configure IAM user policies to lock down permissions for specific users. Enable AWS CloudTrail to identify API calls from users. Use AWS Config to audit any changes, and configure Amazon SNS to send notifications.

B.
Configure IAM user policies to lock down permissions for specific users. Enable AWS CloudTrail to identify the API calls from users. Configure AWS CodeCommit to audit any changes in configurations, and configure Amazon SNS to send notifications.

C.
Configure IAM user policies to lock down permissions for specific users. Enable AWS CloudTrail to identify the API calls from users. Configure Amazon Macie to use machine learning to identify any configuration changes, and configure Amazon SNS to send notifications.

D.
Configure IAM role policies to lock down permissions for specific users. Configure Amazon GuardDuty to audit and monitor configuration changes, and configure Amazon SNS to send notifications.

Answer: D
Explanation:

QUESTION NO: 98

A computing team is evaluating whether to place a high performance computing (HPC) application in AWS. The team is concerned about application performance and wants to know what options are available to increase networking performance.

Which of the following changes would increase performance for this application? (Choose two.)

A.
Place the application across many smaller instances to achieve higher total throughput.

B.
Increase the MTU of the VPC to 9001.

C.
Enable an MTU of 9001 in the application's operating system.

D.
Enable enhanced networking on the instances.

E.
Deploy the application in two Availability Zones and insert them in one placement group.

Answer: B,D
Explanation:

QUESTION NO: 99

An organization has created a web application inside a VPC and wants to make it available to 200 client VPCs. The client VPCs are in the same region but are owned by other business units within the organization.

What is the best way to meet this requirement, without making the application publicly available?

A.
Configure the application as an AWS PrivateLink-powered service, and have the client VPCs connect to the endpoint service by using an interface VPC endpoint.

B.
Enable VPC peering between the web application VPC and all client VPCs.

C.
Deploy the web application behind an internet-facing Application Load Balancer and control which clients have access by using security groups.

D.
Deploy the web application behind an internal Application Load Balancer and control which clients have access by using security groups.

Answer: C
Explanation:

QUESTION NO: 100

A company's IT Security team needs to ensure that all servers within an Amazon VPC can communicate with a list of five approved external IPs only. The team also wants to receive a notification every time any server tries to open a connection with a non-approved endpoint.

What is the MOST cost-effective solution that meets these requirements?

A.
Add allowed IPs to the network ACL for the application server subnets. Enable VPC Flow Logs with a filter set to ALL. Create an Amazon CloudWatch Logs filter on the VPC Flow Logs log group filtered by REJECT. Create an alarm for this metric to notify the Security team.

B.
Enable Amazon GuardDuty on the account and the specific region. Upload a list of allowed IPs to Amazon S3 and link the S3 object to the GuardDuty trusted IP list. Configure an Amazon CloudWatch Events rule on all GuardDuty findings to trigger an Amazon SNS notification to the Security team.

C.
Add allowed IPs to the network ACL for the application server subnets. Enable VPC Flow Logs with a filter set to REJECT. Set an Amazon CloudWatch Logs filter for the log group on every event. Create an alarm for this metric to notify the Security team.

D.
Enable Amazon GuardDuty on the account and specific region. Upload a list of allowed IPs to Amazon S3 and link the S3 object to the GuardDuty threat IP list. Integrate GuardDuty with a compatible SIEM to report on every alarm from GuardDuty.

Answer: A
Explanation:

QUESTION NO: 101

The Security department has mandated that all outbound traffic from a VPC toward an on-premises datacenter must go through a security appliance that runs on an Amazon EC2 instance.

Which of the following maximizes network performance on AWS? (Choose two.)

A.
Support for the enhanced networking drivers

B.
Support for sending traffic over the Direct Connect connection

C.
The instance sizes and families supported by the security appliance

D.
Support for placement groups within the VPC

E.
Security appliance support for multiple elastic network interfaces

Answer: B,C
Explanation:

QUESTION NO: 102

A Network Engineer needs to be automatically notified when a certain TCP port is accessed on a fleet of Amazon EC2 instances running in an Amazon VPC.

