Amazon AWS Certified Advanced Networking - Specialty

AWS Certified Advanced Networking - Specialty Exam

Version: 9.0

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

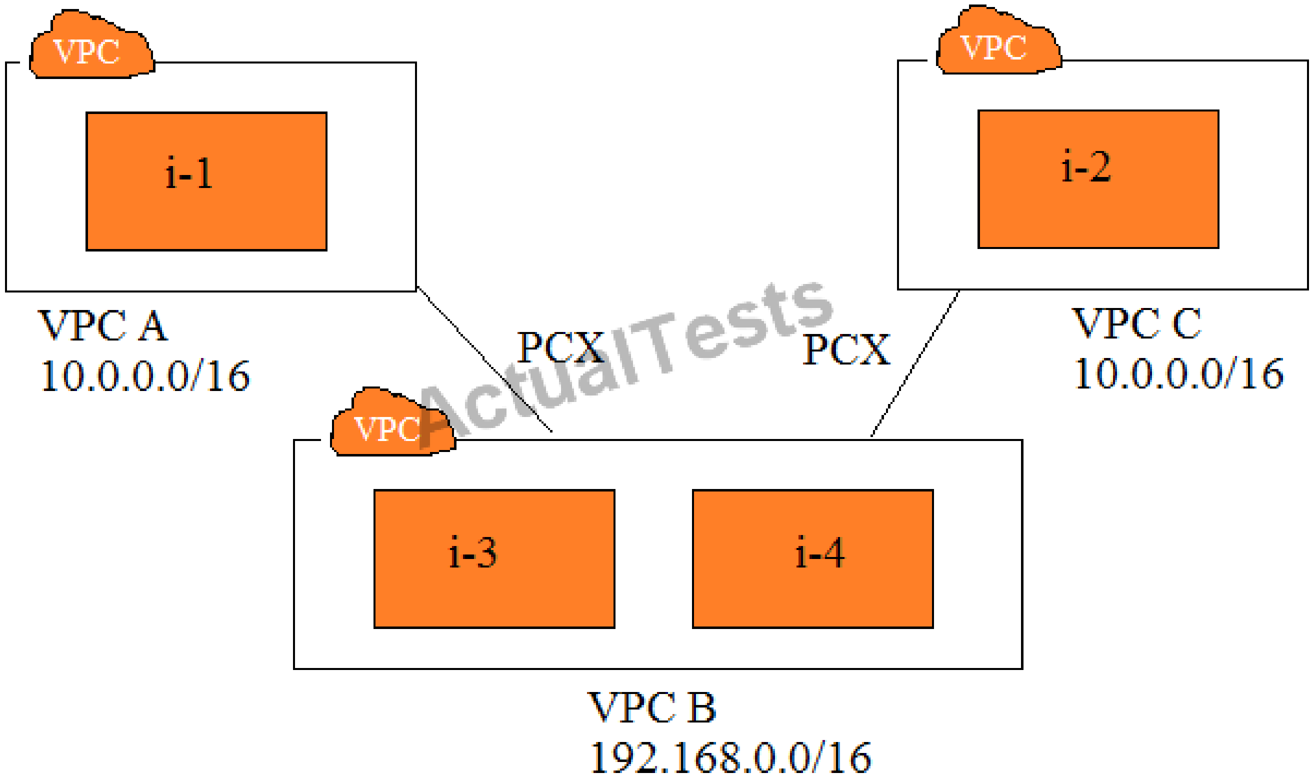
D.
AWS hardware VPN between the virtual private gateways in each region

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 balanced 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:

An ACCEPT record for the originating ping that was allowed by both the network ACL and the security group, and therefore was allowed to reach your instance.

A REJECT record for the response ping that the network ACL denied.

If your network ACL permits outbound ICMP traffic, the flow log displays two ACCEPT records (one for the originating ping and one for the response ping). If your security group denies inbound ICMP traffic, the flow log displays a single REJECT record, because the traffic was not permitted to reach your instance.

Reference: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

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 ENAs.

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

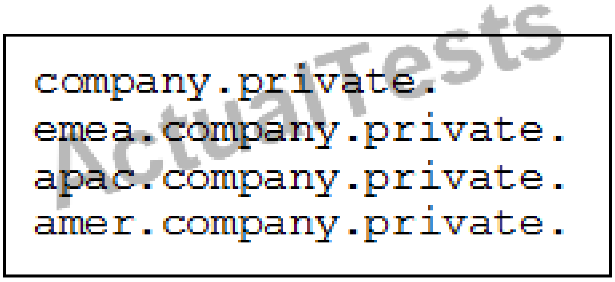
D.
Use a Route 53 private hosted zone for example.com and perform subdomain delegation for dev.example.com

Answer: A

Explanation:

QUESTION NO: 69

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



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

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

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

A.
Create a Route 53 Private Hosted Zone for each of the four zones and associate them with the three VPCs.

B.
Create a single Route 53 Private Hosted Zone for the zone company.private. and associate it with the three VPCs.

C.
Create a Route 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.

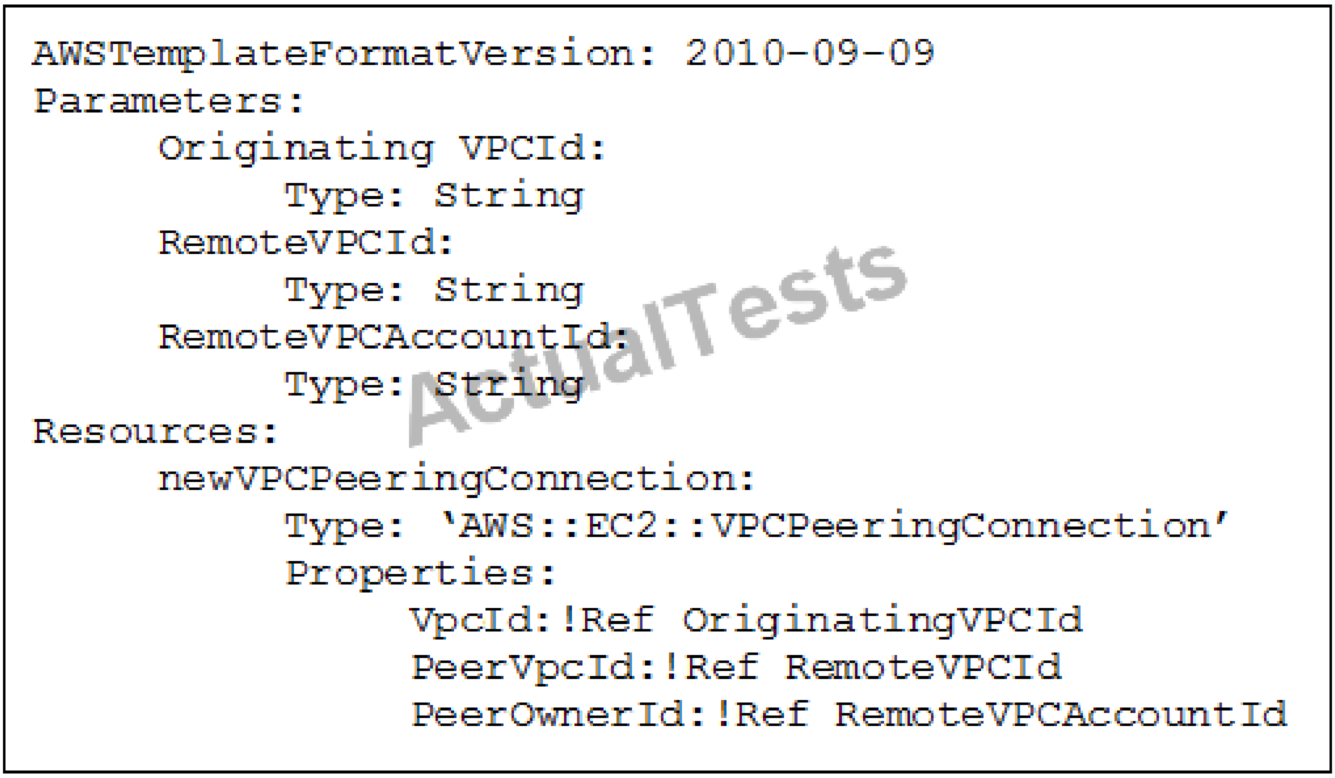
D.
Use an Application Load Balancer to automatically preserve the source IP address in the X-Forwarded-For header.

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.

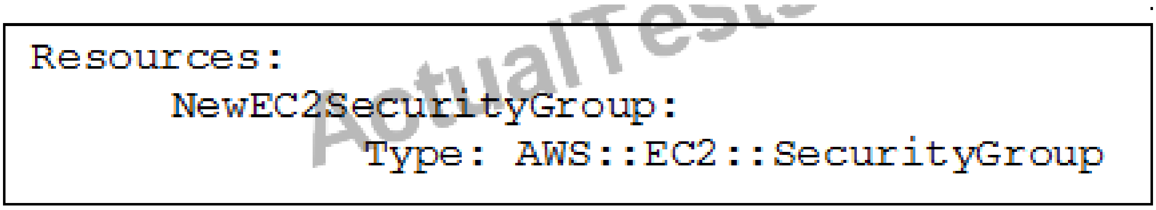
The template below creates the VPC peering connection in the Originating account. It contains these components:



```
AWSTemplateFormatVersion: 2010-09-09
Parameters:
      Originating VPCId:
            Type: String
      RemoteVPCId:
            Type: String
      RemoteVPCAccountId:
            Type: String
Resources:
      newVPCPeeringConnection:
            Type: ‘AWS::EC2::VPCPeeringConnection’
            Properties:
                  VpcId:!Ref OriginatingVPCId
                  PeerVpcId:!Ref RemoteVPCId
                  PeerOwnerId:!Ref RemoteVPCAccountId
```

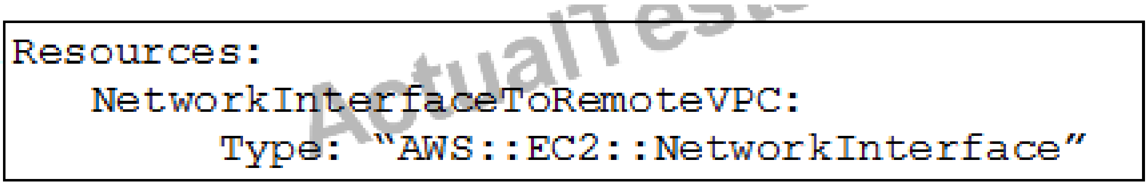
Which additional AWS CloudFormation components are necessary in the Originating account to create an operational cross-account VPC peering connection with AWS CloudFormation? (Choose two.)

A.



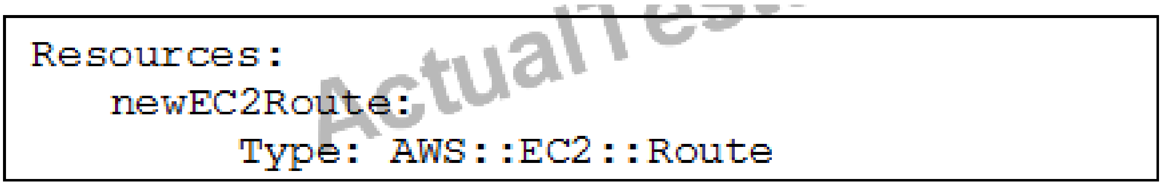
```
Resources:
      NewEC2SecurityGroup:
            Type: AWS::EC2::SecurityGroup
```

B.



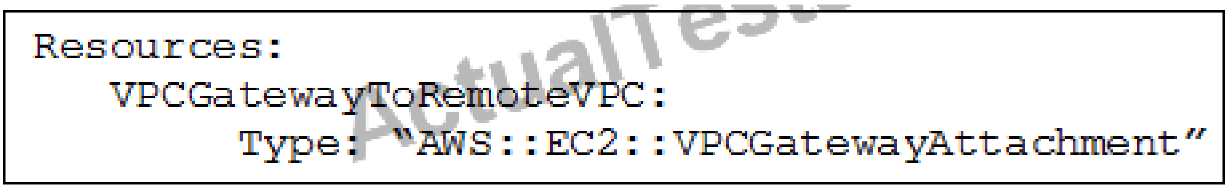
```
Resources:
   NetworkInterfaceToRemoteVPC:
         Type: “AWS::EC2::NetworkInterface”
```

C.



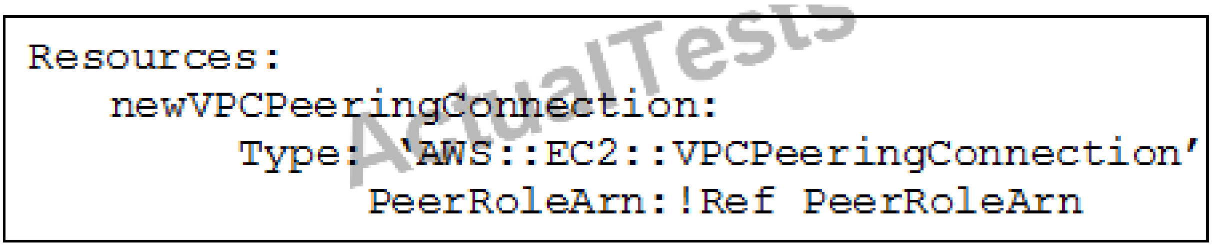
```
Resources:
   newEC2Route:
         Type: AWS::EC2::Route
```

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.

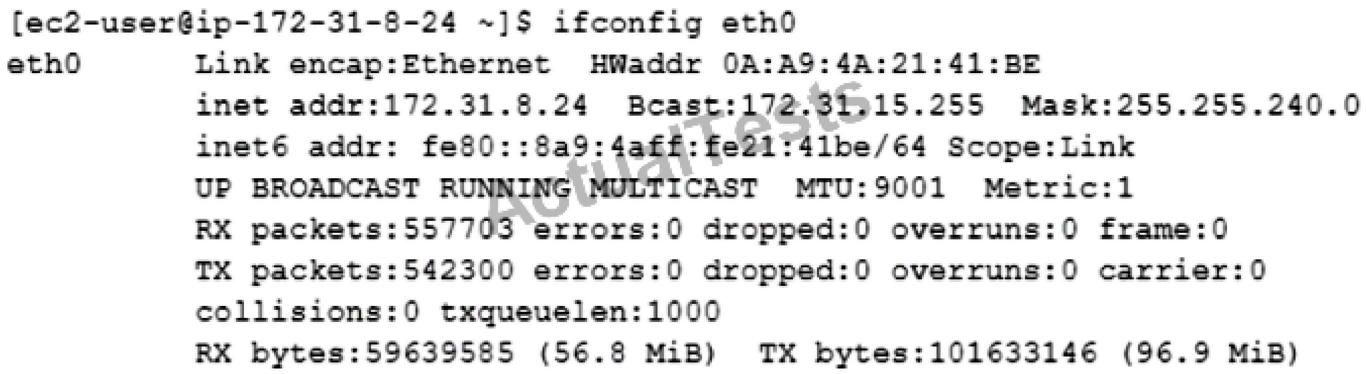
D.
Create a CNAME for ‘app’ in the DNS zone ‘example.com’ to the public DNS name for the Amazon EC2 instance.

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: B
Reference:

https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html

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:

QUESTION NO: 111

You can turn on the AWS Config service from the AWS CLI by running the subscribe command and passing as parameters a valid IAM role, SNS topic, and ____.

A.
EBS volume

B.
EC2 instance

C.
S3 bucket

D.
Kinesis stream

Answer: C
Explanation:

You can use the AWS CLI to turn on AWS Config. All it takes is the subscribe command and a few additional parameters. The parameters are -s3-bucket, which specifies the S3 bucket to which AWS Config data will be saved, -sns-topic, which specifies to which SNS topic messages from AWS Config will be sent, and -iam-role, which is an IAM role containing appropriate permissions for AWS Config to access the resources it monitors.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/gs-cli-subscribe.html

QUESTION NO: 112

You would like to automate the monitoring of changes in the configurations of your AWS resources and respond programmatically to configurations of only a certain type. To do this, you could use Amazon ____ as the endpoint for the Amazon SNS topics that generate messages from AWS Config.

A.
Kinesis

B.
Simple Email Service (SES)

C.
Simple Storage Service (S3)

D.
Simple Queue Service (SQS)

Answer: D
Explanation:

AWS Config uses Amazon Simple Notification Service (SNS) to send you notifications every time a supported AWS resource is created, updated, or otherwise modified as a result of user API activity. However, you might be interested in only certain resource configuration changes. For example, you might consider it critical to know when someone modifies the configuration of a security group, but not need to know every time there is a change to tags on your Amazon EC2 instances. Or, you might want to write a program that performs specific actions when specific resources are updated. For example, you might want to start a certain workflow when a security group configuration is changed. If you want to programmatically consume the data from AWS Config in these or other ways, use an Amazon Simple Queue Service queue as the notification endpoint for Amazon SNS.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/monitor-resource-changes.html

QUESTION NO: 113

You can use the ____ command of the AWS Config service CLI to see the compliance state for each AWS resource of a specific type.

A.
describe-compliance-by-resource

B.
get-compliance-details-by-config-rule

C.
describe-compliance-by-config-rule

D.
get-compliance-details-by-resource

Answer: A

Explanation:

You can use the AWS Config console, AWS CLI, or AWS Config API to view the compliance state of your rules and resources. The describe-compliance-by-resource command of the AWS Config CLI to see the compliance state for each AWS resource of a specific type. This is distinct from the describe-compliance-by-config-rule command, which gives the compliance state of each rule in AWS Config .

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_view-compliance.html

QUESTION NO: 114

When an AWS Config rule is triggered a JSON object known as an AWS Config Event is created. This object contains another JSON string in its ____ parameter, which describes the event that triggered the rule.

A.
resultToken

B.
eventLeftScope

C.
invokingEvent

D.
configRuleName

Answer: C

Explanation:

The JSON object for an AWS Config event contains an invoking Event attribute, which describes the event that triggers the evaluation for a rule. If the event is published in response to a resource configuration change, the value for this attribute is a string that contains a JSON configuration Item or a configuration Item Summary (for oversized configuration items). The configuration item represents the state of the resource at the moment that AWS Config detected the change. If the event is published for a periodic evaluation, the value is a string that contains a JSON object. The object includes information about the evaluation that was triggered. For each type of event, a function must parse the string with a JSON parser to be able to evaluate its contents.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_exa mple-events.html

QUESTION NO: 115

When an AWS Config rule is triggered a JSON object known as an AWS Config Event is created. This object contains a(n) ____ attribute, which is a JSON-formatted set of key/value pairs the receiving AWS Lambda function processes as part of its evaluation logic.

A.
inputParameters

B.
invokingEvent

C.
ruleConfiguration

D.
mappingTemplate

Answer: A

Explanation:

The JSON object for an AWS Config event contains a ruleParameters attribute, which is a set of key/value pairs that the AWS Lambda function receiving the event processes as part of its evaluation logic. You define parameters when you use the AWS Config console to create a custom rule. You can also define parameters with the InputParameters attribute in the PutConfigRule AWS Config API request or the put-config-rule AWS CLI command. The JSON code for the parameters is contained within a string, so a function must parse the string with a JSON parser to be able to evaluate its contents

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_exa mple-events.html

QUESTION NO: 116

When using AWS Config, which two items are stored on S3 as a part of its operation?

