Amazon

Exam Questions AWS-Certified-Advanced-Networking-Specialty

Amazon AWS Certified Advanced Networking - Specialty

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
A company has two AWS accounts: one for Production and one for Connectivity. A network engineer needs to connect the Production account VPC to a transit gateway in the Connectivity account. The feature to auto accept shared attachments is not enabled on the transit gateway.
Which sot of stops should the network engineer follow in each AWS account to meet those requirements?

A. * 1. In the Production account Create a resource share In AWS Resource Access Manager for the transit gateway Provide the Connectivity account ID Enable thefeature to allow external accounts* 2. In the Connectivity account Accept the resource* 3. In the Connectivity account Create an attachment to the VPC subnets* 4. In the Production account: Accept the attachmen
B. Associate a route table with the attachment.
C. * 1. In the Production account Create a resource share In AWS Resource Access Manager for the VPC subnets Provide the Connectivity account ID Enable the feature to allow external accounts.* 2. In the Connectivity account Accept the resource* 3. In the Production account Create an attachment on the transit gateway to the VPC subnets* 4. In the Connectivity account Accept the attachment Associate a route table will the attachment.
D. * 1. In the Connectivity account Create a resource share in AWS Resource Access Manager for the VPC subnet
E. Provide the Production account ID Enable the feature lo allow external accounts.* 2. In the Production account Accept the resource* 3. In the Connectivity account Create an attachment on the transit gateway to the VPC subnets A In the Production account Accept the attachment Associate a route table with the attachment.
F. * 1. In the Connectivity account Create a resource share in AWS Resource Access Manager for the transit gateway Provide the Production account ID Enable the feature to allow external accounts* 2. In the Production account Accept the resource.* 3 In the Production account Create an attachment to the VPC subnets* 4. In the Connectivity account Accept the attachmen
G. Associate a route tab e win toe attachment

Answer: A

NEW QUESTION 2
A company has an application running on Amazon EC2 instances in a VPC The application must publish custom metrics to Amazon CloudWatch in the same AWS Region The metrics include proprietary information All connectivity must be over private IP addresses.
Which solution will meet these requirements'?

A. Connect to CloudWatch through a NAT gateway
B. Connect to CloudWatch through a gateway endpoint
C. Connect to CloudWatch through an internet gateway
D. Connect to CloudWatch through an interface endpoint

Answer: D

NEW QUESTION 3
A company has a hybrid environment across its on-premises network and the AWS Cloud The company wants to use Amazon Elastic File System (Amazon EFS) to store and share data between on-premises services that are required to resolve DNS queries through on-premises DNS servers The company wants to use a custom domain name to connect to Amazon EFS The company also wants to avoid using the Amazon EFS target IP address.
What should a network engineer do to meet these requirements?

A. Create an Amazon Route 53 Resolver outbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 public hosted zone, and add a new CNAME record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 public hosted zone
B. Create an Amazon Route 53 Resolver inbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 private hosted zone, and add a new CNAME record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 Resolver
C. Create an Amazon Route 53 Resolver outbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 private hosted zone,and add a new CNAME record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 Resolver
D. Create an Amazon Route 53 Resolver inbound endpoint and configure it for the VPC where Amazon EFS resides Create a Route 53 private hosted zone, and add a new PTR record with the value of the Amazon EFS DNS name Configure forwarding rules on the on-premises DNS servers to forward queries for the custom domain host to the Route 53 private hosted zone

Answer: A

NEW QUESTION 4
A logistics company has deployed a hybrid environment that has multiple VPCs in both the us-east-1 Region and the af-south-1 Region The on-premises data center is connected to us-east-1 through an AWS Direct Connect connection The Direct Connect connection is connected to a Direct Connect gateway that is associated with a transit gateway The transit gateway is attached to all the VPCs in us-east-1
An application that is deployed in af-south-1 requires access to a database in the data center The application also requires access to file storage in a VPC in us-east-1
Which solution will meet these requirements with the LOWEST latency?

A. Create a transit gateway in af-south-1, and attach the VPCs Create a transit gateway peering connection between the transit gateways
B. Create a Direct Connect connection in af-south-1, and attach the VPCs with a Direct Connect gateway and a transit gateway Create an AWS Site-to-Site VPN connection over the internet between the Direct Connect connections.
C. Create a transit gateway in af-south-1 and attach the VPCs Associate the transit gateway in af-south-1 with the Direct Connect gateway tn us-east-1
D. Create inter-Region VPC peering connections between the VPCs in each Region Use the transit gateway attachments in us-east-1 to access the database in the data center

Answer: A

NEW QUESTION 5
A company wants to enforce a compliance requirement that its Amazon EC2 instances use only on-premises DNS servers tor name resolution Outbound DNS requests lo all other name servers must be denied. A network engineer configures the following set of outbound rules for a security group.

Type	Protocol	Port Range	Destination
DNS (UDP)	UDP	53	10.200.120.5/32
DNS (UDP)	UDP	53	10.200.120.6/32
DNS (TCP)	TCP	53	10.200.120.6/32
DNS (TCP)	TCP	53	10.200.120.5/32
HTTPS	TCP	443	0.0.0.0/0

The network engineer discovers that the EC2 instances are still able to resolve DNS requests by using Amazon DNS servers inside the VPC Why is the solution tailing to meet the compliance requirement9

A. The security group cannot filter outbound traffic to the Amazon DNS servers
B. The security group must have inbound rules to prevent DNS requests from coming back to EC2 instances.
C. The EC2 instances are using the HTTPS port to send DNS queries to Amazon DNS servers
D. The security group cannot filter outbound traffic to destinations within the same VPC

Answer: A

NEW QUESTION 6
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: A

NEW QUESTION 7
A company has deployed a production environment in the AWS Cloud The environment is contained in a VPC and includes a virtual private gateway The company has established an AWS Direct Connect connection which includes a private virtual interface (VIF) and a VPN connection to the on-premises data center
For traffic originating in the VPC what is the order of BGP path selection from MOST preferred to LEAST preferred?

A. Direct Connect BGP routes static routes longest prefix match, VPN BGP routes
B. Static routes longest prefix match Direct Connect BGP route
C. VPN BGP routes
D. Longest prefix match static routes Direct Connect BGP routes VPN BGP routes
E. Longest prefix match VPN BGP routes, static route
F. Direct Connect BGP routes

Answer: B

NEW QUESTION 8
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: C

Explanation:
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#proxy-proto

NEW QUESTION 9
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: AD

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

NEW QUESTION 10
A company wants to migrate its workloads to the AWS Cloud. The company has two web applications and wants to run them in separate, isolated VPCs. The company needs to use Elastic Load Balancing to distribute requests between application instances.

For security reasons, internet gateways must not be attached to the application VPCs. Inbound HTTP requests to the application must be routed through a centralized VPC. and the application VPCs must not be exposed to any other inbound traffic The application VPCs cannot be allowed to initiate any outbound connections
What should a network engineer do to meet these requirements?

A. Run the applications behind private Application Load Balancers (ALBs) in separate VPC
B. Create a public Network Load Balancer (NLB) in the centralized VP
C. Create target groups for the private DNS names of the ALBs Configure host-based routing to route application traffic to the corresponding target group through the NLB.
D. Run the applications behind private Application Load Balancers (ALBs) in separate VPC
E. Create a public Network Load Balancer (NLB) in the centralized VP
F. Create target groups for the private IP addresses of the ALBs Configure host-based routing to route application traffic to the corresponding target group through the NLB.
G. Run the applications behind private Network Load Balancers (NLBs) in separate VPC
H. Create VPC peering connections between the application VPCs and the centralized VP
I. Create a public Application Load Balancer (ALB) in the centralized VP
J. Create target groups for the private DNS names of the NLB
K. Configure host-based routing to route application traffic between individual applications though the ALB.
L. Run the applications behind private Network Load Balancers (NLBs) inseparate VPC
M. Configure each NLB as an AWS PrivateLink endpoint service with associated VPC endpoints in the centralized VPC Create target groups that include the private IP addresses of each endpoin
N. Create a public Application Load Balancer (ALB) in the centralized VP
O. Configurehost-based routing to route application traffic to the corresponding target group through the ALB.

Answer: D

NEW QUESTION 10
A company's application runs in a VPC and stores sensitive data in Amazon S3 The application's Amazon EC2 instances are located in a private subnet with a NAT gateway deployed in a public subnet to provide access to Amazon S3 The S3 bucket is located in the same AWS Region as the EC2 instances The company wants to ensure that this bucket can be accessed only from the VPC where the application resides
Which changes should a network engineer make to the architecture to meet these requirements?

A. Delete the existing S3 bucket and create a new S3 bucket inside the VPC in the private subnet Configure the S3 security group to allow only the application instances to access the bucket
B. Deploy an S3 VPC endpoint in the VPC where the application resides Configure an S3 bucket policy with a condition to allow access only from the VPC endpoint
C. Configure an S3 bucket policy, and use an IP address condition to restrict access to the bucket Allow access only from the VPC CIDR range, and deny all other IP address ranges
D. Create a new 1AM role for the EC2 instances that provides access to the S3 bucket and assign the role to the application instances Configure an S3 bucket policy to allow access only from the role

Answer: B

NEW QUESTION 14
A company runs a large-scale application on a feel of Amazon EC2 instances that ate distributed across several VPCs A Network Load Balancer (NLB) in a separate VPC routes traffic to the EC2 instances The NLB's VPC is peered to all the application VPCs
The application must process millions of requests each minute during times of peak utilization Users are reporting that the connections to the application are failing during peak times Monitoring shows an increase in port allocation errors on the NLB.
Which action will solve this issue with the LEAST change to the architecture?

A. Increase the number of EC2 instances in the target group
B. Create an Application Load Balancer for the target group
C. Add a new target group to the same NLB listener
D. Change the target group type to 'instance"

Answer: C

NEW QUESTION 17
A company has established an AWS Direct Connect connection between its customer gateway at its on-premises data center and a virtual private gateway m the AWS Cloud The BGP routing protocol
configuration includes the Autonomous System Number {ASN) of 7224 on the AWS end of the connection
and the BGP ASN of 65004 on the company end of the connection
The company's IT administrators report that servers that run at the on-premises data center are not able to
communicate with the company's web application that runs on a fleet of Amazon EC2 Instances A network engineer performs initial troubleshooting The network engineer finds that the private VIF is operational and that there is a fully established BGP peering session However, the company still cannot route traffic over the private VIF
Which of the following is a possible cause of this connectivity issue?

A. Firewall or ACL rules are blocking TCP pod 179 or are blocking high-numbered ephemeral TCP pons
B. The provider is advertising 50 prefixes for private VIFs
C. VPC route tables am lacking prefixes that point to the virtual private gateway to which the private VIF is connected
D. Peer IP addresses for both sides of the BGP peering session are not configured correctly.

Answer: A

NEW QUESTION 22
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: C

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/control-routes-direct-connect/

NEW QUESTION 24
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 privatesubnets, each with a route to a different NAT gateway.

Answer: CE

NEW QUESTION 29
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: A

Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#

NEW QUESTION 32
A company is deploying a critical application on two Amazon EC2 instances in a VPC Failed client connections to the EC2 instances must be logged according to company policy.
What is the MOST cost-effective solution to meet these requirements'?

A. Move the EC2 instances to a dedicated VPC Enable VPC Flow Logs with a filter on the deny action Publish the flow logs to Amazon CloudWatch Logs
B. Move the EC2 instances to a dedicated VPC subnet Enable VPC Flow Logs for the subnet with a filter on the reject action Publish the flow logs to an Amazon Kinesis Data Firehose stream with a data delivery to an Amazon S3 bucket
C. Enable VPC Flow Logs, filtered for rejected traffic for the elastic network interfaces associated with the instances Publish the flow logs to an Amazon Kinesis Data Firehose stream with a data delivery to an Amazon S3 bucket
D. Enable VPC Flow Logs, filtered for rejected traffic for the elastic network interfaces associated with the instances Publish the flow logs to Amazon CloudWatch Logs

Answer: D

NEW QUESTION 34
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: D

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

NEW QUESTION 39
A company uses multiple AWS accounts within AWS Organizations and has services deployed in a single AWS Region. The instances in a private subnet occasionally download patches from the internet through a NAT gateway The company recently migrated from VPC peering to AWS Transit Gateway The cumulative traffic through deployed NAT gateways Is less than 1Gbps The NAT gateway hourly charge contributes to most of the NAT gateway costs across all linked accounts.

What should the company do to reduce NAT gateway hourly costs?

A. Deploy and use NAT gateways in the same Availability Zone as the heavy-traffic resources.
B. Move to a centralized NAT gateway architecture with NAT gateways deployed in an egress VPC Use VPC peering to send traffic through the centralized NAT gateways.
C. Use VPC endpoints to send traffic to AWS services in the same Region.
D. Move to a centralized NAT gateway architecture with NAT gateways deployed in an egress VPC Use AWS Transit Gateway to send traffic through the centralized NAT gateways.

Answer: B

NEW QUESTION 40
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 accoun
B. Attach one private VIF per VPC.
C. Create a public VIF on the Direct Connect connectio
D. Leverage the public VIF to create a VPN connection to each VPC.
E. Create hosted private VIFs in the existing accoun
F. Connect a private VIF to an AWS Direct Connect gateway in each accoun
G. Connect the gateway in each account to the VPCs.
H. 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:
https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html

NEW QUESTION 43
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 Consol
D. Type in the CIDR blocks for the VPC and subnets.
E. Create the VPCs using AWS CLI and use the dry-run flag to validate if the current CIDR range is in use.

Answer: A

NEW QUESTION 47
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: D

NEW QUESTION 48
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

NEW QUESTION 53
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: B

NEW QUESTION 57
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

NEW QUESTION 61
You have a global corporate network with 153 individual IP prefixes in your internal routing table. You establish a private virtual interface over AWS Direct Connect to a VPC that has an Internet gateway (IGW). All instances in the VPC must be able to route to the Internet via an IGW and route to the global corporate network via the VGW.
How should you configure your on-premises BGP peer to meet these requirements?

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

Answer: B

NEW QUESTION 64
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: B

NEW QUESTION 68
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 VG
B. Use this routing table across all subnets in your VPC.
C. Configure two routing tables: one that has a default route via the IGW, and another that has a default route via the VG
D. Associate both routing tables with each VPC subnet.
E. Configure a single routing table with a default route via the IG
F. Propagate a default route via BGP on the AWS Direct Connect customer route
G. Associate the routing table with all VPC subnet.
H. Configure a single routing table with a default route via the IG
I. Propagate specific routes for theon-premises networks via BGP on the AWS Direct Connect customer route
J. Associate the routing table with all VPC subnets.

Answer: D

NEW QUESTION 71
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: D

NEW QUESTION 73
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: B

NEW QUESTION 77
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: B

Explanation:
https://blog.cloudthat.com/configuring-vpn-between-the-vpcs-across-regionsaccounts/

NEW QUESTION 78
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: C

Explanation:
https://docs.aws.amazon.com/vpc/latest/peering/create-vpc-peering-connection.html#create-vpc-peering-connec

NEW QUESTION 83
A company is building a hybrid PCI-DSS compliant application that runs in the us-west-2 Region and
on-premises. The application sends access logs from all locations to a single Amazon S3 bucket in us-west-2 To protect this sensitive data, the bucket policy is configured to deny access from public IP addresses
How should an engineer configure the network to meet these requirements?

A. Configure an AWS Direct Connect private virtual interface to the company's AWS VPC in us-west-2 Create a VPC endpoint and configure the on-premises systems to leverage an HTTPS proxy in the VPC to access Amazon S3
B. Configure a VPN connection to the company's AWS VPC in us-west-2 and use BGP to advertise routes for Amazon S3
C. Configure a Direct Connect connection public virtual interface to us-west-2 Leverage an on-premises HTTPS proxy to send traffic to Amazon S3 over a Direct Connect connection
D. Configure a VPN connection to the company's AWS VPC in us-west-2 Create a NAT gateway and configure the on-premises systems to leverage an HTTPS proxy in the VPC to access Amazon S3

Answer: C

NEW QUESTION 87
A VPC is deployed with a 10 0 0.0/16 CIDR block. The engineering team is reviewing DHCP options and there is disagreement about the valid DNS addresses available for the VPC Which addresses are valid IP addresses provided by Amazon for this subnet' (Select TWO.)

A. 8.8.8.8
B. 10.00.2
C. 10.1.0.2
D. 169.254.169.253
E. 169.254.169.254

Answer: BE

NEW QUESTION 88
A company uses an AWS Site-to-Site VPN to connect its corporate network The company recently added an AWS Direct Connect connection A network engineer wants all traffic to use the Direct Connect connection and for the VPN to be used as backup However after the Direct Connect connection was added traffic continued to pass through the VPN connection
What should the network engineer do to route the traffic through the Direct Connect connection'?

A. Add routes to the VPC route tables that specify the Direct Connect connection
B. Set local preference BGP community tags on the on-premises router
C. Advertise the same network routes over the Direct Connect connection and VPN connection
D. Ensure the Direct Connect connection AS_PATH is longer than the VPN connection AS_PATH

Answer: C

NEW QUESTION 91
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

NEW QUESTION 96
All IP addresses within a 10.0.0.0/16 VPC are fully utilized with application servers across two Availability Zones. The application servers need to send frequent UDP probes to a single central authentication server on the Internet to confirm that is running up-to-date packages. The network is designed for application servers to use a single NAT gateway for internal access. Testing reveals that a few of the servers are unable to communicate with the authentication server.

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

Answer: C

Explanation:
Ref: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
"A NAT gateway can support up to 55,000 simultaneous connections to each unique destination. This limit also applies if you create approximately 900 connections per second to a single destination (about 55,000 connections per minute). If the destination IP address, the destination port, or the protocol (TCP/UDP/ICMP) changes, you can create an additional 55,000 connections. For more than 55,000 connections, there is an increased chance of connection errors due to port allocation errors. These errors can be monitored by viewing the ErrorPortAllocation CloudWatch metric for your NAT gateway. For more information, see Monitoring NAT Gateways Using Amazon CloudWatch."

NEW QUESTION 98
An organization processes consumer information submitted through its website. The organization’s security policy requires that personally identifiable information (PII) elements are specifically encrypted at all times and as soon as feasible when received. The front-end Amazon EC2 instances should not have access to decrypted PII. A single service within the production VPC must decrypt the PII by leveraging an iAM role.
Which combination of services will support these requirement? (Select two.)

A. Amazon Aurora in a private subnet
B. Amazon CloudFront using AWS Lambda@Edge
C. Customer-managed MySQL with Transparent Data Encryption
D. Application Load Balancer using HTTPS listeners and targets
E. AWS Key Management Services

Answer: BE

NEW QUESTION 100
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: D

Explanation:
https://cloakable.irdeto.com/2017/10/11/how-to-implement-vpc-peering-between-2-vpcs-in-the-same-aws-accou

NEW QUESTION 102
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: A

Explanation:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-dhcp-options.html

NEW QUESTION 105
A company wants to use thin clients running virtual desktops to replace 500 desktop computers used by its call center employees The company is evaluating Amazon Workspaces as a solution
A network engineer who is testing with a thin client is unable to conned to Amazon Workspaces After entering credentials the network engineer receives the following error:
"An error occurred while launching your Workspace Please try again" What should the network engineer do to resolve this issue?

A. Update the inbound rules on the network ACL on the subnets used for Amazon Workspaces to allow UDP on port 4172 and TCP on port 4172
B. Update the company's corporate firewall to allow outbound access to UDP on port 4172 and TCP on port 4172 Open inbound ephemeral ports explicitly to allow return communication
C. Update the inbound rules on the security group assigned to Amazon Workspaces to allow UDP on port 4172 and TCP on port 4172
D. Update the company's corporate firewall to allow inbound access to UDP on port 4172 and TCP on port 4172 Open outbound ephemeral ports explicitly to allow return communication

Answer: C

NEW QUESTION 110
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 subnetWeb: /26 per subnet
B. Network Load Balancer: /28 per subnetWeb: /25 per subnet
C. Network Load Balancer: /28 per subnetWeb: /27 per subnet
D. Network Load Balancer: /28 per subnetWeb: /26 per subnet

Answer: D

NEW QUESTION 112
A company has a hybrid architecture with dual AWS Direct Connect connections and applications running in the AWS Cloud and on premises The company uses its on-premises DNS servers to provide name resolution tor its internal domain company com The company uses an Amazon Route 53 private hosted zone, aws company com for resolution of AWS resource records
A new application that runs on Amazon EC2 in the company's VPC needs to resolve records in the company.com domain and on other AWS resources
What should the company do to meet these requirements?

A. Create a new DHCP options set Configure the DHCP options set name servers to be the on-premises DNS servers, and configure the domain name to be company com Assign the DHCP options set to the VPC with the EC2 instances
B. Create Route 53 Resolver outbound endpoints in each subnet in the VPC Configure a Route 53 forwarding rule with a rule type of Forward for company com that points to the on-premises DNS servers Configure a Route 53 forwarding rule with a rule type of System for aws company com
C. Create Route 53 Resolver outbound endpoints in each subnet in the VPC Configure conditional forwarding rules on the on-premises DNS servers to forward queries for the domain aws company com to the Route 53 Resolver endpoints Modify the DHCP options set to configure instances to resolve hostnames using the on-premises DNS servers
D. Create a private hosted zone for company com within the AWS account Create Route 53 Resolver inbound endpoints in each subnet in the VPC Configure the on-premises DNS servers to send outbound zone transfers for company com to the Route 53 Resolver endpoints

Answer: C

NEW QUESTION 117
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

NEW QUESTION 119
A legacy, on-premises web application cannot be load balances effectively. There are both planned and unplanned events that cause usage spikes to millions of concurrent users. The existing infrastructure cannot handle the usage spikes. The CIO has mandated that the application be moved to the cloud to avoid further disruptions, with the additional requirement that source IP addresses be unaltered to support network traffic-monitoring needs. Which of the following designs will meet these requirements?

A. Use an Auto Scaling group of Amazon EC2 instances behind a Classic Load Balancer.
B. Use an Auto Scaling group of EC2 instances in a target group behind an Application Load Balancer.
C. Use an Auto Scaling group of EC2 instances in a target group behind a Classic Load Balancer.
D. Use an Auto Scaling group of EC2 instances in a target group behind a Network Load Balancer.

Answer: D

Explanation:
NLBs are highly scalable AND also preserve the source IP address. https://aws.amazon.com/elasticloadbalancing/features/

NEW QUESTION 123
A company's network engineer needs to evaluate and monitor DNS traffic The company uses Amazon Route 53 as the DNS service for its public hosted zone All DNS queries must be captured for future analysis.
What should the network engineer do to meet these requirements?

A. Use AWS WAF to log information to Amazon CloudWatch Logs about the queries that Route 53 receives
B. Use VPC Flow Logs to log information to Amazon CloudWatch Logs Insights about the queries that Route 53 receives
C. Use Route 53 query logging to log information to Amazon CloudWatch Logs about the queries that Route 53 receives
D. Use AWS CloudTrail to log information to Amazon CloudWatch Logs Insights about the queries that Route 53 receives

Answer: A

NEW QUESTION 124
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

NEW QUESTION 129
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 tableAPIs.
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.

Answer: C

Explanation:
https://aws.amazon.com/blogs/aws/subscribe-to-aws-public-ip-address-changes-via-amazon-sns/

NEW QUESTION 134
A customer is using ABC Telecom as a network provider. The customer has 10 different offices connected to ABC Telecom’s MPLS backbone. The customer is setting up an AWS Direct Connect connection to AWS and has provided the LOA-CFA to ABC Telecom. ABC Telecom has terminated the Direct Connect circuit into their MPLS backbone. To uniquely identify the customer’s traffic over the MPLS backbone, the customer must encapsulate all traffic with VLAN tag 100. The customer wants to send traffic to multiple VPCs.
Which two steps should be taken to meet the customer’s requirement? (Select two.)

A. The customer performs Q-in-Q tunneling, with the AWS-required VLAN tag in the inside and VLAN 100 as the outside tag.
B. Create a support ticket with AWS to request the removal of the outer VLAN tag 100 as the traffic reaches AWS routers.
C. Send the traffic for all VPCs with the same VLAN tag 100 and use BGP to ensure that proper routing takes place to the appropriate VPC.
D. ABC Telecom removes the other tag before sending the packet to AWS.
E. ABC Telecom creates a support ticket with AWS to exchange MPLS labels and include the AWS port as part of their MPLS network.

Answer: AD

NEW QUESTION 137
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

NEW QUESTION 142
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

NEW QUESTION 145
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: A

NEW QUESTION 149
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: A

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

NEW QUESTION 150
You have a three-tier web application with separate subnets for Web, Applications, and Database tiers. Your CISO suspects your application will be the target of malicious activity. You are tasked with notifying the security team in the event your application is port scanned by external systems.
Which two AWS Services cloud you leverage to build an automated notification system? (Select two.)

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

Answer: BD

Explanation:
References:
https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-specific-apis-are-called-by-using-aws-cloudt

NEW QUESTION 154
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. in front
What ELB configuration complies with the corporate encryption policy?

A. Configure the ELB load balancer protocol as HTT
B. Configure the application instances for SSL terminatio
C. Configure Amazon RDS for SSL, and use REQUIRE SSL grants.
D. Configure the ELB protocols in TCP mod
E. Configure the application instances for SSL termination.Configure Amazon RDS for SSL, and use REQUIRE SSL grants.

F. Configure the ELB load balancer protocol as HTTP
G. Offload application instance encryption to the load balance
H. Install your SSL certificate on Amazon RDS, and configure SSL.
I. Configure the ELB protocols in SSL mod
J. Offload application instance encryption to the load balancer.Install your SSL/TLS certificate on Amazon RDS, and configure SSL.

Answer: B

Explanation:
Refer: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-listener-config.html

NEW QUESTION 157
An AWS CloudFormation template is being used to create a VPC peering connection between two existing operational VPCs, each belonging to a different AWS account. All necessary components in the 'Remote' (receiving) account are already in place.
The template below creates the VPC peering connection in the Originating account. It contains these components:
AWSTemplateFormation Version: 2010-09-09 Parameters:
Originating VCId: Type: String RemoteVPCId: Type: String
RemoteVPCAccountId: Type: String Resources:
newVPCPeeringConnection:
Type: 'AWS::EC2::VPCPeeringConnection' Properties:
VpcdId: !Ref OriginatingVPCId PeerVpcId: !Ref RemoteVPCId PeerOwnerId: !Ref RemoteVPCAccountId
Which additional AWS CloudFormation components are necessary in the Originating account to create an operational cross-account VPC peering connection with AWS CloudFormation? (Select two.)

A. Resources:NewEC2SecurityGroup:Type: AWS::EC2::SecurityGroup
B. Resources:NetworkInterfaceToRemoteVPC:Type: "AWS::EC2NetworkInterface"
C. Resources:newEC2Route:Type: AWS::EC2::Route
D. Resources:VPCGatewayToRemoteVPC:Type: "AWS::EC2::VPCGatewayAttachment"
E. Resources:newVPCPeeringConnection:Type: 'AWS::EC2VPCPeeringConnection'PeerRoleArn: !Ref PeerRoleArn

Answer: CE

Explanation:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/AWS_EC2.html

NEW QUESTION 161
A Lambda function needs to access the private address of an Amazon ElastiCache cluster in a VPC. The Lambda function also needs to write messages to Amazon SQS. The Lambda function has been configured to run in a subnet in the VPC.
Which of the following actions meet the requirements? (Select two.)

A. The Lambda function needs an IAM role to access Amazon SQS
B. The Lambda function must route through a NAT gateway or NAT instance in another subnet to access the public SQS API.
C. The Lambda function must be assigned a public IP address to access the public Amazon SQS API.
D. The ElastiCache server outbound security group rules must be configured to permit the Lambda function's security group.
E. The Lambda function must consume auto-assigned public IP addresses but not elastic IP addresses.

Answer: AB

Explanation:
https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html https://docs.aws.amazon.com/lambda/latest/dg/vpc.html

NEW QUESTION 166
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

NEW QUESTION 168
.....

Relate Links

100% Pass Your AWS-Certified-Advanced-Networking-Specialty Exam with Exambible Prep Materials

https://www.exambible.com/AWS-Certified-Advanced-Networking-Specialty-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/