Which of the following is the MOST reliable solution?

A.
Create an inbound rule in the VPC's network ACL that matches the TCP port. Create an Amazon CloudWatch alarm on the NetworkPackets metric for the ACL that uses Amazon SNS to notify the Administrator when the metric is greater than zero.

B.
Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to notify the Administrator with Amazon SNS each time the TCP port is accessed.

C.
Create VPC Flow Logs that write to Amazon CloudWatch Logs, with a metric filter matching connections on the required port. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.

D.
Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to publish to a custom Amazon CloudWatch metric each time the TCP port is accessed. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.

Answer: A

Explanation:

QUESTION NO: 103

A network engineer deploys an application in a private subnet in a VPC that connects to many external video feed providers using RTMP over the internet. A NAT gateway has been deployed in a public subnet and is working as expected. From the Amazon EC2 instance, the application is able to connect to all feed providers except one, which hangs when connecting. Manually testing a connection from an Amazon EC2 instance in the public subnet to the problem feed indicates that the feed works as expected.

What is causing this issue?

A.
The NAT gateway does not support fragmented packets.

B.
The internet gateway only supports an MTU of 1500 bytes.

C.
An Amazon EC2 instance expects to communicate with an MTU of 9001.

D.
The security group on the instances does not allow PMTUD.

Answer: D
Explanation:

QUESTION NO: 104

A company has an application running in an Amazon VPC that must be able to communicate with on-premises resources in a data center. Network traffic between AWS and the data center will initially be minimal, but will increase to more than 10 Gbps over the next few months. The company's goal is to launch the application as quickly as possible.

The Network Engineer has been asked to design a hybrid IT connectivity solution.

What should be done to meet these requirements?

A.
Submit a 1 Gbps AWS Direct Connect connection request, then increase the number of Direct Connect connections, as needed.

B.
Allocate elastic IPs to Amazon EC2 instances for temporary access to on-premises resources, then provision AWS VPN connections between an Amazon VPC and the data center.

C.
Provision an AWS VPN connection between an Amazon VPC and the data center, then submit an AWS Direct Connect connection request. Later, cut over from the VPN connection to one or more Direct Connect connections, as needed.

D.
Provision a 100 Mbps AWS Direct Connect connection between an Amazon VPC and the data center, then submit a Direct Connect connection request. Later, cut over from the hosted connection to one or more Direct Connect connections, as needed.

Answer: B
Explanation:

QUESTION NO: 105

A company has recently established an AWS Direct Connect connection from its on-premises data center to AWS. A Network Engineer has blocked all traffic destined for Amazon S3 over the company's gateway to the internet from its on-premises firewall. S3 traffic should only traverse the Direct Connect connection. Currently, no one in the on-premises data center can access Amazon S3.

Which solution will resolve this connectivity issue?

A.
Configure a private virtual interface on the Direct Connect connection. Update the on-premises routing tables to choose Direct Connect as the preferred next hop for traffic destined for Amazon S3.

B.
Establish an S3 VPC endpoint for the company's Amazon VPC. Configure a private virtual interface on the Direct Connect connection. Update the on-premises routing tables to choose Direct Connect as the preferred next hop.

C.
Configure a public virtual interface on the Direct Connect connection. Update the on-premises routing tables to choose Direct Connect as the preferred next hop for traffic destined for Amazon

S3.

D.
Configure a public virtual interface on the Direct Connect connection. Establish an AWS managed VPN over the connection. Update the on-premises routing tables to choose the VPN connection as the preferred next hop.

Answer: A
Explanation:

QUESTION NO: 106

A company provisions an AWS Direct Connect connection to permit access to Amazon EC2 resources in several Amazon VPCs and to data stored in private Amazon S3 buckets. The Network Engineer needs to configure the company's on-premises router for this Direct Connect connection.

Which of the following actions will require the LEAST amount of configuration overhead on the customer router?