A.
Configuration Items and Configuration History

B.
Configuration Recorder and Configuration Snapshots

C.
Configuration History and Configuration Snapshots

D.
Configuration Snapshots and Configuration Streams

Answer: C

Explanation:

S3 is used to store the Configuration History files and any Configuration Snapshots of your data within a single bucket, which is defined within the Configuration Recorder. You can get AWS Config to create a new bucket for you and select an existing bucket. If you have multiple AWS accounts you may want to aggregate your Configuration History and Snapshot files into the same S3 Bucket for your primary account, just be aware that this can be achieved. However, you will need to grant write access for the service principal (config.amazonaws.com) in your other accounts write access to the S3 bucket.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/config-concepts.html#config-items

QUESTION NO: 117

You can use the ____ page of the AWS Config console to look up resources that AWS Config has discovered, including deleted resources and resources that are not currently being recorded.

A.
snapshot listing

B.
configuration history

C.
resource inventory

D.
resource database

Answer: C

Explanation:

You can use the AWS Config console, AWS CLI, and AWS Config API to look up the resources that AWS Config has taken an inventory of, or discovered, including deleted resources and resources that AWS Config is not currently recording. AWS Config discovers supported resource types only. You can use the AWS Config console in the AWS Management console to look up these resources. The Resource Inventory page lets you perform this search.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/looking-up-discovered-resources.html

QUESTION NO: 118

An AWS Config rule can be set to be evaluated if a certain set of resources undergoes a configuration change. The set of resources to which the rule applies can be restricted by the rule's ____, which can include a combination of a resource type and a resource ID, for example.

A.
trigger

B.
domain

C.
manifest

D.
scope

Answer: D
Explanation:

When you add an AWS Config rule to your account, you can specify when you want AWS Config to run the rule; this is called a trigger. AWS Config evaluates your resource configurations against the rule when the trigger occurs. You choose which resources trigger the evaluation by defining the rule's scope. The scope can include the following:

One or more resource types

A combination of a resource type and a resource ID A combination of a tag key and value.

When any recorded resource is created, updated, or deleted AWS Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to constrain which resources trigger evaluations. Otherwise, evaluations are triggered when any recorded resource changes.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html

QUESTION NO: 119

Which other AWS service is used to track `Related Events' within the Configuration Item?

A.
AWS WAF

B.
SQS

C.
AWS CloudTrail

D.
S3

Answer: C

Explanation:

`Related Events' displays the AWS CloudTrail event ID that is related to the change that triggered the creation of the CI. There is a new CI made for every change made against a resource. As a result a different CloudTrail event IDs will be created. This allows you you to deep-dive into who or what and when made the change that triggered this CI. A great feature allowing for some great analysis to be taken, specifically when this affects security resources.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/resource-config-reference.html#config-item-table

QUESTION NO: 120

Non-compliant resources identified through the use of AWS Config Rules are automatically removed from operational service.

A.
It depends on the Rule configuration

B.
Only if it remains non-compliant for more than 6 hours

C.
True

D.
False

Answer: D

Explanation:

Each time a change is made to one of your supported resources, AWS config will check its compliance against any Config Rules that you have in place. If there is a violation against these rules then AWS Config will send a message to the Configuration Stream via SNS and the resource will be marked as `noncompliant'.

It's important to note that this does not mean the resource will be taken out of service or it will stop working. It will continue to operate exactly as it is with its new configuration. AWS Config simply alerts you that there is a violation and it's up to you to take the appropriate action.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_view-compliance.html

QUESTION NO: 121

Which element of AWS Config can be used to help maintain internal and external compliance controls?

A.
Configuration Item

B.
Configuration Recorder

C.
Configuration Streams

D.
Config Rules

Answer: D

Explanation:

AWS Config allows you to utilise Config Rules to help you manage and organise this compliance which acts as an automatic resource compliance checker. When a change is made to a resource, AWS Config will check to see if the resource matches a rule, and if so it will check the compliance of that resource against the rule following the changes made.

Reference: https://aws.amazon.com/config/

QUESTION NO: 122

Which AWS service is used within an AWS Config Rule to perform the logic evaluation of that rule?

A.
Inspector

B.
WAF

C.
Lambda

D.
SWF

Answer: C
Explanation:

AWS Config Rules are a great way to help you enforce specific compliance controls and checks across your resources and allows for you to adopt an `ideal' deployment specification for each of your resource types. Each Rule is simply a Lambda function that when called upon evaluates the resource and carries out some simply logic to determine the compliance result with the rule.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_nodejs-sample.html

QUESTION NO: 123

AWS Config flags a resource as ____ if a resource violates any conditions of an AWS Config rule that it evaluates on the resource in question.

A.
corrupted

B.
noncompliant

C.

invalid

D.
misconfigured

Answer: B
Explanation:

Use AWS Config to evaluate the configuration settings of your AWS resources. You do this by creating AWS Config rules, which represent your ideal configuration settings. AWS Config provides customizable, predefined rules called managed rules to help you get started. You can also create your own custom rules. While AWS Config continuously tracks the configuration changes that occur among your resources, it checks whether these changes violate any of the conditions in your rules. If a resource violates a rule, AWS Config flags the resource and the rule as noncompliant.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html

QUESTION NO: 124

Each custom AWS Config rule you create must be associated with a(n) AWS ____, which contains the logic that evaluates whether your AWS resources comply with the rule.

A.
Lambda function

B.
Configuration trigger

C.
EC2 instance

D.
S3 bucket

Answer: A
Explanation:

You can develop custom AWS Config rules to be evaluated by associating each of them with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule. You associate this function with your rule, and the rule invokes the function either in response to configuration changes or periodically. The function then evaluates whether your resources comply with your rule, and sends its evaluation results to AWS Config.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules.html

QUESTION NO: 125

A user is trying to understand the detailed CloudWatch monitoring concept. Which of the below mentioned services does not provide detailed monitoring with CloudWatch?

A.
AWS Route53

B.
AWS EMR

C.
AWS ELB

D.
AWS RDS

Answer: B

Explanation:

CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. Services, such as RDS, EC2, Auto Scaling, ELB, and Route 53 can provide the monitoring data every minute.

Reference:

http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/supported_services.html

QUESTION NO: 126

You can use the ____ command of the AWS Config service CLI to see the compliance state of each of your rules.

A.
get-compliance-details-by-resource

B.
describe-compliance-by-config-rule

C.
get-compliance-details-by-config-rule

D.
describe-compliance-by-resource

Answer: B

Explanation:

You can use the describe-compliance-by-config-rule command of the AWS Config CLI to see the compliance state of each of your rules. For each rule that has a compliance type of NON_COMPLIANT, AWS Config returns the number of noncompliant resources for the CappedCount parameter.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_view-compliance.html

QUESTION NO: 127

You have several Amazon Glacier vaults you would like to monitor. How might you monitor those vaults?

A.
Create a custom AWS Config rule.

B.
Use an AWS master Config rule.

C.
Use an AWS managed Config rule.

D.
Create a KMS policy and attach it to your Amazon Glacier vault.

Answer: A

Explanation:

AWS Config does not currently record Amazon Glacier resources; you must create a custom rule if you wish to monitor such a resource.

Reference:

http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_nodejs.html#creating-custom-rules-for-additional-resource-types

QUESTION NO: 128

In order to change the name of the AWS Config ____, you must stop the configuration recorder, delete the current one, and create a new one with a new name, since there can only be one of these per AWS account.

A.
SNS topic

B.
configuration history

C.
delivery channel

D.
S3 bucket path

Answer: C

Explanation:

As AWS Config continually records the changes that occur to your AWS resources, it sends notifications and updated configuration states through the delivery channel. You can manage the delivery channel to control where AWS Config sends configuration updates. You can have only one delivery channel per AWS account, and the delivery channel is required to use AWS Config. To change the delivery channel name, you must delete it and create a new delivery channel with the desired name. Before you can delete the delivery channel, you must temporarily stop the configuration recorder. The AWS Config console does not provide the option to delete the delivery channel, so you must use the AWS CLI, the AWS Config API, or one of the AWS SDKs.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/update-dc.html

QUESTION NO: 129

Which of the following characters is not allowed while creating a Namespace for a CloudWatch metric?

A.
/

B.
:

C.
#

D.
@

Answer: D
Explanation:

Namespace is a grouping or a container for a CloudWatch metric. The names must be valid XML characters, typically containing the alphanumeric characters "0-9A-Za-z" plus "."(period), "-" (hyphen), "_" (underscore), "/" (slash), "#" (hash), and ":" (colon). All AWS namespaces follow the convention AWS/<service>, such as AWS/EC2 and AWS/ELB.

Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

QUESTION NO: 130

You would like to ensure that all Amazon S3 buckets going forward, current and newly created ones, have logging enabled. What type of trigger(s) should you use?

A.
only a periodic trigger

B.
only a configuration change trigger

C.
both configuration change and periodic triggers

D.
only a transitioning trigger

Answer: B
Explanation:

This case requires only a configuration change trigger because you only need to trigger when S3 buckets are created and changed. There is no time component to when the trigger needs to fire.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config-rules.html

QUESTION NO: 131

You have many IAM users with the ability to create EC2 volumes. Most of the data your team works with is sensitive, so you would like to make sure all volumes are encrypted. How might you facilitate this requirement?

A.
Create an AWS KMS policy and attach it to all IAM users that can create EC2 volumes.

B.
Use AWS Config and create a rule that requires all volumes, upon creation, be encrypted.

C.
Use AWS Config to send out reminders to IAM users every time they create an EC2 volume.

D.
Set EC2 to notify creators to encrypt their EC2 volumes.

Answer: B
Explanation:

AWS Config is used to evaluate the configuration settings of many AWS resources. When an EC2 volume in created, AWS Config can evaluate the volume against a rule that requires volumes to be encrypted. If the volume is not encrypted, AWS Config flags the volume and the rule as noncompliant.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html

QUESTION NO: 132

You can use the ____ command of the AWS Config service CLI to see the compliance state of each resource that AWS Config evaluates for a specific rule.

A.
describe-compliance-by-resource

B.
describe-compliance-by-config-rule

C.
get-compliance-details-by-config-rule

D.
get-compliance-details-by-resource

Answer: C
Explanation:

You can use the get-compliance-details-by-config-rule command of the AWS Config CLI to see the compliance state of each resource that AWS Config evaluates for a specific rule.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_view-compliance.html

QUESTION NO: 133

A user is running a batch process on EBS backed EC2 instances. The batch process launches few EC2 instances to process hadoop Map reduce jobs which can run between 50-600 minutes or sometimes for even more time. The user wants a configuration that can terminate the instance only when the process is completed. How can the user configure this with CloudWatch?

A.
Configure a job which terminates all instances after 600 minutes

B.
It is not possible to terminate instances automatically

C.

Set up the CloudWatch with Auto Scaling to terminate all the instances

D.
Configure the CloudWatch action to terminate the instance when the CPU utilization falls below 5%

Answer: D
Explanation:

Amazon CloudWatch alarm watches a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The user can setup an action which terminates the instances when their CPU utilization is below a certain threshold for a certain period of time. The EC2 action can either terminate or stop the instance as part of the EC2 action.

Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html

QUESTION NO: 134

You need to create a subnet in a VPC that supports 14 hosts. You need to be as accurate as possible since you run a very large company. What CIDR should you use?

A.
/28

B.
/24

C.
/25

D.
/27

Answer: D
Explanation:

/27 supports 27 hosts since AWS reserves 5 addresses. /25 supports 123 hosts, /28 supports 11, /24 supports 251.

QUESTION NO: 135

You have a DX connection and a VPN connection as backup for your 10.0.0.0/16 network. You just received a letter indicating that the colocation provider hosting the DX connection will be undergoing maintenance soon. It is critical that you do not experience any downtime or latency during this period.

What is the best course of action?

A.
Configure the VPN as a static VPN instead of dynamic.

B.
Configure AS_PATH Prepending on the DX connection to make it the less preferred path.

C.
Advertise 10.0.0.0/9 and 10.128.0.0/9 over your VPN connection.

D.
None of the above.

Answer: D
Explanation:

A more specific route is the only way to force AWS to prefer a VPN connection over a DX connection. A /9 is not more specific than a /16.

QUESTION NO: 136

You have two enhanced networking capable instances in a placement group. One with an Intel network interface and one with an ENA.

What network speed will be achieved between the two?

A.
10Gbps

B.
20Gbps

C.
5Gbps

D.
You cannot have different network interfaces in a placement group.

Answer: A
Explanation:

10Gbps. The Intel interface has a max speed of 10 and the ENA is 20. The speed will be the lesser of the two.

QUESTION NO: 137

Your company has placement groups in two different availability zones. There is a large project coming up and, although resilience is important, cost and speed are the most important factors. The servers in each placement group need to be able to achieve the highest speed possible.

How can this be achieved?

A.
Create AMIs from all of the instances, terminate them, and deploy them all into one placement group.

B.
In the CLI, run the command "aws ec2 set-placement-group 1 " for all of the instances.

C.
Duplicate the VPC, peer the new VPC, create AMIs of the instances, terminate them, and redeploy them in two separate placement groups between the two VPCs.

D.
Peer the two placement groups using AWS PG Peering.

Answer: A
Explanation:

There is no AWS PG Peering option, Duplicating the VPC does not align with the cost concern, there is no "aws ec2 set-placement-group" command.

QUESTION NO: 138

Your network utilizes jumbo frames on its servers and your router. You are trying to access your AWS resources, and you are having issues with packet loss. What is the best solution?

A.
Remove the "Do not Fragment" flag on the packets.

B.
Lower the MTU for your network.

C.
Call AWS support.

D.
You will have to upgrade to Direct Connect.

Answer: A
Explanation:

Remove the "Don't Fragment" Flag on your router. AWS will drop any data with an MTU of greater than 1500 if the "Do not Fragment" flag is set, so you need your router to indicate that data can be fragmented.

QUESTION NO: 139

You have two VPCs that you need to connect to an on-premises datacenter using VPNs. When you create the tunnels, you find that both tunnels use the same addresses. What two things can you do to overcome this? (Choose two.)

A.
Delete the VPN, create a "dummy VPN", recreate the VPN, then delete the "dummy" VPN.

B.
Delete your AWS account and create a new one since the VPN tunnel addresses are created from a hash of your account number and a proprietary algorithm.

C.
Create a VHF within you router for each network.

D.
Create a VRF within your router for each network.

Answer: A,D

Explanation:

QUESTION NO: 140

Your company just purchased a domain using another registrar and wants to use the same nameservers as your current domain hosted with AWS. How would this be achieved?

A.
Every domain must have different nameservers.

B.
In the API, create a Reusable Delegation Set.

C.
Import the domain to your account and it will automatically set the same nameservers.

D.
In the console, create a Reusable Delegation Set.

Answer: B

Explanation:

You can't create a reusable delegation set in the console. AWS does not provide the same nameservers to new domains, but a reusable delegation set can be used with as many domains as you like.

QUESTION NO: 141

Your company is connecting one data center with one router to several VPCs and needs to access them transitively. What should you do?

A.
Create a VPN to one VPC and peer the others.

B.
This is not possible.

C.

Use a transit VPC with a VPN running on one or more EC2 instances to route traffic between the VPCs.

D.
Just connect; VPCs are transitive in nature.

Answer: C
Explanation:

VPCs are not transitive, so you will need a "transit VPN" in order to route between the VPCs.

QUESTION NO: 142

Your AWS WorkSpaces users are unable to authenticate. What could be one reason for this?

A.
Your AD server is running Windows Server 2016

B.
Port 3389 is not open to your AD server.

C.
Port 389 is not open to your AD server.

D.
Your AD server is running Windows Server 2012 Core Edition.

Answer: C
Explanation:

AD requires port 389.

QUESTION NO: 143

You have just deployed a website that utilizes CloudFront, ELB, and S3 to serve content. When users access your site, they are seeing broken image links. You know you configured CloudFront to use cdn.yourdomain.com. What is the most likely reason why your users not seeing the images?

A.
There is no rule in your bucket policy allowing public access.

B.
The images in S3 are saved as .png instead of .jpg.

C.
There is no record in Route 53 pointing cdn.yourdomain.com to the ALIAS.

D.
The users are using Internet Explorer.

Answer: C
Explanation:

You must have a Route 53 record. You never want to give public access to your content bucket.

QUESTION NO: 144

You are responsible for several EC2 instances deployed from Amazon AMIs that are required to upload information to an S3 bucket. This information must not traverse the public internet. You must also be able to update the instances. Which option is your best solution?

A.
An S3 endpoint and a NAT

B.
An S3 endpoint

C.
A VPN to the IP addresses specified in the AWS official S3 prefix list

D.
A NACL with the AWS prefix list added to it and a VPN.

Answer: B
Explanation:

A NAT is not required as an S3 endpoint will allow an instance to update. C and D are not possible.

QUESTION NO: 145

Your company is building a new data center. You currently have an on-premises data center that accesses your single VPC via VPN. You need to provide access to your single VPC to your new data center. Since your new data center build is already over budget, you need to keep costs low.

How should you accomplish this?

A.
Add a Private VIF and create a Direct Connect connection.

B.
Create a new Customer Gateway and add it to your VPN using a CloudHub infrastructure model.

C.
Add a Public VIF and create a Direct Connect connection.

D.
Create a new Virtual Gateway and add it to your VPN using a CloudHub infrastructure model.

Answer: B

Explanation:

Create a new Customer Gateway. A Private VIF would work, but you want to keep costs low. A Public VIF is only for AWS specific resources, such as S3. A Virtual Gateway would be created if you were creating a new VPN connection in a new VPC. A Customer Gateway would allow you to add the new datacenter to your VPN.

QUESTION NO: 146

You have a website hosted on EC2 that is not serving web pages. You have ensured that the server is running and the site is configured properly. What could be the problem?

A.
Your NACL does not allow port 80 outbound.

B.
Your NACL does not allow ports 1024 65535 outbound.

C.
Your NACL does not allow ports 1024 65535 inbound. D. Your security group does not allow outbound traffic.

Answer: B

Explanation:

The ephemeral ports 1024 65535 are required outbound for return traffic. For the server to access websites, those same ports need to be allowed inbound.

QUESTION NO: 147

You are auditing an AWS infrastructure after you noticed some abnormal charges on the bill. You use AWS Config to monitor your changes. What else is required to find out who made the change?

A.
There is no information to find this. You will need to sign up for Config Premium.

B.
Use the eventID of the change and reference it with your Flow Logs.

C.
Use the eventId of the change and reference it with CloudTrail to find the culprit.

D.
Use the eventID of the change and reference it with CloudWatch to find the culprit.

Answer: C

Explanation:

CloudTrail is for finding "who" performed an action.

QUESTION NO: 148

Your organization has placed a project on hold and has stopped 30 public EC2 instances. These instances use instance store volumes and do not have custom AMIs associated. You are still being charged every month.

What is the charge probably for?

A.

AWS charges for dormant accounts.

B.
You have Elastic IPs associated with those instances.

C.
There is a "stopped instance" fee that AWS charges every month.

D.
You are being charged for the EBS volumes.

Answer: B
Explanation:

You have Elastic IPs associated with those instances. AWS charges for any unused Elastic IPs in your account.

QUESTION NO: 149

You need to quickly view inbound traffic to an instance to determine why it isn't reaching the instance properly. What is the best tool for this?

A.
Wireshark

B.
CloudWatch

C.
CloudTrail

D.
Flow Logs

Answer: D
Explanation:

CloudWatch only shows the amount of data in. Wireshark cannot see anything inside AWS infrastructure. You can only use it to view instance traffic.

QUESTION NO: 150

Your company has just completed a transition to IPv6 and has deployed a website on a server. You were able to download software on the instance without an issue. This website is deployed using IPv6, but the public is not able to access it. What should you do to fix this problem?

A.
Add an internet gateway for the instance.

B.
Add an egress-only internet gateway.

C.
Add an inbound rule to your security group that allows inbound traffic on port 80 for ::/0.

D.
Add an inbound rule to your security group that allows inbound traffic on port 80 for 0.0.0.0/0.

Answer: C

Explanation:

Your instance can reach the internet if it was able to download sofftware, so an IGW is not needed. 0.0.0.0/0 is for IPv4.

QUESTION NO: 151

Your company has two DX locations. You need to configure one link as passive. What should you configure in your router to set that link as the passive link.

A.
Set a higher MED.

B.
Configure AS_PATH Prepending on the link.

C.
Advertise a network with a higher CIDR.

D.
Call your service provider and have the ASN changed for that link.

Answer: B

Explanation:

You should configure AS_PATH prepending on the link. A higher CIDR is the same as a more specific prefix, which will make the link more preferred. A higher MED will make the path less preferred, but this is not the preferred method to accomplish this. Changing your ASN will not help. Configuring AS_PATH Prepending is the preferred method of AWS to configure an Active-Passive configuration with Direct Connect.

QUESTION NO: 152

You have just configured an Elastic Load Balancer. Assuming all settings are configured properly, about how long will it take an instance to become healthy with a 6 second HealthCheck Interval, an unhealthy threshold of 5 and a healthy threshold of 10?

A.
120 seconds

B.
30 seconds

C.
6 seconds

D.
60 seconds

Answer: D
Explanation:

60 seconds. 10 healthcheck successes with 6 second intervals.

QUESTION NO: 153

Your company needs to directly update an S3 bucket that serves as a CloudFront origin with the most reliability possible. Your company also has a set of private EC2 servers that it needs to access with the same reliability. Which combination will provide the best solution?

A.
A Virtual Gateway and a Public VIF

B.
A Private VIF is all you need to access all AWS resources.

C.
A Hosted VIF and a Private VIF

D.
A Public VIF and a Private VIF

Answer: D
Explanation:

The Public VIF will allow access to the S3 bucket, and the Private VIF will allow access to the EC2 instances.

QUESTION NO: 154

You wish to have a sub-1G connection to AWS to save on costs. How can you achieve this?

A.
Just set your router to the speed you want and AWS will charge you based on the actual speed of the port.

B.
Contact AWS, they will put you in contact with a technical account manager who can help you get this setup.

C.
You can't. The only speeds available for Direct Connect are 1G and 10G.

D.
Contact an AWS partner, AWS does not provide sub-1G connection speeds.

Answer: D
Explanation:

Sub-1G service is only available through AWS partners.

QUESTION NO: 155

You have just peered two VPCs, and you need to improve performance for instances you plan on deploying. What are two steps you would take to do this? (Choose two.)

A.
Create two subnets in the same AZ and create a placement group.

B.
Set the MTU of your instances to 1500.

C.
Create two subnets in different AZs and create a placement group.

D.
Ensure you choose instances that use enhanced networking.

Answer: A,D
Explanation:

A placement group can only be deployed in the same AZ and is only useful with enhanced networking instances.

QUESTION NO: 156

You have just deployed a website that utilizes CloudFront, ELB, and S3 to serve content. When users access your site, they are seeing broken image links. What is most likely the problem?

A.
There is no record in Route 53 pointing cdn.yourdomain.com to the CloudFront ALIAS.

B.
You need to create Origin Access Identity for CloudFront and add it to your bucket policy.

C.
The images in S3 are saved as .png instead of .jpg.

D.
There is no rule in your bucket policy allowing public access.

Answer: B
Explanation:

You must have an OAI if the bucket policy does not allow public access, which is bad practice.

QUESTION NO: 157

You have a static VPN connecting your data center and your VPC. You currently have 50 routes added to your route table. You want to add more; how should you do this?

A.
50 is the most you can have for any connection.

B.
Just add them, you have a maximum of 100 static routes per route table.

C.
Set up Direct Connect. A VPN will not support more routes.

D.
Convert your VPN to a dynamic VPN and use BGP.

Answer: D
Explanation:

A dynamic routing table can support 100 routes. A static can only support 50 per IPv4 and 50 per IPv6. Direct Connect will work, but it would be more than you needed.

QUESTION NO: 158

Your company needs an inexpensive solution to host their AD data in the cloud. They do not need all of the features of AD but do need to be able to use it with WorkSpaces. What is the best solution?

A.
AD Connector

B.
Hosted Microsoft AD

C.
Simple AD

D.
Deploy an AD server on an M3.large instance

Answer: C

Explanation:

Simple AD is the best choice here. If authentication is all you need, it is the most inexpensive option for in-cloud directory.

QUESTION NO: 159

You need to find the MTU used by another instance, but tracepath is not working. You know the instance you are trying to tracepath has open security group and NACL rules. Which protocol do you need to allow to access your instance to remedy this?

A.
Protocol 6: TCP

B.
Protocol 47: GRE

C.
Protocol 17: UDP

D.
Protocol 1: ICMP

Answer: D

Explanation:

You need to allow Protocol 1, ICMP, to access your instance. tracepath specifically needs the "destination unreachable" feature of ICMP.

QUESTION NO: 160

You are under a DDoS attack and you have added a deny all TCP rule to your NACL, but traffic is still coming. What did you do wrong?

A.
You configured the rule number to be too low.

B.

A NACL can't protect against a DDoS.

C.
The DDoS isn't a TCP attack.

D.
You need to add a deny rule outbound also since NACLs are stateful.

Answer: C
Explanation:

The DDoS isn't a TCP attack (this time.) A DDoS can use several different protocols. NACLs are stateless. The lower the rule number, the higher the priority.

QUESTION NO: 161

When configuring Active/Passive HA on VPN tunnels, choose the two best ways to configure this. (Choose two.)

A.
Keep both tunnels up.

B.
Configure AS_PATH prepending on one of the paths.

C.
Turn off one of the paths until you need it.

D.
Configure MED on one of the tunnels.

Answer: A,B
Explanation:

AWS prefers AS_PATH prepending and for a tunnel to provide true failover, it must always be on.

QUESTION NO: 162

Your company is working on a transition from IPv4 to IPv6 but is concerned about the security of having public IPv6 addresses attached to instances in a public network. They currently use a NAT to allow outbound traffic for instances. Outbound traffic is required for updates. What are two options to alleviate your company's concerns? (Choose two.)

A.
Remove any rules allowing ::/0 inbound in the security group.

B.
Block ::/0 inbound in the NACL.

C.
Create an egress-only internet gateway.

D.
Block 0.0.0.0/0 inbound in the NACL.

Answer: A,C
Explanation:

0.0.0.0/0 will only block IPv4, blocking ::/0 in the NACL will prevent return traffic and updates to the instances. An egress-only internet gateway or blocking ::/0 inbound in the security group will allow the instances to initiate outbound connections and receive the return traffic, while still preventing outside attackers from initiating connections to the instances.

QUESTION NO: 163

You have two placement groups in a VPC. What communication speed can be expected between the two placement groups?

A.
5Gbps

B.
10Gbps

C.
20Gbps

D.
You cannot communicate between two placement groups.

Answer: A

Explanation:

5Gbps is the maximum speed for traffic outside of a placement group.

QUESTION NO: 164

You have two Direct Connect connections and two VPN connections to your network. Site A is VPN 10.1.0.0/24 AS 65000 65000, Site B is VPN 10.1.0.252/30 AS 65000, Site C is DX 10.0.0.0/8 AS 65000 and Site D is DX 10.0.0.0/16 AS 65000 65000 65000. Which site will AWS choose to reach your network?

A.
Site A: VPN 10.0.1.0/24 AS 65000 65000

B.
Site B: VPN 10.0.1.252/30 AS 65000 65000 65000

C.
Site C: DX 10.0.0.0/8 AS 65000

D.
Site D: DX 10.0.0.0/16

Answer: B
Explanation:

Site B, the most specific prefix always wins.

QUESTION NO: 165

You manage a website that uses a load balancer. You are noticing one of the servers is receiving more traffic than the other. What is probably the cause of this?

A.
An Elastic Load Balancer sends traffic based on server load. One server must be a larger instance.

B.
You have DNS latency routing set, so it is diverting traffic to a different instance.

C.
You have sticky sessions configured and there are several power users that happen to be on the other server.

D.
The server has more connections available.

Answer: C
Explanation:

Sticky sessions can keep users on a particular server throughout their session. Latency routing would route to the load balancer, not the instances. Load balancers use a round-robin algorithm to balance.

QUESTION NO: 166

Your website is under attack and a malicious party is stealing large amounts of data. You have default NACL rules. Stopping the attack is the ONLY priority in this case. Which two commands should you use? (Choose two.)

A.
aws ec2 delete-network-acl-entry -network-acl-id acl-5fb84d47 -ingress -rule-number 32768

B.
aws ec2 delete-network-acl-entry -network-acl-id acl-5fb84d47 -egress rule-number 100

C.
aws ec2 delete-network-acl-entry -network-acl-id acl-5fb84d47 -ingress rule-number 100

D.
aws ec2 create-network-acl-entry -network-acl-id acl-5fb84d47 -ingress rule-number 100 -protocol -1 -port-range From =-1,To =-1 -cidr-block 0.0.0.0/0 -rule-action deny

Answer: B,C
Explanation:

You should remove the default allow rules in your NACL and a default deny will be the only rule left for inbound and outbound. If you attempt to create a rule number 100, it will encounter an error as there is already a rule 100.

QUESTION NO: 167

You are a holdings company that buys many businesses and must integrate their VPCs into your network. You are constantly encountering networks with similar or overlapping subnets.

What is the best way to manage this.

A.
BFD

B.
VRF

C.
A standby router for the overlapping subnets.

D.
A strict IP addressing policy that forces new companies to change the IP addresses of their VPCs.

Answer: B

Explanation:

VRF, or Virtual Routing and Forwarding will allow you to have multiple routing tables on your router.

QUESTION NO: 168

Your company has a high-availability hybrid solution that utilizes a two Direct Connect connections and a backup VPN connection. For some reason, traffic is preferring the VPN connection instead of the direct connection. You have prepended a longer AS_PATH on the VPN connection, but AWS still prefers it over the Direct Connect connections.

What might you be able to do to fix this issue?

A.
Advertise a less specific prefix on the VPN.

B.
Remove the prepended AS_PATH.

C.
Reconfigure the VPN as a static VPN instead of dynamic.

D.
Increase the MED on the VPN.

Answer: A
Explanation:

The only reason a VPN would be preferred over Direct Connect is if it has a more specific prefix. This was not discussed in the question but is assumed since it is the only criteria in the path selection process that supersedes Direct Connect.

QUESTION NO: 169

You work for an international corporation that uses AWS. Due to regulations, you are now required to route the US and China to two different websites. You set up the records and now no other countries can access your site.

Why is this?

A.
You forgot to set a default geolocation record.

B.
You probably broke your DNS.

C.
You must have a geolocation in place for every country.

D.
Geolocation features are only available in CloudFront.

Answer: A
Explanation:

A default record is required for traffic that does not match a geolocation criteria to follow.

QUESTION NO: 170

Your company is expanding its cloud infrastructure and moving many of its flat files and static assets to S3. You currently use a VPN to access your compute infrastructure, but you require more reliability for your static files as you are offloading all of your important data to AWS. What is your best course of action while keeping costs low?

A.
Create a Direct Connect connection using a Private VIF to access both compute and S3 resources.

B.
Create an S3 endpoint and create a route to the endpoint prefix list for your VPN to allow access to your S3 resources.

C.
Create two Direct Connect connections. Each connected to a Private VIF to ensure maximum resiliency.

D.
Create a Direct Connect connection using a Public VIF and route your VPN over the DX connection to your VPN endpoint.

Answer: D

Explanation:

An S3 endpoint cannot be used with a VPN. A Private VIF cannot access S3 resources. A Public VIF with a VPN will ensure security for your compute resources and access to your S3 resources. Two DX connections are very expensive and a Private VIF still won't allow access to your S3 resources.

QUESTION NO: 171

Your company currently has a LAG to AWS with two 1Gbps connections. What is the best way to increase throughput on this LAG?

A.
Add three 1Gbps connections to the LAG.

B.
Add one 10Gbps connections to the LAG.

C.
Configure your router to use "jumbo frames" with an MTU of 9001.

D.

Add two 1Gbps connections to the LAG.

Answer: D

Explanation:

Add two 1Gbps connections to the LAG. DX does not support jumbo frames, a LAG only supports 4 connections, and adding a 10Gbps connection will be limited to the lowest speed of 1Gbps.

QUESTION NO: 172

You have 4 Direct Connect connections from your datacenter. Site A advertises 172.16.0.0/16 AS 65000, Site B advertises 172.16.0.128/25 AS 65000 65000 65000, Site C advertises 172.0.0.0/8 AS 65000 and Site D advertises 172.16.0.0/24 AS 65000. Which site will AWS choose to reach your network?

A.
Site A: 172.16.0.0/16 AS 65000

B.
Site B: 172.16.0.128/25 AS 65000 65000 65000

C.
Site C: 172.0.0.0/8 AS 65000

D.
Site D: 172.16.0.0/24 AS 65000

Answer: B

Explanation:

172.16.0.128/25 AS 65000 65000 65000. The most specific prefix is always the first choice for BGP routing. Also, AWS will not accept an advertisement of a network less than /16.

QUESTION NO: 173

You have a server that serves www, FTP, and mail. You need to access this server using www.yourname.com, ftp.yourname.com, and mail.yourname.com. You want to ensure an IP change results in the least number of other changes.

What is the best solution?

A.
Create PTR records and point the IP address of the server back to www, ftp, and mail.

B.
Create an A record pointing to the server's IP address and create CNAME records for www, ftp, and mail and point those to the A record.

C.
Create an A record for www, ftp and mail, and point it to the ALIAS of the server.

D.
Create CNAME records for www, ftp, and mail and point those to the A record already provided to the instance by AWS.

Answer: B

Explanation:

There is no ALIAS record for an EC2 instance, CNAME records pointed to the A record provided by AWS won't work because if the IP changes, the A record will change also. A PTR record is not appropriate here and cannot point to more than one record. Having three CNAME records and one A record will result in only having to change the A record if the IP changes.

QUESTION NO: 174

Your company has a DX connection and you just added a new VPC and Private VIF to which you have connected to your DX link. You copied the settings from the other VPC to ensure it's the same. Once you connected the new VIF, you began seeing problems with connectivity to both VPCs.

You checked to make sure you didn't use the same CIDR with each VPC, so what could be the problem?

A.
You used the same VLAN ID for both connections.

B.
You overloaded your DX circuit.

C.
Your MPLS provider does not allow traffic to two VPCs.

D.
You can only connect one VIF to a DX circuit.

Answer: A
Explanation:

You can only have 1 instance of any VLAN ID.

QUESTION NO: 175

You need to find the public IP address of an instance that you're logged in to. What command would you use?

A.
curl ftp://169.254.169.254/latest/meta-data/public-ipv4

B.
scp localhost/latest/meta-data/public-ipv4

C.
curl http://127.0.0.1/latest/meta-data/public-ipv4

D.
curl http://169.254.169.254/latest/meta-data/public-ipv4

Answer: D
Explanation:

curl http://169.254.169.254/latest/meta-data/public-ipv4

QUESTION NO: 176

You have a hybrid infrastructure and you have configured your own DNS server on an EC2 instance in your 10.1.3.0/24 subnet. This subnet resides on the VPC 10.1.0.0/16. You need your data center to be able to resolve Route 53 queries in your private hosted zone. What do you need to do to accomplish this?

A.

Disable the source/destination check flag for the DNS instance.

B.
Configure your DNS server to forward queries for the private hosted zone to 10.1.3.2.

C.
Configure your DNS server to forward queries for the private hosted zone to 10.1.0.2.

D.
Configure the VPC DHCP option set in the VPC to point to the EC2 DNS server.

Answer: C
Explanation:

10.1.3.2 is not the DNS server. A DHCP option set is not needed since you are resolving AWS resources from on-premises not from a VPC and those instances are already configured to look to Route 53 DNS.

QUESTION NO: 177

Your company has signed up to trial AWS WorkSpaces. You aren't sure you're going to keep it, but you want to try it out to see if it works for your organization of 112 users. You need to deploy it with as little work and up-front expense as possible while still allowing access to your Active Directory for authentication.

What two things should you do? (Choose two.)

A.
Create a VPN connection.

B.
Create an AD connector

C.
Setup AWS hosted Microsoft AD

D.
Create a Direct Connect connection to AWS.

Answer: A,B
Explanation:

A VPN connection and an AD connector will allow you to get up and running without having to migrate users, setup expensive equipment or pay for another directory service.

QUESTION NO: 178

You have two autoscaling groups in your VPC. One deploys servers that host the index of your website and another that deploys servers that host the images for your website. What three steps would you take to ensure the right servers are used for the right purpose? (Choose three.)

A.
Create a path-based routing rule to route traffic destined for "/" to target group 1 and "/*.jpg" to target group 2.

B.
Create two target groups and associate them with each autoscaling group.

C.
Configure a Classic Load Balancer

D.
Configure an Application Load Balancer

Answer: A,B,D
Explanation:

A Classic Load Balancer does not support path-based routing rules

QUESTION NO: 179

You have two VPCs that you've peered. You created a route for VPC A to get to an instance in VPC. You are unable to ping the instance. You have double checked your security groups and NACLs.

Why might this be?

A.
You forgot to add a return route.

B.

ICMP is not supported over peering connections.

C.
You have to enable Source/Destination check in the VPCs.

D.
You have to configure the peering connection to allow two way traffic.

Answer: A
Explanation:

Every route needs a return route for ICMP traffic.

QUESTION NO: 180

You want to ensure you have the absolute best transmission rates inside and outside your VPC. You are concerned about the MTU settings. What is the best way to configure your T2 instances to ensure the best compatibility?

A.
Set all MTU to 1500 as that is the best way to ensure compatibility.

B.
Leave everything as is.

C.
Configure two ENIs, one for internal traffic and one for external traffic. Configure the external ENI with an MTU of 1500 and the internal ENI with an MTU of 9001.

D.
Set all MTU to 9001 as that is the best way to ensure the best speed. The packets will be fragmented if they have to be.

Answer: C
Explanation:

By using two ENIs, you ensure the right MTU goes to the proper destination.

QUESTION NO: 181

Which of the following does not configure Amazon CloudFront cache behaviors to forward cookies to an origin for web distributions?

A.
Origin server

B.
AWS CLI

C.
Amazon EMR

D.
Amazon S3

Answer: D

Explanation:

Amazon S3 and some HTTP servers do not process cookies. Do not configure Amazon CloudFront cache behaviors to forward cookies to an origin that doesn't process cookies or you'll adversely affect cache ability and consequently performance.

Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Cookies.html

QUESTION NO: 182

You received reports from clients in another time zone that they experienced an outage of your website several hours before you arrived at work. What two AWS services could prove crucial in figuring out what happened? (Choose two.)

A.
AWS Support

B.
CloudTrail

C.
CloudWatch

D.
Flow Logs

Answer: C,D

Explanation:

CloudTrail is for finding out who made a change. This could be a reason for the outage, but you need to see the metrics first. CloudWatch and Flow Logs are the best for this.

QUESTION NO: 183

You wish to access all European regions using your Direct Connect connection. How should you accomplish this?

A.
Peer VPCs in the different regions and connect DX to one of the regions to communicate with the other.

B.
Use a DX Gateway.

C.
Find the prefix list for the other region and add it to your route table.

D.
One DX connection will connect you to all regions.

Answer: B

Explanation:

The DX Gateway will allow access to multiple regions.

QUESTION NO: 184

You are using the CLI to assign multiple IP addresses to interfaces. The operation fails. What is the most likely reason?

A.
You cannot assign IP addresses in the CLI.

B.
You can only assign 5 IP addresses at a time through the CLI.

C.
One or more of the IP addresses could not be assigned.

D.
All of the IP addresses could not be assigned.

Answer: C
Explanation:

One more of the IP addresses could not be assigned. It only takes one failed assignment for the entire operation to fail.

QUESTION NO: 185

You are a network admin of a US company called Webby Widgets that is expanding to Europe. The company has a website that serves dynamic and static content.

You have been instructed to ensure the European clients receive the least latency possible, no matter where in Europe they live, while still allowing the US clients to receive the same user experience and performance they have been accustomed to. You have also been instructed to ensure both countries use the same URL to access the site and keep costs low.

What two things should you do? (Choose two.)

A.
Deploy three VPCs; one for the US, one for the EU, and one as a central VPC that hosts an Elastic Load Balancer that will distribute traffic between the US and EU VPCs.

B.
Create two A records: eu.webbywidgets.com that points to the EU resources and us.webbywidgets.com that points to the US resources.

C.
Use the Traffic Flow policy creator to create the perfect routing policy.

D.
Create a CloudFront distribution to serve the static content from an S3 bucket.

Answer: C,D
Explanation:

The Traffic Flow policy creator costs $50/mo. per policy and Elastic Load Balancers cannot distribute traffic between VPCs.

QUESTION NO: 186

You are configuring a CloudFront distribution, and when you try to attach an SSL, you do not see your SSL listed. What is the most likely reason for this?

A.
You must configure an https record in Route 53 first.

B.
Sometimes, it won't show, and you need to retrieve the ARN for the SSL and enter it manually.

C.
You requested an SSL for the wrong region.

D.
You didn't wait 48 hours after approving the SSL.

Answer: C
Explanation:

QUESTION NO: 187

Your company has decided to use AWS WorkSpaces for its hosted desktop solution. Your company has an existing AD of about 57,000 users, and you want to minimize authentication traffic from AWS to your datacenter. Your company has a lot of personnel changes, and it is crucial that these changes are reflected reliably.

What two steps should you take? (Choose two.)

A.
Deploy Hosted AD in AWS.

B.
Deploy an AD Connector in AWS.

C.
Create a DX connection between the datacenter and AWS.

D.
Create a VPN between the datacenter AWS.

Answer: A,C
Explanation:

A VPN is not reliable enough, and an AD connector will cause too much authentication traffic.

QUESTION NO: 188

You are configuring multiple Direct Connect links for your organization and need them to be in an HA Active/Passive configuration with extreme sensitivity to outages in order to encourage very quick failover times. You also need to be able to control which link is active.

What two configuration changes should you implement? (Choose two.)

A.
MPLS

B.
BFD

C.
AS_PATH Prepending

D.
BGP

Answer: B,C
Explanation:

Bidirectional-Forwarding Detection will allow for faster failover times. AS_PATH Prepending will allow you to choose the default path. BGP is already implemented and MPLS does not matter.

QUESTION NO: 189

What number does the binary number 10101000 correspond to?

A.
168

B.
128

C.
192

D.
160

Answer: A
Explanation:

128 + 0 + 32 + 0 + 8 + 0 + 0 + 0 = 168

QUESTION NO: 190

What number does the binary number 11000000 correspond to?

A.
128

B.
192

C.
64

D.
117

Answer: B
Explanation:

128 + 64 + 0 + 0 + 0 + 0 + 0 + 0 = 192

QUESTION NO: 191

What value in a packet dictates the priority of the packet in a QoS enabled network?

A.
BFD

B.
IPv6

C.
NAT

D.
DSCP

Answer: D
Explanation:

The Differentiated Services Code Point value, or DSCP, is used to label packets on QoS enabled networks for prioritization.

QUESTION NO: 192

What is the IPv6 subnet CIDR used by a VPC?

A.
/128

B.
/56

C.
/48

D.
/16

Answer: B
Explanation:

A VPC will always use /56 as its CIDR

QUESTION NO: 193

What is the name of the label applied to packets to allow routers to know where to forward in an MPLS network?

A.
BFD

B.
BGP

C.
FEC

D.
ABC

Answer: C
Explanation:

Forward Equivalency Class is how routers know where to send packets.

QUESTION NO: 194

What port and protocol is used by DNS?

A.
80/TCP

B.
22/TCP

C.
80/TCP and UDP

D.
53/TCP and UDP

Answer: D
Explanation:

DNS uses port 53 and either TCP or UDP depending on what type of DNS message is being sent.

QUESTION NO: 195

Which port range must be allowed through a NACL to ensure all return traffic is successful?

A.
1024 65,535

B.
22

C.
65,000 65,535

D.
80 443

Answer: A
Explanation:

1024 65,535 is the full "ephemeral port" range.

QUESTION NO: 196

To allow all traffic to access an instance in "Subnet 1" that uses "Security Group 1", what two options need to be configured? (Choose two.)

A.
NACL rule allowing 0.0.0.0/0 to access "Subnet 1"

B.
Security Group rule in "Security Group 1" that allows 0.0.0.0/0 inbound

C.
Security Group rule in "Security Group 1" that allows outbound traffic to 0.0.0.0/0

D.
NACL rule allowing 0.0.0.0/0 to access "Security Group 1"

Answer: A,B

Explanation:

You must allow traffic through the NACL and through the Security Group to access the instance. If there is not an Outbound allow setup in the NACL, you may need to set that, but an outbound rule for Security Group 1 is not necessary as security groups are stateful.

QUESTION NO: 197

You have created a custom VPC. What are two things you may need to do in order to SSH directly into your instance? (Choose two.)

A.
Enable SSH on the instance

B.
Attach a NAT Gateway

C.
Enable Public IP addresses

D.
Attach an Internet Gateway

Answer: C,D

Explanation:

Public IP addresses are not enabled by default in a custom VPC. An Internet Gateway is also required.

QUESTION NO: 198

Which of these addresses cannot be given to an EC2 instance in your VPC?

A.
10.0.0.157

B.
10.0.0.3

C.
10.0.0.4

D.
10.0.0.253

Answer: B
Explanation:

10.0.0.3 is reserved by AWS for future use.

QUESTION NO: 199

Which ports must you allow for HTTP and HTTPS traffic?

A.
25/465

B.
21/22

C.
3389/3306

D.
80/443

Answer: D
Explanation:

80 and 443 are the ports for HTTP and HTTPS, respectively.

QUESTION NO: 200

If you have one VPC peered with two VPCs with overlapping CIDRs, which route will be more preferred?

A.

10.1.0.0/16

B.
10.0.0.0/8

C.
10.1.1.5/32

D.
10.1.1.0/24

Answer: C
Explanation:

10.1.1.5/32. The most specific route is preferred.

QUESTION NO: 201

How many BGP advertised routes can you have per route table?

A.
50

B.
200

C.
100

D.
As many as you want as long as you contact AWS first.

Answer: C
Explanation:

You can only have 100 advertised routes from BGP. This cannot be changed.

QUESTION NO: 202

What MTU is recommended for VPN and Direct Connect links?

A.
1500

B.
2000

C.
128

D.
Jumbo Frames

Answer: A
Explanation:

Jumbo frames will not pass through VPN and Direct Connect links using AWS connections. You must use an MTU of 1500.

QUESTION NO: 203

Which statement about placement groups is incorrect?

A.
A placement group is a logical grouping of instances in a single AZ.

B.
If you stop an instance and restart it, it will always return to the same placement group.

C.
To help ensure capacity in a placement group, deploy all instances at once.

D.
There is no charge for creating a placement group.

Answer: B
Explanation:

There may not be sufficient capacity in the placement group.

QUESTION NO: 204

Which two statements about placement groups are correct? (Choose two.)

A.
A placement group can span multiple VPCs.

B.
A placement group can span multiple Availability Zones.

C.
You cannot merge placement groups.

D.
It is best to use the same instance types in a placement group.

Answer: A,C
Explanation:

A placement group can span multiple VPCs but may not experience the full performance benefit. The only way to add instances from one placement group to another is to create AMIs out of the instances and spin them all up into one placement group.

QUESTION NO: 205

What are two reasons to have multiple IP addresses or interfaces on one server? (Choose two.)

A.
You can host multiple SSLs

B.
Create management networks

C.
Direct Connect connections

D.
Teaming multiple NICs for more throughput

Answer: A,B
Explanation:

You cannot bind multiple interfaces for faster speeds on AWS

QUESTION NO: 206

Which statement about Elastic IP addresses is incorrect?

A.
Additional EIPs associated with one instance incur a charge.

B.
Once an EIP is associated with an instance, you must manually change the hostname if you want it to match.

C.
Once you associate an EIP with an instance, the original public IP is released.

D.
Disassociated EIPs incur a charge.

Answer: B
Explanation:

The hostname automatically changes to match the new EIP.

QUESTION NO: 207

Which of these is not specified on an ENI?

A.
A primary private IPv4 address

B.
A source/destination check flag

C.
A MAC address

D.
An A record

Answer: D

Explanation:

An A record is not specified on an ENI. This is created in Route 53.

QUESTION NO: 208

What are two reasons that could cause an HTTP health check to fail? (Choose two.)

A.
Security group blocking port 80 to the instance

B.
HTTP server not running

C.
No Internet Gateway

D.
NACL blocking port 443 to the instance

Answer: A,B

Explanation:

A load balancer does not perform health checks through the internet gateway, so it is not necessary and 443 is HTTPS not HTTP

QUESTION NO: 209

Which one of these healthcheck reason codes is not a valid reason code?

A.
Elb.InitialHealthChecking

B.
Target.UnHealthy

C.
Target.NotInUse

D.
Target.InvalidState

Answer: B
Explanation:

Target.UnHealthy does not exist.

QUESTION NO: 210

What are two features of an Application Load Balancer? (Choose two.)

A.
Scales to handle any amount of traffic without interference

B.
Can distribute traffic over multiple Availability Zones

C.
Can receive a static IP address

D.
Can support SSLs

Answer: B,D
Explanation:

The network load balancer can scale larger and receive a static IP address, but not the Application load balancer.

QUESTION NO: 211

What must be added to your web server configuration to view the true requesting IP address?

A.
X-Actual-IP

B.

X-Forwarded-Proto

C.
X-Amzn-Trace-ID

D.
X-Forwarded-For

Answer: D
Explanation:

X-Forwarded-For. X-Forwarded-Proto is to see the protocol, X-Actual-IP doesn't exist and X-Amzn-Trace-ID is for Amazon's unique identifier.

QUESTION NO: 212

What are 2 possible ALIAS records? (Choose two.)

A.
DynamoDB

B.
Elastic Beanstalk

C.
CloudFront

D.
EC2 Instance

Answer: B,C
Explanation:

You cannot create an ALIAS record that points to an EC2 instance or DynamoDB.

QUESTION NO: 213

What are two routing methods used by Route 53? (Choose two.)

A.
RIP

B.
Failover

C.
Latency

D.
AS_PATH

Answer: B,C
Explanation:

RIP is used for network routing and AS_PATH is used for BGP path manipulation.

QUESTION NO: 214

Which is not a valid Route 53 record?

A.
SPF

B.
NAPTR

C.
AAAA

D.
BFD

Answer: D
Explanation:

BFD stands for Bi-directional Forwarding Detection and has nothing to do with Route 53.

QUESTION NO: 215

What is the minimum number of subnets for an RDS subnet group?

A.
3

B.
4

C.
1

D.
2

Answer: D
Explanation:

This allows for high availability and failover in case an RDS instance goes down.

QUESTION NO: 216

What is the DNS server address for a VPC (10.111.0.0/16) with a subnet of 10.111.4.0/24?

A.
10.111.0.2

B.
10.111.4.2

C.
10.111.1.2

D.
10.111.4.1

Answer: A
Explanation:

The DNS server is the base VPC CIDR + 2.

QUESTION NO: 217

Which statement about VPC endpoints is incorrect?

A.
Endpoints are transitive for Direct Connect connections.

B.
Endpoints cannot be extended out of a VPC.

C.
Endpoints cannot be tagged.

D.
An S3 endpoint allows Amazon AMIs to install some software.

Answer: A

Explanation:

Endpoints are not transitive for Direct Connect connections or any other connections. To access S3 resources through an endpoint from outside of a VPC, an EC2 proxy must be used.

QUESTION NO: 218

Which two methods can be used to ensure items are distributed only to the correct parties? (Choose two.)

A.
Signed URLs

B.
Signed cookies

C.
Signed biscuits

D.
Signed SSLs

Answer: A,B

Explanation:

Signed cookies and signed URLs are used to ensure only intended parties can access CloudFront resources.

QUESTION NO: 219

What is NOT a benefit of CloudFront?

A.
Helps ease the strain on your web servers

B.
Distributes traffic evenly to EC2 instances

C.
Speeds up distribution of RTMP content

D.
Speeds up distribution of static and dynamic web content

Answer: B

Explanation:

Elastic Load balancers distribute traffic to EC2 instances.

QUESTION NO: 220

What two items are required for all AWS VPNs? (Choose two.)

A.
Virtual Private Gateway

B.
ASN

C.
A hardware router

D.
Customer Gateway

Answer: A,D

Explanation:

An ASN is only required for dynamic VPNs and hardware routers are not required.

QUESTION NO: 221

What are two ways to influence the direction of Dynamic VPN traffic over multiple links? (Choose two.)

A.
AS_PATH Prepending

B.
BFD

C.
MED

D.
Shouting at it

Answer: A,C

Explanation:

BFD detects failed links but does not create them. Shouting at it just isn't nice.

QUESTION NO: 222

Which of these is not a requirement to set up a DX connection?

A.
Support for 802.1q VLANs

B.
BGP MD5 Authentication

C.
Autonegotiation enabled

D.
Single mode fiber capability

Answer: C
Explanation:

Autonegotiation must be disabled.

QUESTION NO: 223

Which of these is not required when setting up a VIF?

A.
BGP Key

B.
VLAN ID

C.
ASN

D.
BGP MED

Answer: D
Explanation:

BGP MED is used to steer traffic and not for requesting a VIF.

QUESTION NO: 224

Which path will be chosen first?

A.
192.168.0.0/16 AS 65000 over Direct Connect

B.
192.0.0.0/8 AS 65000 over Direct Connect

C.
192.168.1.0/24 AS 65000 65000 65000 over a Dynamic VPN

D.
192.168.0.0/16 AS 65000 over a Static VPN

Answer: C
Explanation:

The path selection process always chooses the most specific prefix first.

QUESTION NO: 225

What statement about LAGs is incorrect?

A.
If you create a new connection, you will have to fill out another LOA-CFA.

B.
You can pool connections with multiple speeds to create one faster speed.

C.
You will receive 1 LOA-CFA with a page for each connection.

D.
All connections in the LAG must terminate at the same DX endpoint.

Answer: B
Explanation:

All links must be the same speed for a LAG to be operational.

QUESTION NO: 226

Which one of the following options is not true about WorkSpaces?

A.
WorkSpaces allows integration with Microsoft AD.

B.
WorkSpaces is great for running Linux applications.

C.
WorkSpaces is a fully managed, secure desktop computing service.

D.
WorkSpaces can query on-premises domains for authentication.

Answer: D
Explanation:

QUESTION NO: 227

Which two choices can serve as a directory service for WorkSpaces? (Choose two.)

A.
Simple AD

B.
Enhanced AD

C.
Direct Connection

D.
AWS Microsoft AD

Answer: A,D
Explanation:

There is no such thing as "Enhanced AD" and DX is not a directory service.

QUESTION NO: 228

Which of these modes is not a configuration mode for a WAF?

A.
Block

B.
Allow

C.
Sleep

D.
Monitor

Answer: C
Explanation:

There is no sleep mode for a WAF. WAFs are hard workers.

QUESTION NO: 229

Which of these metrics cannot help detect a DDoS?

A.
EC2 CPUUtilization

B.
ELB SurgeQueueLength

C.
EMR EMRspersecond

D.
CloudFront Requests

Answer: C
Explanation:

EMR EMRspersecond doesn't exist.

QUESTION NO: 230

Which service would you use to see who changed your infrastructure?

A.
Config

B.
CloudTrail

C.
Flow Logs

Answer: B

Explanation:

QUESTION NO: 231

Which service would you use to see CPU usage?

A.
CloudTrail

B.
Config

C.
CloudWatch

D.
None of the above

Answer: C

Explanation:

QUESTION NO: 232

Your on-premises network has an IP address range of 11.11.0.0/16. Only IPs within this network range can be used for inter-server communication. The IP address range 11.11.253.0/24 has been allocated for the cloud.

You need to design a VPC in AWS. The servers within the VPC should be able to communicate with hosts both on the Internet and on-premises through a VPN connection.

What combination of configuration steps meets your needs? (Choose two)

A.
Set up the VPC with an IP address range of 11.11.253.0/24.

B.
Set up the VPC with an RFC 1918 private IP address range (e.g., 10.10.10.0/24), and set up a NAT gateway to do translation between 10.10.10.0/24 and 11.11.253.0/24 for all outbound traffic.

C.
Set up a VPN connection between a VGW and an on-premises router, set the VGW as the default gateway for all traffic, and configure the on-premises router to forward traffic to the Internet.

D.
Set up a VPN connection between a VGW and an on-premises router, set the VGW as the default gateway for traffic destined to 11.11.0.0/24, and add a VPC subnet route to point the default gateway to an Internet gateway for Internet traffic.

E.
Set up the VPC with an RFC 1918 private IP address range (e.g., 10.10.10.0/24), and set the VGW to do a source IP translation of all outbound packets to 11.11.0.0/16.

Answer: A,C

Explanation:

The VPC needs to use a CIDR block in the assigned range (and be non-overlapping with the data center). All traffic not destined for the VPC is routed to the VGW (that route is assumed) and must then be forwarded to the Internet when it arrives on-premises. B and E are wrong because they are not in the assigned range (you can use non-RFC 1918 addresses in a VPC). D is wrong because it directs traffic to the Internet through the Internet gateway.

QUESTION NO: 233

You are architecting an HPC solution in AWS. The system consists of a cluster of EC2 instances that require low-latency communications between them.

Which method should you use to set up a cluster to meet these requirements?

A.
Create a VPC with one subnet in a single Availability Zone. Keep the size of the subnet equal to the number of instances required in the cluster. Launch instances for the cluster in this small subnet to guarantee low-latency network performance.

B.
Create a placement group. Choose an EC2 instance type compatible with placement groups for the cluster. Launch instances for the cluster in the placement group.

C.
Launch Amazon EC2 instances with the largest available number of cores and RAM. Attach all instances to an Amazon EBS PIOPS volume. Implement a shared memory system across all instances in the cluster, using this shared EBS volume to minimize latency of communication.

D.
Choose an EC2 instance type that offers enhanced networking. Attach a 10-Gbps non-blocking elastic network interface to the instances. Configure the elastic network interface to optimize network performance to reduce latency.

Answer: B

Explanation:

Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. A is incorrect because the size of a subnet has no impact on network performance. C is incorrect because an EBS volume cannot be shared between EC2 instances. D is only half the solution because the enhanced networking affects the network behavior of an EC2 instance but not the network infrastructure between instances.

QUESTION NO: 234

Your customer's internal security teams receive requests to allow Amazon S3 access from inside the corporate network. All external traffic must be explicitly whitelisted through your corporate firewalls.

How can your security team grant this access?

A.
Obtain the list of IP prefixes from AWS Forum announcements, and use those prefixes in firewall rules.

B.
Obtain the list of IP prefixes from ip-ranges.json, and use those prefixes in firewall rules.

C.
Obtain the list of IP prefixes by performing a DNS lookup on Amazon S3 endpoints, and use those prefixes in firewall rules.

D.

Connect your data center to a VPC via Direct Connect. Create routes that forward traffic from your data center to an S3 private endpoint.

Answer: B

Explanation:

ip-ranges.json contains the latest list of IP addresses used by AWS. AWS no longer posts IP prefixes in Forum announcements. DNS lookups would not provide an exhaustive list of possible IP prefixes. D would require transitive routing, which is not possible.

QUESTION NO: 235

Your application server instances reside in the private subnet of your VPC. These instances need to access a Git repository on the Internet. You create a NAT gateway in the public subnet of your VPC. The NAT gateway can reach the Git repository, but instances in the private subnet cannot. You confirm that a default route in the private subnet route table points to the NAT gateway. The security group for your application server instances permits all traffic to the NAT gateway.

What configuration change should you make to ensure that these instances can reach the patch server?

A.
Assign public IP addresses to the instances and route 0.0.0.0/0 to the Internet gateway.

B.
Configure an outbound rule on the application server instance security group for the Git repository.

C.
Configure inbound network access control lists (network ACLs) to allow traffic from the Git repository to the public subnet.

D.
Configure an inbound rule on the application server instance security group for the Git repository.

Answer: B

Explanation:

The traffic leaves the instance destined for the Git repository; at this point, the security group must allow it through. The route then directs that traffic (based on the IP) to the NAT gateway. A is wrong because it removes the private aspect of the subnet and would have no effect on the blocked traffic anyway. C is wrong because the problem is that outgoing traffic is not getting to the NAT gateway. D is wrong because to allow outgoing traffic to the Git repository requires an outgoing security group rule.

QUESTION NO: 236

Considering your knowledge of both the OSI and TCP/IP models – select the following statement which you consider to NOT be true.

A.
The TCP/IP Application layer maps to 2 of the OSI Layers

B.
The top layer in the OSI model is named the Application layer

C.
The TCP/IP Application layer maps to 3 of the OSI Layers

D.
The top layer in the TCP/IP model is named the Application layer

Answer: A
Explanation:

The OSI model is a 7 layered model. The TCP/IP model is a 4 layered model. The top layer in both models is called the Application layer. The TCP/IP Application layer maps to the top 3 OSI layers (Application, Presentation, and Session layers).

Reference: https://en.wikipedia.org/wiki/OSI_model

QUESTION NO: 237

From the following options, select the answer that correctly describes the implementation of the HTTP protocol

A.
By definition, HTTP is a connection-less oriented protocol and therefore utilises TCP

B.
By definition, HTTP is a connection orientated protocol and therefore utilises TCP

C.
By definition, HTTP is a connection-less oriented protocol and therefore utilises UDP

D.
By definition, HTTP can be configured to be either connection or connection-less oriented – by specifying the appropriate HTTP header.

Answer: B
Explanation:

HTTP is a connection orientated protocol and therefore utilizes TCP

Reference: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

QUESTION NO: 238

You have just provisioned a new VPC a with a CIDR block of 172.16.12.0/24. The entire CIDR block is fully utilized by subdividing it into 6 subnets, we will refer to these as Subnet1 through to Subnet6. The first 2 subnets (Subnet1 and Subnet2) are the same size. The last 4 subnets (Subnet3, Subnet4, Subnet5, Subnet6) are also the same size. Subnet5 is half the size of Subnet2. The address space as occupied by the first two subnets is contiguous, as is the address space occupied by the last 4 subnets. Within Subnet3 AWS reserves the address 172.16.12.129 for the VPC router.

Select the correct IP address reserved by AWS for DNS in the Subnet2.

A.
172.16.64.1

B.
172.16.64.65

C.
172.16.12.66

D.
172.16.12.64

Answer: C
Explanation:

From the documentation above – we know AWS reserves the address x.x.x.1 for the VPC router, and x.x.x.2 for DNS from within each subnet. This question states that Subnet 3 reserves 172.16.12.130 for the VPC router. Given that we now know that the Subnet 3 (the 1st of the last 4 Subnets) starts at 172.16.12.128 - then it must follow that Subnet2 ends at 172.16.12.127. From here we know we have 128 addresses that are halved evenly between Subnet1 and Subnet2 - 128/2 = 64 or /26 in CIDR form. Therefore it follows that the address reserved by AWS for DNS in the Subnet2 must be 172.16.12.66

Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html

QUESTION NO: 239

Select the VPC Peering statement below that is NOT true

A.
VPC peering supports transitive peering relationships for IPv6 traffic but not IPv4

B.
VPC peering can be performed between VPCs in different AWS accounts in the same region

C.
TCP connections can be performed between peered VPCs

D.
UDP connections can be performed between peered VPCs

Answer: A
Explanation:

VPC peering supports transitive peering relationships for IPv4 and IPv6 traffic

Reference: http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/vpc-peering-basics.html#vpc-peering-limitations

QUESTION NO: 240

Select the answer/s that correctly state how Jumbo Frames work

A.
Jumbo Frames assist with application disk storage

B.
Jumbo Frames can assist with application performance

C.
Jumbo Frames are supported across Virtual Private Gateway connections

D.
Jumbo Frames are enabled by increasing the MTU size to 9000 kilobytes

Answer: B

Explanation:

We know by definition that Jumbo Frames support 9000 byte MTU – therefore Answer A is incorrect (the stated unit is kilobytes). Jumbo Frames is a data transmission unit configuration option - it does not change or alter anything related to security – therefore Answer B is incorrect. Answer C is correct - we can get improved application performance when used within appropriate scenarios. Jumbo Frames are not supported over VPG IPsec VPN connections - therefore Answer D is incorrect. Answer E is nonsensical – Jumbo Frames is a networking construct and has nothing to do with disk storage.

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html

QUESTION NO: 241

You are the AWS cloud architect and have been tasked with designing an appropriate subnetting design for your production VPC. Your production VPC requires secure communications back to the corporate private network. Quality of Service (QoS) is very important 24 × 7 for this particular connection, as real-time data is passed continually backwards and forwards between your on-prem bioinformatics enterprise application, and the number crunching servers deployed in the cloud. Any potential latency incurred on this connection will have a direct impact on the company's ability to attract investors and expansion into new markets.

Select the correct network configuration that best facilitates your company's continued growth plans.

A.
Provision a Direct Connect connection - between your service provider's data center and the AWS region that your cloud compute resources exist in. Configure just a Private Virtual Interface. As this is a Direct Connection, a Virtual Private Gateway is not required

B.
Configure a site-to-site layer 2 software router using OpenVPN within your VPC and ensure that QoS enabled - this is a secure and cheap option

C.
Configure a site-to-site layer 3 software router using OpenVPN within your VPC and ensure that QoS enabled - this is a secure and cheap option

D.
Provision a Direct Connect connection – between your existing service provider's data center and the AWS region that your cloud compute resources exist in. Configure a Virtual Private Gateway and Private Virtual Interface

Answer: D

Explanation:

Answers A, B, and C all rely on an Internet connection. An Internet connection cannot guarantee QoS and will be subject to performance fluctuations - therefore they are all incorrect options. The only difference between these options is whether a Virtual Private Gateway is required – the answer is yes and therefore the correct answer is D.

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

QUESTION NO: 242

You are your company's AWS cloud architect. You have created a VPC topology that consists of 3 VPCs. You have a centralised VPC (VPC-Shared) that provides shared services to the remaining 2 departmental dedicated VPCs (VPC-Dept1 and VPC-Dept2). The centralised VPC is VPC peered to both of the departmental VPCs, that is a VPC peering connection exists between VPC-Shared and VPC-Dept1, and a VPC peering connection exists between VPC-Shared and VPC-Dept2.

Select the correct option from the list below.

A.
Network traffic is possible between VPC-Shared instances and VPC-Dept1 and VPC-Dept2 instances as long as the appropriate routes and security groups are in place, but only for communication that is initiated from VPC1-Shared instances as the default peering bi-directional communication flag has been disabled.

B.
Instances within VPC-Dept1 can communicate directly with instances in VPC-Shared, as long as

the appropriate routes and security groups are in place, and vice versa regardless of who initiates communication

C.
All network communication remains blocked between all VPCs until the respective peering bi-directional communication flags are set to the appropriate setting that allows traffic to flow.

D.
Network traffic is possible between VPC-Shared instances and VPC-Dept1 and VPC-Dept2 instances as long as the appropriate routes and security groups are in place, but only for communication that is initiated from VPC1-Shared instances as the default peering bi-directional communication flag has been enabled.

Answer: B
Explanation:

Answers A, C and D are incorrect answers as they reference a non-existing setting - there is no such thing as a "default peering bi-directional communication flag".

Reference: http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-partial-access.html#one-to-two-vpcs-instances

QUESTION NO: 243

In your current role as the corporate network architect – you have decided to replace your existing hardware firewall appliances with a pair of Juniper SRX-Series Services Gateways. You have chosen these as AWS lists these as supportable devices for establishing IPsec connections. With this in mind, select the minimum set of options to ensure that you can establish IPsec connectivity between your on premise private corporate network and your AWS hosted VPC.

Select which option is NOT required.

A.
Initiate network connections from somewhere within your corporate network, this is required to bring the tunnels UP

B.
Deploy a Customer Gateway within your corporate network

C.
Deploy a Customer Gateway within your VPC

D.

Deploy a Virtual Private Gateway within your VPC

Answer: B

Explanation:

A customer gateway within the corporate network is NOT required. The Customer Gateway (CGW) is a component that you deploy within your VPC that logically represents you VPN physical hardware's perimeter public IP - therefore Answer C is required. A Virtual Private Gateway (VPG) is the AWS VPN Concentrator end point – and is always a requirement that needs to be deployed in your VPC - therefore it must always be deployed – therefore Answer D is required.

AWS only supports IPsec in Tunnel mode – therefore Answer A is required.

Reference: https://aws.amazon.com/vpc/faqs/

QUESTION NO: 244

You need to create a baseline of normal traffic flow in order to implement some security changes to your organization.

What two items would be best to use? (Choose two.)

A.
Wireshark

B.
CloudTrail

C.
An IDS

D.
CloudWatch

Answer: A,D

Explanation:

QUESTION NO: 245

Your company has just deployed IPv6 in a VPC. All of the instances currently use a NAT, but once they configured the instances for IPv6 only, they were unable to access the resources on the instances via IPv6. What is the best option to fix this?

A.
Configure the NAT for IPv6.

B.
Configure an egress-only internet gateway.

C.
Add a route for ::/0 to the NAT.

D.
Add an internet gateway.

Answer: B

Explanation:

NAT is not compatible with IPv6 and an IGW would allow full access to the instances, which is not good. An egress-only IGW is the best solution.

QUESTION NO: 246

Your company just acquired a new company. You have two VPCs ?one is 172.31.0.0/16 and one is 10.111.0.0/16. The acquired company uses 10.111.0.0/16 for their VPC. Your VPC "A" has a group of 12 servers in the range 10.111.2.101 ?10.111.2.112. Their VPC "B" has 20 servers from 10.111.2.171 ?10.111.2.190. You need to access both VPCs from the 172.31.0.0/16 VPC "C".

What is the best way to approach this problem?

A.
From VPC C, create a peering connection and add a route to VPC A's peering connection for 10.111.2.96/27 and a route to VPC B's peering connection for 10.111.2.0/24.

B.
From VPC C, create a peering connection and add a route to VPC A's peering connection for 10.111.2.96/28 and a route to VPC B's peering connection for 10.111.2.0/24.

C.
From VPC C, create a peering connection and adjust the route tables to direct traffic to the individual servers by exact IP address of the servers.

D.
Invest the money and change the CIDR of one of the VPCs since one VPC cannot be peered to two VPCs with the same CIDR block.

Answer: A

Explanation:

You can peer VPCs with the same CIDR block to a third VPC, so changing the CIDR block is not necessary. You can adjust the route tables to point to individual servers, but this would be very inefficient. 10.111.2.96/28 does not provide enough addresses for the AWS required addresses. AWS reserves 5 addresses per subnet and this only allows 11 addresses. 10.111.2.96/27 provides 32 addresses with 27 usable. Since it is a /27, it will take precedence over the /24 and route the traffic destined for these instances correctly.

QUESTION NO: 247

Due to security requirements, all traffic must be encrypted between your VPC and your on-premises data center. You also want to maintain reliability.

What two options will allow you to achieve this? (Choose two.)

A.
A Direct Connect connection with a Private VIF

B.
A VPN connection

C.
A Direct Connect connection with a Hosted VIF

D.
A Direct Connect connection with a Public VIF

Answer: B,D

Explanation:

To run VPN over DX, you need to have a public VIF to access the VPN endpoints.

QUESTION NO: 248

You have deployed a website that utilizes CloudFront, Elastic Loadbalancer, and S3 to serve content. When users access your site, they receive a "mixed content" security warning.

What is most likely the problem?

A.
There is no rule in your bucket policy allowing public access.

B.
You have applied your SSL to your Elastic Loadbalancer but not your CDN.

C.
Your S3 Bucket permissions are incorrect.

D.
You are using an SSL from an external CA.

Answer: B

Explanation:

You must apply the SSL to your Elastic Loadblanacer and your CDN to encrypt all aspects of your site.

QUESTION NO: 249

You are a network engineer at a company that just purchased a DX connection. You ensured your equipment met all of the technical requirements, you have verified with your AWS account manager and your colocation provider that everything is connected, and all of your information is correct. For some reason, the link does not operate correctly.

What could be the problem?

A.
The CAT6 cable is frayed.

B.
Autonegotiation is enabled.

C.
You are using 802.1q VLANs instead of 802.1w.

D.
BFD is disabled.

Answer: B
Explanation:

Autonegotiation is enabled. A DX connection uses single-mode fiber, not CAT6; BFD is optional, and 802.1q is the correct standard. Autonegotiation must be disabled for DX to work properly.

QUESTION NO: 250

You have configured a dynamic VPN between your datacenter and your VPC. Your router says the tunnel is up and BGP is active, but for some reason, you are not seeing your routes propagate.

What is most likely the issue?

A.
You need to configure the firewall for BGP.

B.
Your router does not support BFD.

C.
You need to obtain a new BGP MD5 key.

D.
You forgot to set route propagation to "yes" in the route table.

Answer: D
Explanation:

You forgot to set route propagation to "yes" in the route table. If the route table says BGP is active and the tunnel is up, then you do not have a firewall issue. BFD has nothing to do with route propagation. You do not need a BGP MD5 key for VPN.

QUESTION NO: 251

Your company just deployed a WAF to protect its resources. You need to create a baseline before you start blocking traffic. How will you achieve this?

A.
Set the WAF to Monitor mode.

B.
Set the WAF to its defaults and let it do its job.

C.
Setup a Lambda function to monitor Flow Logs and analyze the traffic using Elasticsearch.

D.
A WAF is default deny and does not allow this. You need to use an IDS instead.

Answer: A

Explanation:

Monitor mode is the only good choice.

QUESTION NO: 252

Your website utilizes EC2, S3, ELB-Classic, and CloudFront. Your manager has shifted focus to security and wants you to ensure the site is as secure as possible. What two items could you recommend? (Choose two.)

A.
An NACL that blocks all ports to your subnets.

B.
A restricted bucket policy.

C.
A WAF on the load balancer.

D.
A WAF on your CloudFront distribution.

Answer: B,D

Explanation:

A WAF on CloudFront and a restricted bucket policy to ensure the only access is from CloudFront. You cannot apply a WAF to a classic load balancer and an NACL that blocks all ports would block access to the load balancer.

QUESTION NO: 253

You have two public applications on different domains that use two front-end servers and two back-end servers each. You wish to achieve high availability for both applications. What two options should you configure? (Choose two.)

A.
Route 53: 2 public zones and 2 private zones.

B.
Route 53: 2 public zones and 1 private zone.

C.
3 load balancers: 2 public and 1 internal.

D.
4 load balancers: 2 public and 2 internal.

Answer: A,D
Explanation:

Route 53: 2 public zones and 2 private zones and 4 load balancers: 2 public and 2 internal. This will allow one domain to be balanced over two application servers which will then have traffic balanced to the two backend servers.

QUESTION NO: 254

Your company was recently acquired and a Direct Connection connection was extended from your new parent corporation to your AWS VPC using a hosted VIF. What data charges are billed to your account for that connection?

A.
You are only responsible for the port hours of the VIF.

B.
You are not charged anything.

C.
You are responsible for all data transfer out.

D.
You are responsible for all data transfer in.

Answer: C
Explanation:

You are only responsible for the data transfer out. The port hours are the responsibility of the owner of the connection.

QUESTION NO: 255

The IPsec protocol suite is made up of various components covering aspects such as confidentiality, encryption, and integrity.

Select the correct statement below regarding the correct configuration options for ensure IPsec confidentiality:

A.
The following protocols may be used to configure IPsec confidentiality, DES, 3DES, MD5

B.
The following protocols may be used to configure IPsec confidentiality, DES, 3DES, AES

C.
The following protocols may be used to configure IPsec confidentiality, PSK, RSA

D.
The following protocols may be used to configure IPsec confidentiality, PSK, MD5

E.
The following protocols may be used to configure IPsec confidentiality, PSK, RSA

Answer: B
Explanation:

Answer A is incorrect - as MD5 is a hashing protocol (data integrity) Answer C is incorrect - as PSK is short for Pre-Shared Keys (key exchange) - and again MD5 is a hashing protocol (data integrity)

Answer D is incorrect - as both MD5 and SHA are hashing protocols (data integrity) Answer E is incorrect - as both PSK and RSA are used for key exchanges This leaves Answer B is the only correct IPsec configuration covering confidentiality. DES, 3DES, and AES are all encryption protocols.

Reference: https://en.wikipedia.org/wiki/IPsec

QUESTION NO: 256

Which of the following statements does not describe Jumbo Frames in an AWS VPC environment?

A.
For instances that are collocated inside a placement group, jumbo frames help to achieve the maximum network throughput possible

B.
Jumbo Frames are not supported for traffic that exits the Virtual Private Gateway

C.
Jumbo Frames are not supported for traffic that exits the Internet Gateway

D.
T2.micro instances do not support Jumbo Frames

Answer: D
Explanation:

All answers except for Answer D are correct. Answer D is incorrect in that AWS does indeed support Jumbo Frames on all instance types within the T2 family class - including the T2.micro instance type.

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html

QUESTION NO: 257

Within the TCP/IP model what is the name of the Packet Data Unit (PDU) used between Transport Layers for communication between sender and receiver

A.
Frames

B.
Packets

C.
Data

D.
Segments

Answer: D
Explanation:

Segments is the PDU used between transport layers.

Reference: https://en.wikipedia.org/wiki/Transmission_Control_Protocol

QUESTION NO: 258

Considering the rules of IPv4 subnetting, how many subnets and hosts per subnet are possible given the following network 192.168.130.130/28? (in this question ignore the fact that AWS reserves 5 IP addresses)

A.
8 subnets and 30 hosts per subnet

B.
16 subnets and 14 hosts per subnet

C.
32 subnets and 30 hosts per subnet

D.
8 subnets and 14 hosts per subnet

Answer: B
Explanation:

16 subnets and 14 hosts per subnet are possible in the CIDR.

Reference: https://en.wikipedia.org/wiki/IPv4_subnetting_reference

QUESTION NO: 259

An unfortunate situation has just come to your attention. A business critical application with sensitive data running on-prem will run out of storage disk space in 24hrs. This business critical application is dependent a very large set of routes – required for integration with other system. You make a quick but well informed decision to migrate this application quickly to AWS. You are able to quickly launch a new VPC and within it equivalent infrastructure to re–home the application. In order to complete the replication of application data and ensure the application remains operational beyond the next 24hrs, select the best implementation.

A.
Within the new VPC – establish a Direct Connect connection with max 10Gbps port speed for data replication. Establish a 802.1Q VLAN and configure a Virtual Private Gateway and Private Virtual Interface, and ensure Jumbo Frames is enabled.

B.
Within the new VPC – deploy a Virtual Private Gateway, Customer Gateway, and establish a new IPsec VPN Connection with BGP dynamic routing

C.
Within the new VPC – deploy a Virtual Private Gateway, Customer Gateway, and establish a new IPsec VPN Connection with static routing, and ensure Jumbo Frames is enabled.

D.
Within the new VPC – deploy a software based virtual router (for example a Cisco CSR). Configure with dual ENIs (external and internal), create and attach an EIP to the external ENI, Configure and setup IPsec VPN tunnels, and ensure Jumbo Frames is enabled.

Answer: B

Explanation:

Answer A – Let's start by stating that all possible options are actually workable solutions. The key criteria of the question is to complete the data migration aspects as *quickly* as possible. With this in mind we can immediately rule out Answer A – due to the time it takes to provision and activate a fully functional Direct Connect connection, 72+ hrs. Answer C is the same as Answer D but lacks BGP – therefore we would need to setup the routes manually – more time and effort. Additionally Answer D uses Jumbo Frames – but AWS does not support Jumbo frames over the Virtual Private Gateway – therefore Answer D's use of Jumbo Frames is negated. Overall Answer B is considered the quickest option.

Reference:
http://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/GenericConfig.html

QUESTION NO: 260

Convert the following IPv4 address in presented in binary form, into dotted decimal form 10101100.01111011.00001101.10011101.

A.
172.123.13.157

B.
173.13.13.157

C.
172.122.13.15

D.
172.124.13.57

Answer: A
Explanation:

An IPv4 address in dotted decimal format is constructed using binary arithmetic. In binary arithmetic, each bit within a group represents a power of two. Specifically, the first bit in a group represents 2 to the power of 0, the second bit represents 2 to the power of 1, the third bit represents 2 to the power of 2, and so on. Binary format is simple because each successive bit in a group is exactly twice the value of the previous bit.

The first octet is 128 + 32 + 8 + 4 = 172

The second octet 64 + 32 + 16 + 8 + 2 + 1 = 123

The third octet 8 + 4 + 1 = 13

The fourth octet is 128 + 16 + 8 + 4 + 1 = 157

Reference: https://en.wikipedia.org/wiki/IPv4

QUESTION NO: 261

You have been tasked with migrating your company's proprietary massively large dataset sorting application to AWS. The application currently runs on 4 highly spec'd servers that are in a cluster arrangement and runs 24x7, with the average CPU utilisation across any 24hr period being approx 85% - the migration of this cluster once up and running on AWS is expected to run similarly. The servers shuffle data internally and between themselves. Your company's financial performance is entirely dependent on the speed at which it can sort your customers datasets, that is the faster a sorted result can be returned the better your company's bottom line.

Of the choices presented below, select the optimal network configuration that will ensure the best financial results for your company.

A.
Disable Jumbo Frames to ensure better data throughput between instances

B.
Enable Jumbo Frames to ensure better data throughput between instances

C.
Create an autoscaled group of c4.8xlarge instances - with min 1 and max 4 - this will ensure your operational costs a minimal

D.
Configure a CloudWatch Alarm to add more CPUs to the instances when average cluster CPU utilisation breaches 85%

Answer: B
Explanation:

Answer C does not meet the brief – the question states that the requirement is to run a cluster of 4 servers 24x7 – and that the average CPU utilisation across any 24hr period is 85% – therefore have an ASG with min 1 and max 4 provides no benefit, and if anything scaling down from 4 machines would impact the speed at which sorting results are returned – and therefore this would affect the company's bottom line. We know that of the Answers A and B we need to choose one – Answer B best supports our requirements – to move data faster between servers. Answer D is nonsensical – AWS doesn't support adding or removing CPUs to instances.

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html

QUESTION NO: 262

Which statement is NOT true about accessing remote AWS region in the US by your AWS Direct Connect which is located in the US?

A.
To connect to a VPC in a remote region, you can use a virtual private network (VPN) connection over your public virtual interface.

B.
To access public resources in a remote region, you must set up a public virtual interface and establish a border gateway protocol (BGP) session.

C.
If you have a public virtual interface and established a BGP session to it, your router learns the routes of the other AWS regions in the US.

D.
Any data transfer out of a remote region is billed at the location of your AWS Direct Connect data transfer rate.

Answer: D

Explanation:

AWS Direct Connect locations in the United States can access public resources in any US region. You can use a single AWS Direct Connect connection to build multi-region services. To connect to a VPC in a remote region, you can use a virtual private network (VPN) connection over your public virtual interface.

To access public resources in a remote region, you must set up a public virtual interface and establish a border gateway protocol (BGP) session. Then your router learns the routes of the other AWS regions in the US. You can then also establish a VPN connection to your VPC in the remote region.

Any data transfer out of a remote region is billed at the remote region data transfer rate.

Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html

QUESTION NO: 263

You have a management server that needs to be able to communicate with two subnets. One of these subnets is private. This subnet must remain private and must not pass any traffic back to other subnets.

How would you configure this?

A.
Configure a NACL to allow access from the management server to the private server.

B.

Add an ENI to the management server that resides in the subnet of the private server.

C.
You can't do this without allowing traffic back through the other subnet.

D.
Configure a security group rule to allow access from the management server to the private server.

Answer: B
Explanation:

Add an ENI to the management server that resides in the subnet of the private server. This will allow the management server to communicate with the private server without having to change security rules.

QUESTION NO: 264

You need to find the subnet, the security group and the VPC that your instance is associated with. You only have access to the terminal of an instance with an admin role attached.

What is the first part of the command you would use?

A.
aws ec2 describe-network-acl

B.
aws ec2 describe-instances

C.
aws vpc describe-all

D.
aws ec2 describe-security-groups

Answer: B
Explanation:

aws ec2 describe-instances will tell a significant amount of information about the instances in your account. Apply a filter to be able to see information about your instance. Describe-security-groups and describe-network-acl would not allow you to see which group is associated with your instance and aws vpc describe-all doesn't exist.

QUESTION NO: 265

You are working with a government agency, and you need to choose an encryption standard for their VPN. Which standard should you choose?

A.
Twofish

B.
Blowfish

C.
TripleDES

D.
AES

Answer: D
Explanation:

AES is the US Government standard

QUESTION NO: 266

You have a hybrid infrastructure, and you need AWS resources to be able to resolve your on-premises DNS names. You have configured a DNS server on an EC2 instance in your 10.1.3.0/24 subnet. This subnet resides on the VPC 10.1.0.0/16. What step should you take to accomplish this?

A.
Configure your DNS server to forward queries for the private hosted zone to 10.1.3.2.

B.
Configure the DHCP option set in the VPC to point to the EC2 DNS server.

C.
Configure your DNS server to forward queries for the private hosted zone to 10.1.0.2.

D.
Disable the source/destination check flag for the DNS instance.

Answer: B

Explanation:

Your DNS server will forward queries to your on-premises DNS. You must configure the DHCP option set so the instances will forward queries to your on-premises DNS instead of the VPC DNS.

QUESTION NO: 267

You have several VPCs that are peered. Each VPC has several routes to different subnets. Over the years, your company has acquired many companies. You find that traffic destined for one VPC ends up going to another.

What is the best way to remedy this?

A.
Move the route table entry for the proper VPC higher in the list.

B.
Adjust your routes so the proper VPC has a higher CIDR.

C.
Move the route table entry for the proper VPC lower in the list.

D.
Adjust your routes so the proper VPC has a lower CIDR.

Answer: B

Explanation:

The higher CIDR or more specific route will always take precedence.

QUESTION NO: 268

You have set up an S3 endpoint, and you want to restrict some instances from being able to access it. These instances are all in the same subnet, so you cannot simply remove the prefix list from the route table.

What two approaches can you take to solve this? (Choose two.)

A.
Remove any access to the PL in the security group attached to the instances.

B.
Add A rule in the NACL to block the prefix list ID outbound.

C.
This is not possible.

D.
Modify the endpoint policy.

Answer: A,D

Explanation:

You cannot add a prefix list ID to a NACL.

QUESTION NO: 269

You want to send a broadcast message to your 10.0.0.0/24 subnet, which one of these addresses should you use?

A.
10.0.0.255

B.
10.0.0.1

C.
10.0.0.2

D.
You cannot send a broadcast in an AWS VPC.

Answer: D

Explanation:

You cannot send a broadcast in an AWS VPC, but the address is still reserved.

QUESTION NO: 270

You have two VPCs that require DNS resolution from your on-premises data center. You want to have a DNS server in the cloud, but you don't want to have multiple DNS servers.

What two steps should you take? (Choose two.)

A.
Peer the VPCs and set up routes between them.

B.
Create a VPN between the two VPCs

C.
Configure DHCP option sets in both VPCs to point to the DNS server.

D.
Configure a Route 53 record to forward all DNS requests to the DNS server.

Answer: A,C

Explanation:

Peer the VPCs and configure DHCP option sets. A VPN is not necessary. You cannot create a Route 53 record to forward DNS requests.

QUESTION NO: 271

Your company has a highly-available Direct Connect solution that utilizes two datacenters. Each datacenter was initially configured with one four-connection LAG and one standard DX connection. How many LOA documents have been requested and completed for this configuration?

A.
1

B.
4

C.
2

D.
10

Answer: B

Explanation:

Only one LOA document is required for each physical connection. The logical connections in the LAG do not need separate LOAs, but they do have separate pages.

QUESTION NO: 272

To connect to public AWS products such as Amazon EC2 and Amazon S3 through the AWS Direct Link, which step is NOT required?

A.
Provide public IP address (/31) for each Border Gateway Protocol (BGP) session.

B.
Allocate a Private IP address to your network in 172.x.x.x range.

C.
Provide the public routes that you will advertise over Border Gateway Protocol (BGP).

D.
Provide a public Autonomous System Number (ASN) that you own or a private one to identify your network on the Internet.

Answer: B

Explanation:

To connect to public AWS products such as Amazon EC2 and Amazon S3 through the AWS Direct Connect, you need to provide the following:

A public Autonomous System Number (ASN) that you own (preferred) or a private ASN. Public IP addresses (/30) (that is, one for each end of the BGP session) for each BGP session. The public routes that you will advertise over BGP.

Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

QUESTION NO: 273

True or false: A VPC contains multiple subnets, where each subnet can span multiple Availability Zones.

A.
This is true only for US regions.

B.
This is false.

C.
This is true.

D.
This is true only if requested during the set-up of VPC.

Answer: B
Explanation:

A VPC can span several Availability Zones. In contrast, a subnet must reside within a single Availability Zone.

Reference: https://aws.amazon.com/vpc/faqs/

QUESTION NO: 274

Over which of the following Ethernet standards does AWS Direct Connect link your internal network to an AWS Direct Connect location?

A.
Copper backplane cable

B.
Twisted pair cable

C.
Single mode fiber-optic cable

D.
Shielded balanced copper cable

Answer: C
Explanation:

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet single mode fiber-optic cable.

Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

QUESTION NO: 275

Fill in the blanks: One of the basic characteristics of security groups for your VPC is that you ______ .

A.
can specify allow rules, but not deny rules

B.
can specify deny rules, but not allow rules

C.
can specify allow rules as well as deny rules

D.
can neither specify allow rules nor deny rules

Answer: A
Explanation:

Security Groups in VPC allow you to specify rules with reference to the protocols and ports through which communications with your instances can be established. One such rule is that you can specify allow rules, but not deny rules.

Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

QUESTION NO: 276

Which of the following physical layer standards is required for connection to AWS Direct Connect over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable?

A.
Single mode fiber, 1000BASE-LX for 1 gigabit Ethernet, or 10GBASE-ER for 10 gigabit Ethernet

B.
Multi mode fiber, 1000BASE-LX for 1 gigabit Ethernet, or 10GBASE-ER for 10 gigabit Ethernet

C.
Single mode fiber, 1000BASE-LX for 1 gigabit Ethernet, or 10GBASE-LR for 10 gigabit Ethernet

D.
Multi mode fiber, 1000BASE-SX for 1 gigabit Ethernet, or 10GBASE-SR for 10 gigabit Ethernet

Answer: C
Explanation:

Connections to AWS Direct Connect require single mode fiber, 1000BASE-LX (1310nm) for 1 gigabit Ethernet, or 10GBASE-LR (1310nm) for 10 gigabit Ethernet.

Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

QUESTION NO: 277

In AWS Direct Connect, which of the following is true of configuring your router to connect to the AWS Direct Connect router?

A.
After creating a virtual interface for your AWS Direct Connect connection, you can download the router configuration file from the available link

B.
After Completing the Cross Connect step, the download link for router configuration will be available

C.
After submitting your AWS Direct Connect connection request, you will receive the router configuration details by email within 72 hours

D.
In Create a Virtual Interface step, the general configuration of your router would be available for downloading.

Answer: A
Explanation:

To use the AWS Direct Connect, after you have created a virtual interface for your AWS Direct Connect connection, you can download the router configuration file. This configuration helps your router connect to AWS Direct Connect router. This configuration is related to your created virtual interface details and vendor, platform, and software of your router.

Reference:
http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#routerconfig

QUESTION NO: 278

In AWS Direct Connect, to provide for failover, AWS recommends that you request and configure two dedicated connections to AWS. These connections can terminate on one or two routers in your network. You can do this while __________________ with AWS Direct Connect step.

A.
creating a Virtual Interface

B.
configuring redundant connections

C.
completing the cross-connect

D.
verifying your Virtual Interface

Answer: B
Explanation:

In AWS Direct Connect, to provide for failover, AWS recommends that you request and configure two dedicated connections to AWS.

These connections can terminate on one or two routers in your network. You can do this in Configure Redundant Connections with AWS Direct Connect step.

Reference:
http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#RedundantConnections

QUESTION NO: 279

To get started using AWS Direct Connect, in which of the following steps do you configure Border Gateway Protocol (BGP)?

A.
Complete the Cross Connect

B.
Verify your Virtual Interface

C.
Create a Virtual Interface

D.
Submit AWS Direct Connect Connection Request

Answer: C
Explanation:

In AWS Direct Connect, your network must support Border Gateway Protocol (BGP) and BGP MD5 authentication, and you need to provide a private Autonomous System Number (ASN) for that to connect to Amazon Virtual Private Cloud (VPC). To connect to public AWS products such as Amazon EC2 and Amazon S3, you will also need to provide a public ASN that you own (preferred) or a private ASN. You have to configure BGP in the Create a Virtual Interface step.

Reference:
http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#createvirtualinterface

QUESTION NO: 280

Does Amazon VPC support multicast or broadcast?

A.
Yes, both.

B.
It doesn't support any of them.

C.
Multicast yes, Broadcast no.

D.
Both, but only outside Amazon VPC.

Answer: B
Explanation:

Amazon VPC does not support multicast nor broadcast

Reference: https://aws.amazon.com/vpc/faqs/

QUESTION NO: 281

Imagine you are using AWS Direct Connect with just one connection from your router to the AWS Direct Connect router. If your connection becomes unavailable, the communication with AWS cloud is lost. What is the best method to prevent this from happening?

A.
AWS Direct Connect neither provides BGP nor provides the failover.

B.
AWS Direct Connect recommends to have the same configuration set up in a multi AZ zone to prevent such loss in connections.

C.
AWS Direct Connect recommends that you request and configure two dedicated connections to AWS either using BGP Multipath (Active/Active) connection or the failover (Active/Passive) connection.

D.
AWS Direct connect does not have a provision to prevent the situation but when you design the system, it is recommended to request a back-up instance to which the traffic can be re-routed.

Answer: C

Explanation:

When configuring redundant connections with the AWS Direct Connect, and to provide for failover, we recommend that you request and configure two dedicated connections to the AWS. There are different configuration choices available when you provision two dedicated connections. You can either use Active/Active (BGP multipath) connection or Active/Passive (failover) connection to configure the two dedicated connections.

Reference:
http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted.html#RedundantConnections

QUESTION NO: 282

Which endpoint is considered to be best practice when analyzing data within a Configuration Stream of AWS Config?

A.
SNS

B.
E-Mail

C.
SQS

D.
Kinesis

Answer: C
Explanation:

The Simple Queue Service can be subscribed to the AWS Config topic (the Configuration Stream) which gives you a highly available and decoupled environment for the data within your Configuration Streams. By using SQS it allows you to create and use your own applications to extract only information and data that is pertinent to you. There can be vast amounts of data coming into the Configuration Stream, but you might only want to be notified and made away of any changes that may relate to any potential security issues. As a result, you may want to pull information from the queue that only relate to Security Groups/NACLs/IAM Roles or any other resource type that could affect the security of your environment.

Reference: http://docs.aws.amazon.com/config/latest/developerguide/monitor-resource-changes.html

QUESTION NO: 283

You are the network engineer at your company, and you are noticing issues with QoS in you're the traffic to your instances hosting a VOIP program. You need to inspect the network packets to determine if it is a programming error or a networking error. How should you do this?

A.
Configure a network monitoring program on every instance and stream the logs to an S3 bucket to be parsed.

B.
Use CloudWatch

C.
Set up another instance with an ENI added to act as a monitoring interface. Set the port to "promiscuous mode" and sniff the traffic to analyze the packets. Then output this single stream to an S3 bucket to be parsed.

D.
Inspect Flow Logs

Answer: A
Explanation:

Flow Logs and CloudWatch do not display packet contents. You cannot sniff traffic destined for other instances.

QUESTION NO: 284

Your company has a highly available Direct Connect solution that utilizes two datacenters. Each data center contains one two-connection LAG and one standard DX connection. How many LOAs will be filled out in total if your company completes an order to add a new connection to each one of the LAGs?

A.
1

B.
11

C.
2

D.
6

Answer: D
Explanation:

Four LOAs are required for the first order and two more for the second.

QUESTION NO: 285

Your boss decides to assign an Elastic IP to a production instance. Once he does this, access to the URL for that website fails. What happened?

A.
The original IP address was released back to AWS when the Elastic IP was assigned.

B.
Your boss only needs to restart the Apache service.

C.
Your boss should have turned off the server before assigning the IP address.

D.
Your boss needs to restart the server.

Answer: A

Explanation:

The original IP address was released back to AWS when the Elastic IP was assigned. If you attach an EIP, you lose the address originally assigned to the instance unless you add it to another interface.

QUESTION NO: 286

You have a data center with a 2 connection LAG. You wish to add 2 more connections, how many LOAs must you complete?

A.
2

B.
1

C.
4

D.
0

Answer: A

Explanation:

You must complete a LOA for each new physical connection.

QUESTION NO: 287

Your VPC has a DX connection that is advertising 99 routes. You have two more prefixes to add: 10.223.1.0/24 and 10.223.2.0/24. You have several locations, so you need to be as exact as possible with your routing.

How would you do this?

A.
Add the prefixes; AWS allows for as many BGP routes as you need but not static.

B.
Contact AWS to extend the number of prefixes you are allowed to advertise.

C.
Summarize the routes into a 10.223.0.0/22 and advertise that route instead.

D.
Summarize the routes into a 10.223.0.0/12 and advertise that route instead.

Answer: C

Explanation:

BGP has a strict 100 prefix limit. 10.223.0.0/12 includes both routes but is not very specific. 10.223.0.0/22 is the proper summarization of both routes.

QUESTION NO: 288

You have a hybrid environment in which your VPC queries your on-premises DNS server for up resources in your environment. The EC2 instances in your VPC are unable to resolve on-premises resources.

What are two possible reasons for this problem? (Choose two.)

A.
Your NACL is blocking UDP port 53 outbound

B.
Your security group is blocking port 53 inbound

C.
Your NACL is blocking TCP port 53 outbound.

D.
Your on-premises firewall is blocking port 443

Answer: A,C
Explanation:

DNS requires TCP and UDP port 53.

QUESTION NO: 289

After setting an AWS Direct Connect, which of the following cannot be done with an AWS Direct Connect Virtual Interface?

A.
You can delete a virtual interface; if its connection has no other virtual interfaces, you can delete the connection.

B.
You can change the region of your virtual interface.

C.
You can create a hosted virtual interface.

D.
You can exchange traffic between the two ports in the same region connecting to different Virtual Private Gateways (VGWs) if you have more than one virtual interface.

Answer: D
Explanation:

You must create a virtual interface to begin using your AWS Direct Connect connection. You can create a public virtual interface to connect to public resources or a private virtual interface to connect to your VPC. Also, it is possible to configure multiple virtual interfaces on a single AWS Direct Connect connection, and you'll need one private virtual interface for each VPC to connect to. Each virtual interface needs a VLAN ID, interface IP address, ASN, and BGP key. To use your AWS Direct Connect connection with another AWS account, you can create a hosted virtual interface for that account. These hosted virtual interfaces work the same as standard virtual interfaces and can connect to public resources or a VPC.

Reference:
http://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html

QUESTION NO: 290

In the "start using the AWS Direct Connect steps," when can you complete the Cross Connect step?

A.
After verifying your virtual interface

B.
After you have received your Letter of Authorization and Connecting Facility Assignment (LOA-CFA) from AWS

C.
72 hours after submitting your request for AWS Direct Connect Connection

D.
Immediately after submitting your request for AWS Direct Connect Connection

Answer: B
Explanation:

To complete the steps of "start using the AWS Direct Connect," after submitting your request for AWS Direct Connect connection, AWS will send you an email within 72 hours with a Letter of Authorization and Connecting Facility Assignment (LOA-CFA). After you have received your LOA-CFA, you need to complete your cross-network connection, also known as a cross connect.

Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Colocation.html

QUESTION NO: 291

By default, all AWS accounts are limited to ____ EIPs, because public (IPv4) Internet addresses are a scarce public resource.

A.
5

B.
8

C.
6

D.
2

Answer: A
Explanation:

An Elastic IP address (EIP) is a static IP address designed for dynamic cloud computing. With an EIP, you can mask the failure of an instance by rapidly remapping the address to another instance. By default, all AWS accounts are limited to 5 EIPs, because public (IPv4) Internet addresses are a scarce public resource.

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html

QUESTION NO: 292

A user has created a VPC with CIDR 20.0.0.0/16 with only a private subnet and VPN connection using the VPC wizard. The user wants to connect to the instance in a private subnet over SSH.

How should the user define the security rule for SSH?

A.
The user can connect to a instance in a private subnet using the NAT instance

B.
The user has to create an instance in EC2 Classic with an elastic IP and configure the security group of a private subnet to allow SSH from that elastic IP

C.
Allow Inbound traffic on port 22 from the user's network

D.
Allow Inbound traffic on port 80 and 22 to allow the user to connect to a private subnet over the internet

Answer: C
Explanation:

The user can create subnets as per the requirement within a VPC. If the user wants to connect VPC from his own data centre, the user can setup a case with a VPN only subnet (private) which uses VPN access to connect with his data centre. When the user has configured this setup with Wizard, all network connections to the instances in the subnet will come from his data centre. The user has to configure the security group of the private subnet which allows the inbound traffic on SSH (port 22) from the data centre's network range.

Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario4.html

QUESTION NO: 293

In Amazon CloudFront, if you need to quickly remove objects from a distribution, you can:

A.
delete the objects from cache.

B.
invalidate the objects.

C.
remove your Amazon S3 bucket.

D.
delete your distribution and recreate it.

Answer: B
Explanation:

In Amazon CloudFront, if you need to quickly remove objects from a distribution, you can invalidate them.

Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AddRemoveReplaceObjects.html

QUESTION NO: 294

Which of the following types of contents cannot serve over HTTP or HTTPS in Amazon CloudFront?

A.
Apple HTTP Live Streaming

B.
Static and dynamic download content

C.
Adobe Flash multimedia content

D.
CloudFront RTMP distribution

Answer: C

Explanation:

In Amazon CloudFront, you can use web distributions to serve the following content over HTTP or HTTPS: Static and dynamic download content, for example, .html, .css, .php, and image files, using HTTP or HTTPS.

Multimedia content on demand using progressive download and Apple HTTP Live Streaming (HLS). A live event, such as a meeting, conference, or concert, in real time. You can't serve Adobe Flash multimedia content over HTTP or HTTPS.

Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-overview.html

QUESTION NO: 295

You need to create a subnet in a VPC that supports 1000 hosts. You need to be as accurate as possible since you run a very large company. What CIDR should you use?

A.
/16

B.
/24

C.
/7

D.
/22

Answer: D
Explanation:

/22 supports 1019 hosts since AWS reserves 5 addresses.

QUESTION NO: 296

You are managing a VPC with 4 AZs. There is a load balancer managing the public accessibility to your servers. You have a secondary ENI with a private IPv4 address on an instance that is serving public web traffic. Your server communicates over private addresses to a database in another subnet. Security is a major concern for your company and whitelisting is in effect.

You have to bring the web server down for maintenance, what two things should you do? (Choose two.)

A.
Reboot the instance.

B.
Move the ENI from one server to the other.

C.
Associate the new ENI with the database security group.

D.
Configure a secondary ENI on the standby instance.

Answer: C,D
Explanation:

You must configure a secondary ENI on the standby instance with an IP address that can access the data subnet. This may require modification of the security group for the database.

QUESTION NO: 297

You manage a webserver that serves a webpage on AWS infrastructure. You utilize an Application Load Balancer, CloudFront, S3, and some other AWS services for this site. You are only responsible for the server and you don't have access to the AWS console or API.

You need to find out what IPs are accessing your website. What is the best way to achieve this?

A.
Ask someone with IAM permissions to view the Flow Logs to give you access.

B.
View the access logs. They already show this information.

C.
Run "curl http://169.254.169.254/latest/meta-data/access_log

D.
Add "X-Forwarded For" to the access logs and view the access logs.

Answer: D
Explanation:

Add "X-Forwarded For" to the access logs and view the access logs is the best answer here. IAM permissions could work, but not necessary, the curl command queries metadata, not access logs.

QUESTION NO: 298

You have 3 VPCs that need to be able to pass traffic. In what two ways can you achieve this? (Choose two.)

A.
Peer each VPC to every other VPC to create a full mesh peering.

B.
Peer them, VPC peering allows transitive peering as of December 2017.

C.
Call AWS to enable transitive peering.

D.

Create VPNs between them and adjust the routing tables accordingly.

Answer: A,D

Explanation:

VPN instances can be used to create transitive peering. Full mesh peering is the only way to use peering to allow all VPCs to communicate with all other VPCs. Transitive peering is not possible.

QUESTION NO: 299

You have a Simple AD deployment, and you wish to use it for your Microsoft Exchange email server. You are having issues finding the AD server, why might this be?

A.
You need to contact AWS to receive a PTR record for your email server.

B.
Your firewall is blocking it.

C.
Simple AD is not a full Active Directory server and will not work with many MS products.

D.
SSL is not implemented.

Answer: C

Explanation:

Simple AD is Samba based and does not support full Microsoft AD integration.

QUESTION NO: 300

You have 99 routes in your dynamic BGP propagated route table and you wish to add 2 more: 10.1.0.0 and 10.3.0.0. You cannot modify or remove routes that have already been announced.

What should you do?

A.
Summarize the two routes to combine them into one and advertise it.

B.
Just advertise them, the 100 route limit is a "soft limit" and will be expanded automatically.

C.
You cannot add these routes.

D.
Call AWS support to increase your route limit.

Answer: A

Explanation:

You cannot add these routes. If you try to summarize them, that would create a 10.0.0.0/14, which is too low of a CIDR to advertise to AWS. AWS has a minimum of /16. You cannot have the 100 route limit modified in any way. It is a hard 100 route limit.

QUESTION NO: 301

In the context of CloudFront RTMP Distribution, the Adobe Flash Media Server _________ file specifies which domains can access media files in a particular domain.

A.
accessdomain.JSON

B.
crossdomain.xml

C.
accessdomain.xml

D.
crossdomain.JSON

Answer: B

Explanation:

In the context of CloudFront RTMP Distribution, the Adobe Flash Media Server crossdomain.xml file specifies which domains can access media files in a particular domain.

Reference:

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Streaming_CrossDomain.html

QUESTION NO: 302

In Amazon CloudFront, you cannot configure CloudFront to process cookies for_________.

A.
HTTPS web distributions

B.
Web and RTMP distributions

C.
RTMP distributions

D.
HTTP web distributions

Answer: C
Explanation:

You cannot configure Amazon CloudFront to log cookies for RTMP distributions. For web distributions, CloudFront by default doesn't consider cookies when caching your objects in edge locations. If your origin returns two objects and they differ only by the values in the Set-Cookie header, CloudFront caches only one version of the object.

Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Cookies.html

QUESTION NO: 303

For _______ distributions, CloudFront does not cache cookies in edge caches.

A.
AMI

B.
Web

C.
RTMP

D.
Web and RTMP

Answer: C

Explanation:

For RTMP distributions, when Amazon CloudFront requests an object from the origin server, it removes any cookies before forwarding the request to your origin. If your origin returns any cookies along with the object, CloudFront removes them before returning the object to the viewer.

For RTMP distributions, CloudFront does not cache cookies in edge caches.

Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Cookies.html

QUESTION NO: 304

With respect to Amazon CloudFront, which one of the following statements is correct?

A.
For HTTPS web distributions, you cannot forward cookies to your origin.

B.
For both HTTP and HTTPS web distributions, you can choose to forward cookies to your origin.

C.
For HTTP web distributions, you cannot forward cookies to your origin.

D.
For Real Time Messaging Protocol (RTMP) distributions, you can configure CloudFront to process cookies.

Answer: B

Explanation:

With respect to Amazon CloudFront, for HTTP and HTTPS web distributions, you can choose whether you want CloudFront to forward cookies to your origin. For RTMP distributions, you cannot configure CloudFront to process cookies.

Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Cookies.html

QUESTION NO: 305

What are two services that help mitigate a DDoS? (Choose two.)

A.
AWS Shield

B.
DynamoDB

C.
Elastic Beanstalk

D.
CloudFront

Answer: A,D

Explanation:

AWS Shield and CloudFront can help mitigate the effects of a DDoS

QUESTION NO: 306

Which service would you use to see the DSCP value in a packet header?

A.
CloudTrail

B.
Config

C.
Flow Logs

D.
None of the above

Answer: D

Explanation:

To perform deep packet inspection, you would need a specialized tool such as Wireshark.

QUESTION NO: 307

Which service parses large Flow Logs for consumption by other programs such as Kibana?

A.
S3

B.
ElasticSearch

C.
Elastic Beanstalk

D.
Kinesis

Answer: B

Explanation:

QUESTION NO: 308

Which service would you use to see if your infrastructure has changed?

A.
Config

B.
Elastic Beanstalk

C.
CloudTrail

D.
CloudWatch

Answer: C

Explanation:

QUESTION NO: 309

What service is used to store the log files generated by CloudTrail?

A.
EC2

B.
EBS

C.
S3

D.
VPC

Answer: C

Explanation:

The AWS CloudTrail uses Amazon's Simple Storage Service (S3) to store log files. It also supports the use of S3 life cycle configuration rules to reduce storage costs.

Reference: https://aws.amazon.com/cloudtrail/

QUESTION NO: 310

In AWS, which tool records API calls for a specific AWS account and also delivers the log files for that account?

A.
CloudTrail

B.
Redshift

C.

Beanstalk

D.
Cognito

Answer: A
Explanation:

The AWS CloudTrail is a web service that is used to record AWS API call for a specific AWS account. It also delivers log files, which provide the following details:

Reference: https://aws.amazon.com/cloudtrail/

QUESTION NO: 311

Which CloudWatch attributes are used for the statistics generation?

A.
All the options are used

B.
Dimension

C.
Data point unit

D.
NameSpace

Answer: A
Explanation:

Statistics represents data aggregation of the metric data values over a specific period of time. These aggregations are made using the namespace, metric name, dimensions and the data point unit of measure within the time period that the user has specified.

Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/API_MetricDatum.html

QUESTION NO: 312

AWS CloudTrail can be configured to ____ log files across multiple accounts and regions so that log files are delivered to a single bucket.

A.
aggregate

B.
disperse

C.
replicate

D.
encrypt

Answer: A
Explanation:

You can configure CloudTrail to aggregate log files from multiple regions and deliver them to a single S3 bucket for a single account.

Reference: https://aws.amazon.com/cloudtrail/

QUESTION NO: 313

In AWS, which service provides a reliable and inexpensive way to backup and archive CloudTrail log files?

A.
Amazon Archiver

B.
Amazon Glacier

C.
AWS Storage Gateway

D.

Amazon Elastic Block Store

Answer: B

Explanation:

You control the retention policies for your CloudTrail log files. By default, log files are stored indefinitely, but for cost efficiency, you may want to delete old log files or archive them to Amazon Glacier, a storage service optimized for data archiving and backup of infrequently used data.

Reference: https://aws.amazon.com/cloudtrail/faqs/

QUESTION NO: 314

For web distributions in Amazon CloudFront, your origin can be either an Amazon S3 bucket or _______ .

A.
a DNS server

B.
a proxy server

C.
an FTP server

D.
an HTTP server

Answer: D

Explanation:

For web distributions in Amazon CloudFront, your origin can be either an Amazon S3 bucket or an HTTP server.

Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-overview.html

QUESTION NO: 315

In the context of Amazon CloudFront, when you configure the media player, the path you specify to the media file must contain the characters _____________.

A.
flv/std just before the domain name

B.
flv/std immediately after the domain name

C.
cfx/st just before the domain name

D.
cfx/st immediately after the domain name

Answer: D

Explanation:

In Amazon CloudFront, when you configure the media player, the path you specify to the media file must contain the characters cfx/st immediately after the domain name. For example:

rtmp://s5c39gqb8ow64r.cloudfront.net/cfx/st/mediafile.flv

Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Streaming_URLs.html

QUESTION NO: 316

Which of the following is true when you don't configure Amazon CloudFront to forward cookies to your origin?

A.
CloudFront removes the Cookie header from requests that it forwards to your origin.

B.
CloudFront disables viewer requests to your origin, including all cookies.

C.
CloudFront caches your objects based on cookie values.

D.
CloudFront automates code deployments to any instance.

Answer: A
Explanation:

If you don't configure CloudFront to forward cookies to your origin, CloudFront removes the Cookie header from requests that it forwards to your origin and removes the Set-Cookie header from responses that it returns to your clients.

Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Cookies.html

QUESTION NO: 317

What is the maximum size of a response body that Amazon CloudFront will return to the viewer?

A.
Unlimited

B.
5 GB

C.
100 MB

D.
20 GB

Answer: D
Explanation:

The maximum size of a response body that CloudFront will return to the viewer is 20 GB.

Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/RequestAndResponseBehaviorS3Origin.html#ResponseBehaviorS3Origin

QUESTION NO: 318

How many tunnels do you get with each VPN connection hosted by AWS?

A.
4

B.
1

C.
2

D.
8

Answer: C
Explanation:

All AWS VPNs come with 2 tunnels for resiliency.

QUESTION NO: 319

You are configuring a VPN to AWS for your company. You have configured the VGW and CGW. You have created the VPN. You have also run the necessary commands on your router. You allowed all TCP and UDP traffic between your datacenter and your VPC. The tunnel still doesn't come up. What is the most likely reason?

A.
You forgot to turn on route propagation in the route table.

B.
You do not have a public ASN.

C.
Your advertised subnet is too large.

D.
You haven't added protocol 50 to your firewall.

Answer: D
Explanation:

You haven't allowed protocol 50 through the firewall. Protocol 50 is different from UDP (17) and TCP (6) and requires a rule in your firewall for your VPN tunnel to come up.

QUESTION NO: 320

Your company has decided to deploy AWS WorkSpaces for its hosted desktop solution. Your manager is very concerned with security and cost, as well as reliability.

What two things should be deployed? (Choose two.)

A.
VPN

B.
AWS Hosted AD

C.
Direct Connect

D.
AD Connector

Answer: C,D
Explanation:

A VPN should be deployed over Direct Connect to ensure the traffic is encrypted. You would use an AD Connector here since it doesn't cache any credentials in the cloud. AWS Hosted AD is more expensive and caches credentials.

QUESTION NO: 321

You work for a company that has several instances running with automatically assigned public IPs. You performed an upgrade that required you to restart the instances from the console and your DNS records don't work anymore. What happened?

A.
Your network interfaces need to be reinitialized

B.
You need to restart Route 53

C.
Restarting too many instances at once overloads the system

D.
The instances changed their public IP addresses on restart

Answer: D
Explanation:

Automatically assigned public IPs change on stop or termination of an instance.

QUESTION NO: 322

Your company wishes to improve the performance of its EC2 instances. They require low latency and high throughput. They are currently deployed on T2.medium. It is imperative that you experience as little downtime as possible, but cost and performance are most important. How should you accomplish this?

A.
Create AMIs from the instances, create new instances on t2.medium, and start those instances in a placement group.

B.
Create AMIs from the instances, deploy the instances as i3.large, and start those instances in a placement group.

C.
Stop the instances and restart them in a placement group.

D.
Add an extra ENI to the instances and team them to provide greater throughput.

Answer: B
Explanation:

T2. medium is not compatible with placement groups. You cannot team ENIs to add more throughput on AWS.

QUESTION NO: 323

You need to ensure the files served by your CloudFront distribution are only accessible to authorized users. You hope to serve thousands of users. What two steps should you take? (Choose two.)

A.
Configure signed cookies.

B.
Configure a WAF.

C.
Configure a bucket policy restricting the bucket to only CloudFront OAI.

D.
Configure an SSL on the distribution.

Answer: A,C
Explanation:

A WAF can block users from accessing the site and CloudFront, but that's not the best option since you have so many users. An SSL will encrypt, but not prevent a user from viewing the content.

QUESTION NO: 324

In Amazon CloudFront, which of the following is true of Smooth Streaming?

A.
It is a Microsoft format for streaming of media files.

B.
It is a CloudFront format for streaming of media files in RTMP distribution.

C.
It is the Adobe format for streaming of media files.

D.
It is a CloudFront format for streaming of media files in web distribution.

Answer: A
Explanation:

In the context of Amazon CloudFront, you can use CloudFront for on-demand streaming of media files that you've transcoded into the Microsoft Smooth Streaming format. To distribute Smooth

Streaming content on demand, you have two options: As the origin for your distribution, specify a web server that can stream files that have been transcoded into Microsoft Smooth Streaming format. Enable Smooth Streaming in a CloudFront distribution. Smooth Streaming is a property of cache behaviors, which means that you can use one distribution to distribute Smooth Streaming media files as well as other content.

Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/on-demand-streaming-smooth.html

QUESTION NO: 325

In the context of Amazon CloudFront Actions, you use the _____ when specifying APIs in IAM policies.

A.
object names

B.
class names

C.
entity names

D.
action names

Answer: D

Explanation:

In an AWS IAM policy, you can specify any and all API actions that Amazon CloudFront offers. The action name must be prefixed with the lowercase string cloudfront. For example:

cloudfront:GetDistributionConfig

cloudfront:ListInvalidations

cloudfront:* (for all CloudFront actions).

In the reference link, there are tables that list the canonical names for all CloudFront actions. Use these canonical names when specifying APIs in IAM policies.

Reference:

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/UsingWithIAM.html

QUESTION NO: 326

In Amazon CloudFront, while creating a web distribution, which of the following can be used as origin servers?

A.
Any combination AWS Glacier archives and Oracle server

B.
Any combination of Amazon DB intances and XML servers

C.
Any combination of Amazon S3 buckets and HTTP servers

D.
Any combination of Amazon Data Insights and PHP servers

Answer: C
Explanation:

In Amazon CloudFront, while creating a web distribution, you can create one or more Amazon S3 buckets or configure HTTP servers as your origin servers. An origin is the location where you store the original version of your web content. When CloudFront gets a request for your files, it goes to the origin to get the files that it distributes at edge locations. You can use any combination of Amazon S3 buckets and HTTP servers as your origin servers.

Reference: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-creating.html

QUESTION NO: 327

In Amazon CloudFront, to link to your objects, if your domain name is d111111abcdef8.cloudfront.net and your object is image.jpg, then the URL for the link in your webpage will be _____.

A.

http://d111111abcdef8.cloudfront.net/images/image.jpg

B.
http://d111111abcdef8.dns/images/image.jpg

C.
http://d111111abcdef8.dns/image.jpg

D.
http://d111111abcdef8.cloudfront.net/image.jpg

Answer: D
Explanation:

In Amazon CloudFront, to link to your objects, if your domain name was d111111abcdef8.cloudfront.net and your object was image.jpg, the URL for the link would be: http://d111111abcdef8.cloudfront.net/image.jpg.

If your object is in a folder within your bucket, include the folder in the URL. For example, if image.jpg is located in an images folder, then the URL would be:

http://d111111abcdef8.cloudfront.net/images/image.jpg.

Reference:
http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GettingStarted.html

QUESTION NO: 328

Which service is used by default to store the CloudTrail log files?

A.
Elastic Block Store (EBS)

B.
Redshift

C.
Simple Storage Service (S3)

D.
Glacier

Answer: C

Explanation:

S3 is used by default to store the CloudTrail log files and a dedicated S3 bucket is required during the creation of a new Trail

Reference: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-working-with-log-files.html

QUESTION NO: 329

With AWS CloudTrail, creating multiple trails in one region allows ____ to focus on one aspect of AWS operation.

A.
callers

B.
events

C.
buckets

D.
stakeholders

Answer: D

Explanation:

With multiple trails, different stakeholders such as security administrators, software developers, and IT auditors can create and manage their own trails. For example, a security administrator can create a trail that applies to all regions and configure encryption using one Key Management Service key. A developer can create a trail that applies to one region for troubleshooting operational issues.

Reference: https://aws.amazon.com/cloudtrail/faqs/

QUESTION NO: 330

Your company has installed an AWS Direct Connect connection in an ap-southeast-1 Direct Connect location. A public virtual interface is configured through a router to a dedicated firewall. You advertise your company's public /24 CIDR block to AWS with AS 65500. The company maintains a separate, corporate Internet firewall to map all outbound traffic to a single IP. This firewall maintains a BGP relationship with an upstream Internet provider that has delegated the public IP block your company uses. When the BGP session for the public virtual interface is up, corporate network users cannot access Amazon S3 resources in the ap-southeast-1 region.

Which step should you take to provide concurrent AWS and Internet access?

A.
Configure AS-PATH prepending for the public virtual interface.

B.
Advertise a host route for the corporate firewall on the public virtual interface.

C.
Advertise a host route for the corporate firewall to the upstream Internet provider.

D.
NAT the traffic destined for AWS from the dedicated firewall using the public virtual interface.

Answer: D

Explanation:

When outgoing traffic is routed via the corporate firewall, its return path is via the Direct Connect public virtual interface and therefore through the dedicated firewall. This dedicated firewall does not track the original NAT session and subsequently drops the traffic. Answer A is incorrect because AWS will always prefer Direct Connect over Internet routing. Answer B is incorrect because return traffic is still processed by the dedicated firewall. Answer C is incorrect because it does not change the traffic flow.

QUESTION NO: 331

Your Amazon Kinesis application receives data streams from thousands of devices. The data is then stored in an on-premises Hadoop cluster. You are concerned about historical data that shows periods of sustained traffic between 1 Gbps and 2 Gbps during peaks. You must ensure that you have secure, fault- tolerant connectivity between Amazon Kinesis and your data center.

What should you implement to address these needs?

A.

Deploy a single 1-Gbps Direct Connect connection with a VPN backup.

B.
Deploy three 1-Gbps Direct Connect connections.

C.
Deploy two 1-Gbps Direct Connect connections.

D.
Set up an IPsec VPN connection over Direct Connect with two tunnels.

Answer: B
Explanation:

Three connections are required to provide fault tolerance. All of the other options would be unable to handle the peak loads over 1 Gbps without exceeding the available bandwidth.

QUESTION NO: 332

You have a web application (app.mycompany.com) running on an EC2 instance with a single elastic network interface in a subnet in a VPC. Because of a network redesign, you need to move the web application to a different subnet in the same Availability Zone.

Which of the following migration strategies meets the requirements?

A.
Create an elastic network interface in the new subnet. Attach this interface to the instance, and detach the old interface.

B.
Launch a new instance in the subnet via an AMI created from the instance, and redirect new connections to this new instance using DNS. Decommission the old instance.

C.
Make an API call to change the subnet association of the elastic network interface.

D.
Change the IP addresses manually to another subnet within the server operating system.

Answer: B
Explanation:

Instances cannot change subnets, so a new instance must be created (Response B). A is wrong because you cannot remove the original elastic network interface. C is not possible. D is wrong because the OS has no ability to affect the AWS assigned IP addresses.

QUESTION NO: 333

A user is collecting 1000 records per second. The user wants to send the data to CloudWatch using a custom namespace. Which of the below mentioned options is recommended for this activity?

A.
Aggregate the data with statistics, such as Min, max, Average, Sum and Sample data and send the data to CloudWatch

B.
Send all the data values to CloudWatch in a single command by separating them with a comma. CloudWatch will parse automatically

C.
It is not possible to send all the data in one call. Thus, it should be sent one by one. CloudWatch will aggregate the data automatically

D.
Create one csv file of all the data and send a single file to CloudWatch

Answer: A

Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. The user can publish data to CloudWatch as single data points or as an aggregated set of data points called a statistic set using the command put-metric-data. It is recommended that when the user is having multiple data points per minute, he should aggregate the data so that it will minimize the number of calls to put-metric-data. In this case it will be single call to CloudWatch instead of 1000 calls if the data is aggregated.

Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/publishingMetrics.html

QUESTION NO: 334

A user is having data generated randomly based on a certain event. The user wants to upload that data to CloudWatch. It may happen that event may not have data generated for some period due to randomness.

Which of the below mentioned options is a recommended option for this case?

A.
For the period when there is no data, the user should not send the data at all

B.
The user must upload the data to CloudWatch as having no data for some period will cause an error at CloudWatch monitoring

C.
For the period when there is no data the user should send the value as 0

D.
For the period when there is no data the user should send a blank value

Answer: C

Explanation:

AWS CloudWatch supports the custom metrics. The user can always capture the custom data and upload the data to CloudWatch using CLI or APIs. When the user data is more random and not generated at regular intervals, there can be a period which has no associated data. The user can either publish the zero (0) value for that period or not publish the data at all. It is recommended that the user should publish zero instead of no value to monitor the health of the application. This is helpful in an alarm as well as in the generation of the sample data count.

Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/publishingMetrics.html

QUESTION NO: 335

A user has enabled detailed CloudWatch monitoring with the AWS Simple Notification Service. Which of the below mentioned statements helps the user understand detailed monitoring better?

A.
SNS cannot provide data every minute

B.
There is no need to enable since SNS provides data every minute

C.
SNS will send data every minute after configuration

D.
AWS CloudWatch does not support monitoring for SNS

Answer: A

Explanation:

CloudWatch is used to monitor AWS as well as the custom services. It provides either basic or detailed monitoring for the supported AWS products. In basic monitoring, a service sends data points to CloudWatch every five minutes, while in detailed monitoring a service sends data points to CloudWatch every minute. The AWS SNS service sends data every 5 minutes. Thus, it supports only the basic monitoring. The user cannot enable detailed monitoring with SNS.

Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/supported_services.html

QUESTION NO: 336

A user is trying to send custom metrics to CloudWatch using the PutMetricData APIs. Which of the below mentioned points should the user needs to take care while sending the data to CloudWatch?

A.
The size of a request is limited to 128KB for HTTP GET requests and 64KB for HTTP POST requests

B.
The size of a request is limited to 40KB for HTTP GET requests and 8KB for HTTP POST requests

C.
The size of a request is limited to 16KB for HTTP GET requests and 80KB for HTTP POST requests

D.
The size of a request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests

Answer: D

Explanation:

With AWS CloudWatch, the user can publish data points for a metric that share not only the same time stamp, but also the same namespace and dimensions. CloudWatch can accept multiple data points in the same PutMetricData call with the same time stamp. The only thing that the user needs to take care of is that the size of a PutMetricData request is limited to 8KB for HTTP GET requests and 40KB for HTTP POST requests.

Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html

QUESTION NO: 337

What is the maximum number of CloudTrails that you can create per AWS region?

A.
10

B.
2

C.
16

D.
5

Answer: D

Explanation:

You can create up to five CloudTrails per Amazon AWS region. A trail that applies to all regions exists in each region and is counted as one trail in each region.

Reference: https://aws.amazon.com/cloudtrail/faqs/

QUESTION NO: 338

An AWS account owner has setup multiple IAM users. One of these IAM users, named John, has CloudWatch access, but no access to EC2 services. John has setup an alarm action which stops EC2 instances when their CPU utilization is below the threshold limit. When an EC2 instance's CPU Utilization rate drops below the threshold John has set, what will happen and why?

A.
Nothing will happen. John cannot set an alarm on EC2 since he does not have the permission.

B.
CloudWatch will stop the instance when the action is executed

C.
Nothing will happen because it is not possible to stop the instance using the CloudWatch alarm

D.
Nothing will happen. John can setup the action, but it will not be executed because he does not have EC2 access through IAM policies.

Answer: D

Explanation:

Amazon CloudWatch alarms watch a single metric over a time period that the user specifies and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The user can setup an action which stops the instances when their CPU utilization is below a certain threshold for a certain period of time. The EC2 action can either terminate or stop the instance as part of the EC2 action. If the IAM user has read/write permissions for Amazon CloudWatch but not for Amazon EC2, he can still create an alarm. However, the stop or terminate actions will not be performed on the Amazon EC2 instance.

Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingAlarmActions.html

QUESTION NO: 339

You are architecting your e-business application for PCI compliance. To meet the compliance requirements, you need to monitor web application logs to identify any malicious activity. You also need to monitor for remote attempts to change the network interface of web instances.

Which two AWS services will be helpful to achieve this goal?

A.
Amazon CloudWatch Logs and VPC Flow Logs

B.
AWS CloudTrail and VPC Flow Logs

C.
AWS CloudTrail and CloudWatch Logs

D.
AWS CloudTrail and AWS Config

Answer: C

Explanation:

Web application logs are internal to the operating system, so the only way to monitor them with an AWS service is to export them using CloudWatch Logs. AWS CloudTrail monitors the API activity and can be used to watch for particular API calls. The correct answer is the only one that references both these services.

QUESTION NO: 340

You have an application that is processing confidential data. The data is currently stored in your data center. You are moving workloads to AWS, and you need to ensure confidentiality and integrity of the data in transit to your VPC. Your company has an existing AWS Direct Connect connection.

What combination of steps should you perform to set up the most cost-effective connection between your on-premises data center and AWS? (Choose three.)

A.
Set up a VPC with a virtual private gateway.

B.
Set up a VPC with an Internet gateway.

C.
Configure a public virtual interface on your Direct Connect connection.

D.
Configure a private virtual interface to the virtual private gateway.

E.
Set up an IPsec tunnel between your customer gateway and a software VPN on Amazon EC2 in the VPC.

F.

Set up an IPsec tunnel between your customer gateway appliance and the virtual private gateway.

Answer: A,C,F

Explanation:

Setting up a VPN over your Direct Connect connection will secure the data in transit. The steps to do so are: adding a VGW to the VPC; setting up a public virtual interface; and creating the IPsec tunnel between your data center and the VGW via the public virtual interface. B would send traffic over the public Internet. D is not possible because a public virtual interface is needed to announce the VGW endpoint IPs. E would not take advantage of the already existing Direct Connect connection.

QUESTION NO: 341

You are deploying a web application in a VPC that requires SSL mutual authentication with a client- side, smartcard-stored certificate. The ELB Classic Load Balancer listener must support mutual authentication between the client and the application.

Which load balancer protocol should you select for this application?

A.
HTTP

B.
HTTPS

C.
SSL

D.
TCP

Answer: D

Explanation:

An ELB Classic Load Balancer cannot validate a client side certificate, so it must be passed through as standard TCP on port 443 to let the EC2 instance handle the validation.

QUESTION NO: 342

Use ___________ to get more visibility into the health of your AWS Elastic Beanstalk application and take appropriate actions in case of hardware failure or performance degradation.

A.
Amazon Elastic Beanstalk command line

B.
Amazon EC2 log files

C.
Amazon CloudWatch

D.
Amazon Load balancing

Answer: C
Explanation:

In AWS Elastic Beanstalk, you can use Amazon CloudWatch to get more visibility into the health of your AWS Elastic Beanstalk application and take appropriate actions in case of hardware failure or performance degradation.

Reference: http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts.concepts.design.html

QUESTION NO: 343

To directly manage your CloudTrail security layer, you can use ____ for your CloudTrail log files

A.
SSE-S3

B.
SCE-KMS

C.
SCE-S3

D.
SSE-KMS

Answer: D

Explanation:

By default, the log files delivered by CloudTrail to your bucket are encrypted by Amazon server-side encryption with Amazon S3-managed encryption keys (SSE-S3). To provide a security layer that is directly manageable, you can instead use server-side encryption with AWS KMS-managed keys (SSE-KMS) for your CloudTrail log files.

Reference: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html

QUESTION NO: 344

Which of the following statements is true of AWS Elastic Beanstalk?

A.
AWS Elastic Beanstalk uses CloudWatch for monitoring and alarms, meaning CloudWatch costs are applied to your AWS account for any alarms that you use.

B.
AWS Elastic Beanstalk uses CloudWatch for monitoring and alarms, and both are free of charge.

C.
AWS Elastic Beanstalk doesn't use CloudWatch for monitoring and alarms, but you pay extra for any AWS Elastic Beanstalk Alarm you set in the monitoring tool.

D.
AWS Elastic Beanstalk has its own free-of-charge monitoring tool, and you are not charged for the alarm you set.

Answer: A

Explanation:

AWS Elastic Beanstalk uses CloudWatch for monitoring and alarms, meaning CloudWatch costs are applied to your AWS account for any alarms that you use.

Reference: http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.alarms.html

QUESTION NO: 345

Which of the following services is used to send an alert from CloudWatch?

A.
AWS SNS

B.
AWS EBS

C.
AWS SES

D.
AWS SQS

Answer: A

Explanation:

AWS Auto Scaling and Simple Notification Service (SNS) work in conjunction with CloudWatch. You use Amazon SNS with CloudWatch to send messages when an alarm threshold has been reached.

Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/related_services.html

QUESTION NO: 346

To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use ____.

A.
trusted signers

B.
optimistic locking

C.
integrity validation

D.
root credentialing

Answer: C

Explanation:

The AWS CloudTrail uses log file integrity validation to determine whether the log files were changed or modified since CloudTrail delivered them to an Amazon S3 bucket.

Reference: https://aws.amazon.com/cloudtrail/

QUESTION NO: 347

An AWS CloudTrail log file provides the identity and source IP address of the API caller, and a time of the API call, request parameters, and ____.

A.
response elements

B.
event selectors

C.
port alarms

D.
destination buckets

Answer: A

Explanation:

An AWS CloudTrail log file provide the following details.

Reference: https://aws.amazon.com/cloudtrail/

QUESTION NO: 348

What does the term "statistics" mean with respect to CloudWatch metrics?

A.

Time of a metric collection

B.
Data aggregation over a specific period of time

C.
Status of a metric

D.
Unit of a metric

Answer: B
Explanation:

Statistics represents data aggregation of the metric data values over a specific period of time.

Reference:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/cloudwatch_concepts.html#Statistic

QUESTION NO: 349

You wish to host a mailserver on an EC2 instance. What two steps must you take to ensure utmost reliability?

A.
Create an EIP for the instance.

B.
Configure the mail service to serve as an open relay.

C.
Contact AWS to have a Reverse DNS record configured and to help keep your domain from SPAM blacklists.

D.
Provide open security group access to your instance on ports 25, 3389 and 22.

Answer: A,C
Explanation:

Using an open relay is bad. Your security group does not require 3389 or 22 to be open.