A.
Configure private virtual interfaces for the VPC resources and for Amazon S3.

B.
Configure private virtual interfaces for the VPC resources and a public virtual interface for Amazon S3.

C.
Configure a private virtual interface to a Direct Connect gateway for the VPC resources and for Amazon S3.

D.
Configure a private virtual interface to a Direct Connect gateway for the VPC resources and a public virtual interface for Amazon S3.

Answer: A
Explanation:

QUESTION NO: 107

A company has two redundant AWS Direct Connect connections to a VPC. The VPC is configured using BGP metrics so that one Direct Connect connection is used as the primary traffic path. The company wants the primary Direct Connect connection to fail to the secondary in less than one second.

What should be done to meet this requirement?

A.
Configure BGP on the company's router with a keep-alive to 300 ms and the BGP hold timer to 900 ms.

B.
Enable Bidirectional Forwarding Detection (BFD) on the company's router with a detection minimum interval of 300 ms and a BFD liveness detection multiplier of 3.

C.
Enable Dead Peer Detection (DPD) on the company's router with a detection minimum interval of 300 ms and a DPD liveliness detection multiplier of 3.

D.
Enable Bidirectional Forwarding Detection (BFD) echo mode on the company's router and disable sending the Internet Control Message Protocol (ICMP) IP packet requests.

Answer: B
Reference: https://aws.amazon.com/directconnect/faqs/

QUESTION NO: 108

A company's Network Engineering team is solely responsible for deploying VPC infrastructure using AWS CloudFormation. The company wants to give its Developers the ability to launch applications using CloudFormation templates so that subnets can be created using available CIDR ranges.

What should be done to meet these requirements?

A.
Create a CloudFormation templates with Amazon EC2 resources that rely on cfn-init and cfn-signals to inform the stack of available CIDR ranges.

B.
Create a CloudFormation template with a custom resource that analyzes traffic activity in VPC Flow Logs and reports on available CIDR ranges.

C.
Create a CloudFormation template that references the Fn::Cidr intrinsic function within a subnet resource to select an available CIDR range.

D.
Create a CloudFormation template with a custom resource that uses AWS Lambda and Amazon DynamoDB to manage available CIDR ranges.

Answer: C

Explanation:

QUESTION NO: 109

A company's web application is deployed on Amazon EC2 instances behind a public Application Load Balancer. The application flags malicious requests and uses an AWS Lambda function to add the offending IP addresses to the network ACL to block any further request for 24 hours. Recently, the application has been receiving more malicious requests, which causes the network ACL to reach its limit of allowed entries.

Which action should be taken to block more IP addresses, without compromising the existing security requirements?

A.
Update the AWS Lambda function to remove blocked entries from the network ACL after 2 hours.

B.
Update the AWS Lambda function to block malicious IPs in security groups rather than the network ACL.

C.
Update the AWS Lambda function to block malicious IPs in AWS WAF attached to the Application Load Balancer.

D.
Update the AWS Lambda function to add an additional network ACL to the subnets once the limit for the previous ones has been reached.

Answer: D

Explanation:

QUESTION NO: 110

A company is using AWS to host all of its applications. Each application is isolated in its own Amazon VPC. Different environments such as Development, Test, and Production are also isolated in their own VPCs. The Network Engineer needs to automate VPC creation to enforce the company's network and security standards. Additionally, the CIDR range used in each VPC needs to be unique.

Which solution meets all of these requirements?

A.
Use AWS CloudFormation to deploy the VPC infrastructure and a custom resource to request a CIDR range from an external IP address management (IPAM) service.

B.
Use AWS OpsWorks to deploy the VPC infrastructure and a custom resource to request a CIDR range from an external IP address management (IPAM) service.

C.
Use the VPC wizard in the AWS Management Console. Type in the CIDR blocks for the VPC and subnets.

D.
Create the VPCs using AWS CLI and use the dry-run flag to validate if the current CIDR range is in use.

Answer: A

Explanation: