
# Amazon

## Exam Questions AWS-Certified-Advanced-Networking-Specialty

Amazon AWS Certified Advanced Networking - Specialty

**NEW QUESTION 1**
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 tie
B. Set session stickiness on both, but update the application code to create an application-controlled cookie on the Classic Load Balancer.
C. Use an Application Load Balancer at both the web and application tiers, setting session stickiness at the target group level for both tiers.
D. Deploy a web node and an application node as separate containers on the same host, using task linking to create a relationship between the pai
E. Add an Application Load Balancer with session stickiness in front of all web node containers.
F. 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:** A

**NEW QUESTION 2**
You are deploying an EC2 instance in a private subnet that requires access to the Internet. One of the requirements for this solution is to restrict access to only particular URLs on a whitelist. In addition to the whitelisted URL, the instances should be able to access any Amazon S3 bucket in the same region via any URL.
Which of the following solutions should you deploy? (Select two.)

A. Include s3.amazonaws.com in the whitelist.
B. Create a VPC endpoint for S3.
C. Run Squid proxy on a NAT instance.
D. Deploy a NAT gateway into your VPC.
E. Utilize a security group to restrict access.

**Answer:** BC

**Explanation:**
https://aws.amazon.com/blogs/security/how-to-set-up-an-outbound-vpc-proxy-with-domain-whitelisting-and-co

**NEW QUESTION 3**
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:** D

**NEW QUESTION 4**
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

**NEW QUESTION 5**
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:** C

**NEW QUESTION 6**
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 7**
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 8**
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 9**
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 10**
An organization will be extending its existing on-premises infrastructure into the cloud. The design consists of a transit VPC that contains stateful firewalls that will be deployed in a highly available configuration across two Availability Zones for automatic failover.

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

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

**Answer:** BC

**Explanation:**
https://docs.aws.amazon.com/solutions/latest/cisco-based-transit-vpc/appendix-a.html

**NEW QUESTION 10**
You are designing an AWS Direct Connect solution into your VPC. You need to consider requirements for the customer router to terminate the Direct Connect link at the Direct Connect location.
Which three factors that must be supported should you consider when choosing the customer router? (Select three.)

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

**Answer:** ADE

**Explanation:**
https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html#overview_requirements

**NEW QUESTION 12**
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 13**
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:** AC

**NEW QUESTION 16**
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:** A

**Explanation:**
https://docs.aws.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.html

**NEW QUESTION 19**
A financial services company receives real-time stock quotes in its ingestion VPC. The company plans to perform customer-specific data analysis on the stock quotes in various VPCs. The stock quotes must be distributed simultaneously from Amazon EC2 instances in the ingestion VPC to EC2 instances in the data analysis VPCs

Which set of configuration steps should the company lake to meet these requirements?

A. Configure EC2 instances m f he ingestion VPC as IP unicast senders Configure a transit gateway to serve as a unicast router for instances that send traffic destined for the EC2 instances in the data analysis VPCs.
B. Configure VPC peering between the ingestion VPC and the data analysis VPCs Configure an Application Load Balancer to distribute Virtual Extensible LAN (VXLAN)-encapsulated traffic from the sender EC2 instances to the receiver EC2 instances.
C. Configure EC2 instances m the ingestion VPC as IP multicast senders Configure a transit gateway to serve as a multicast router for instances that send traffic destined for the EC2 instances m the data analysis VPCs
D. Configure Amazon Kinesis Data Forehose to capture streaming data from the ingestion VPC and load the data into Amazon S3 Configure the instances in the data analysis VPCs to download the data from Amazon S3 for processing

**Answer:** D

**NEW QUESTION 23**
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 26**
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:** A

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

**NEW QUESTION 31**
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 34**
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 reques
D. Later, cut over from the VPN connection to one or more Direct Connect connections, as needed.
E. Provision a 100 Mbps AWS Direct Connect connection between an Amazon VPC and the data center, then submit a Direct Connect connection reques
F. Later, cut over from the hosted connection to one or more Direct Connect connections, as needed.

**Answer:** C

**NEW QUESTION 35**
A company with several VPCs in the us-east-1 Region wants to reduce the cost of its workloads A network engineer has identified that all traffic bound to Amazon services is flowing through a NAT gateway. Additionally, all the VPCs are peered to a hub VPC for access to common services.

A. Disable the private DNS name for the SQS endpoin
B. Create an Amazon Route 53 private hosted zone for the domain us-east-1.sqs.amazonaws.co
C. Create a CNAME record to the DNS name of the SQS endpoint Share the private hosted zone with ail other VPCs
D. Disable the private DNS name for the SOS endpoin
E. Create an Amazon Route 53 private hosted zone for the domain sqs.us-east-1 .amazonaws.co
F. Create an alias record to the DNS name of the SOS endpoin
G. Share the private hosted zone with all other VPCs
H. Enable the private DNS name for the SOS endpoint Create an Amazon Route 53 private hosted zone for the domain SQS.us-east-t.amazonaws.co
I. Create a CNAME record to the DNS name of the SQS endpoin
J. Share the private hosted zone with all other VPCs.
K. Enable the private DNS name for the SQS endpoin
L. Create an Amazon Route 53 private hosted zone for the domain us-east-1 .sqs.amazonaws.co
M. Create an alias record to the DNS name of the SQS endpoin
N. Share the private hosted zone with all other VPCs.

**Answer:** A

**NEW QUESTION 37**
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:** C

**NEW QUESTION 41**
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 46**
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:** C

**NEW QUESTION 49**
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

**NEW QUESTION 52**
Your organization requires strict adherence to a change control process for its Amazon Elastic Compute Cloud (EC2) and VPC environments. The organization uses AWS CloudFormation as the AWS service to control and implement changes. Which combination of three services provides an alert for changes made outside of AWS CloudFormation? (Select three.)

A. AWS Config

B. AWS Simple Notification Service
C. AWS CloudWatch metrics
D. AWS Lambda
E. AWS CloudFormation
F. AWS Identify and Access Management

**Answer:** ABD

**Explanation:**
aws.amazon.com/about-aws/whats-new/2018/03/aws-config-notifications-are-now-integrated-with-amazon-clou

**NEW QUESTION 54**
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 subnet
B. Enable VPC Flow Logs with a filter set to AL
C. Create an Amazon CloudWatch Logs filter on the VPC Flow Logs log group filtered by REJEC
D. Create an alarm for this metric to notify the Security team.
E. Enable Amazon GuardDuty on the account and the specific regio
F. Upload a list of allowed IPs to Amazon S3 and link the S3 object to the GuardDuty trusted IP lis
G. Configure an Amazon CloudWatch Events rule on all GuardDuty findings to trigger an Amazon SNS notification to the Security team.
H. Add allowed IPs to the network ACL for the application server subnet
I. Enable VPC Flow Logs with a filter set to REJEC
J. Set an Amazon CloudWatch Logs filter for the log group on every even
K. Create an alarm for this metric to notify the Security team.
L. Enable Amazon GuardDuty on the account and specific regio
M. Upload a list of allowed IPs to Amazon S3 and link the S3 object to the GuardDuty threat IP lis
N. Integrate GuardDuty with a compatible SIEM to report on every alarm from GuardDuty.

**Answer:** C

**NEW QUESTION 56**
A company has a VPC in the us-west-1 Region and another VPC in the ap-southeast-2 Region Network engineers set up an AWS Direct Connect connection from their data center to the us-east-1 Region They create a private virtual interface (VIF) that references a Direct Connect gateway, which is then connected to virtual private gateways in both VPCs When the setup is complete, the engineers cannot access resources in us-west-1 from ap-southeast-2
What should the network engineers do to resolve this issued

A. Add the subnet range for the VPCs in us-west-1 and ap-southeast-2 to the route tables for both VPCs Add the Direct Connect gateway as a target
B. Configure the Direct Connect gateway to route traffic between the VPCs in ap-southeast-2 and us-west-2
C. Establish a VPC peering connection between the VPCs in ap-southeast-2 and us-west-2 Add the subnet ranges to the routing tables
D. Create static routes in each VPC that point to the destination VPC with the virtual private gateway as the route target

**Answer:** A

**NEW QUESTION 59**
A company wants to migrate its production and development applications to the AWS Cloud across multiple VPCs in three AWS Regions us-east-1 (N Virginia), eu-west-1 (Ireland), and ap-southeast-1 (Singapore) The company needs a scalable solution that provides connectivity between all three Regions The solution also must provide private connectivity to the company's on-premises data center in Northern Virginia Data that is transferred from on premises and data that is transferred between Regions must be encrypted in transit The company requires predictable network performance and must minimize cost
The company has initiated a solution by deploying a transit gateway with two route tables in each Region One route table is for the production environment, and one route table is for the development environment
What else must the company do to meet its requirements with the LOWEST latency?

A. Deploy an AWS Direct Connect connection in us-east-1 and a public VIF to the on-premises data center On each transit gateway, create a VPN attachment over the public VIF for the production and development route tables Create transit gateway peennng connections to route traffic between Regions
B. Deploy an AWS Direct Connect connection in us-east-1 and a transit VIF to the on-premises data center Associate all transit gateways and the transit VIF with a different Direct Connect gatewa
C. Create transit gateway peering connections to route traffic between Regions
D. Deploy an AWS Direct Connect connection in us-east-1 and a public VIF to the on-premises data center.On each transit gateway, create a VPN attachment over the public VIF for the production and development route table
E. Route traffic between Regions through the VPN connections.
F. Deploy an AWS Direct Connect connection in us-east-1 to the on-premises data center Create one transit VIF for each transit gateway route table, and associate each transit VIF with a Direct Connect gateway Associate all transit gateways with the Direct Connect gateway Create transit gateway peering connections to route traffic between Regions.

**Answer:** B

**NEW QUESTION 64**
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 65**
A company has Iwo on-premises data center locations. There is a company-managed router at earn data center. Each data center has a dedicated AWS Direct Connect connection to a Direct Connect gateway through a private virtual interface The router for the first location is advertising 110 routes to the Direct Connect gateway by using BGP and the router tor the second location is advertising 60 routes to the Direct Connect gateway by using BGP The Direct Connect gateway is attached to a company VPC through a virtual private gateway
A network engineer receives reports that resources In the VPC are not reachable from various locations in either data center. The network engineer checks the VPC route table and sees that the routes from the first data center. location are not being populated into the route table The network engineer must resolve this issue in the most operationally efficient manner
What should the network engineer do to meet these requirements'

A. Remove the Direct Connect gateway, and create a new private virtual interface from each company router to the virtual private gateway of the VPC
B. Change the router configurations to summarize the advertised routes
C. Open a support ticket to increase the quota on advertised routes to the VPC route table
D. Create an AWS Transit Gateway Attach the transit gateway to the VPC and connect the Direct Connect gateway to the transit gateway.

**Answer:** D

**NEW QUESTION 70**
An organization launched an IPv6-only web portal to support IPv6-native mobile clients. Front-end instances launch in an Amazon VPC associated with an appropriate IPv6 CIDR. The VPC IPv4 CIDR is fully utilized. A single subnet exists in each of two Availability Zones with appropriately configured IPv6 CIDR associations. Auto Scaling is properly configured, and no Elastic Load Balancing is used.
Customers say the service is unavailable during peak load times. The network engineer attempts to launch an instance manually and receives the following message: “There are not enough free addresses in subnet ‘subnet-12345677’ to satisfy the requested number of instances.”
What action will resolve the availability problem?

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

**Answer:** B

**NEW QUESTION 71**
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 73**
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 75**

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:** D

**Explanation:**
https://aws.amazon.com/premiumsupport/knowledge-center/elb-capture-client-ip-addresses/

**NEW QUESTION 79**
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:** CD

**NEW QUESTION 81**
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 83**
A company uses a newly provisioned 1-Gbps AWS Direct Connect connection to configure a virtual interface for access to Amazon S3
Which configuration values is the network engineer required to provide? (Select TWO.)

A. Connection speed
B. VLAN ID
C. IP prefixes to advertise
D. Direct Connect location
E. Virtual private gateway

**Answer:** BE

**NEW QUESTION 87**
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 91**
An organization runs a consumer-facing website on AWS. The Amazon EC2-based web fleet is load balanced using the AWS Application Load Balancer, Amazon Route 53 is used to provide the public DNS services.
The following URLs need to server content to end users: test.example.com
web.example.com example.com
Based on this information, what combination of services must be used to meet the requirement? (Select two.)

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

**Answer:** BC

**Explanation:**
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#rule-condition
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html

**NEW QUESTION 94**
Your company has set up AWS Direct Connect to connect on-premises to an Amazon VPC instance. Two Direct Connect connections terminate at two different Direct Connect locations. You are using two routers, R1 and R2, at your end (one of each Direct Connect connection). R1 and R2 do NOT have connectivity between them. Both routers advertise the same routers over BGP to the VGW. You have a stateful firewall on each router. The routers drop some of the traffic coming from the VPC.
Which two actions should you take to fix this problem? (Select two.)

A. Use BGP AS prepend attribute to prepend additional AS numbers while advertising routers from R1 to VGW.
B. Use BGP local preference attribute to assign R1 to a lower local preference number than R2.
C. Use BGP local preference attribute to assign R1 a higher local preference number than R2.
D. Use BGP MED attribute to assign a higher MED value to the routes advertised R1 to VGW.
E. Use BGP MED attribute to assign a higher MED value to the routes advertised from R2 to VGW.

**Answer:** AD

**NEW QUESTION 97**
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 connectivit
B. Upload it to the AWS Management Console when creating a new Direct Connect connectio
C. AWS will ensure that the cross-connect is installed.
D. Obtain the LOA/CFA from the AWS Management Console when ordering the Direct Connect connectio
E. Provide it to the APN Partner when ordering connectivit
F. The Direct Connect partner will ensure that the cross-connect is installed.
G. Obtain the LOA/CFA each from the AWS Management Console and the APN Partne
H. Provide both tothe Facility Operator of the Direct Connect locatio
I. The Facility Operator will ensure that the cross-connect is installed.
J. Identify the APN Partner in the AWS Management Console when creating the Direct Connect connectio
K. Provide the resulting Connection ID to the APN Partner, who will ensure that the cross-connect is installed.

**Answer:** B

**NEW QUESTION 99**
A bank built a new version of its banking application in AWS using containers that content to an on-premises database over VPN connection. This application version requires users to also update their client application. The bank plans to deprecate the earlier client version. However, the company wants to keep supporting earlier clients through their on-premises version of the application to serve a small portion of the customers who haven't yet upgraded.
What design will allow the company to serve both newer and earlier clients in the MOST efficient way?

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

**Answer:** D

**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 106**
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 107**
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 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:** C

**Explanation:**
https://aws.amazon.com/es/premiumsupport/knowledge-center/virtual-interface-bgp-down/

**NEW QUESTION 117**
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 VP
B. Point the on-premises forwarder to the proxy resolver.
C. Modify the network access control list on the VPC to allow DNS queries from on-premises systems.
D. Configure the on-premises server as a secondary DNS for the private zon
E. Update the NS records.
F. Update the on-premises forwarders with the four name servers assigned to the private hosted zone.

**Answer:** A

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

**NEW QUESTION 121**
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 VP
C. Set up a stream of the flow logs to a central Amazon Elasticsearch cluster.
D. Enable Amazon Macie on each AWS account and configure central reporting.
E. 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-acc

**NEW QUESTION 125**
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:** B

**NEW QUESTION 127**
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 129**
A company installed an AWS Site-to-Site VPN and configured it to use two tunnels The company has learned that the VPN connectivity is unstable During a ping test from the on-premises data center to AWS: a network engineer notices that the first few ICMP replies time out but that subsequent requests are successful The AWS Management Console shows that the status for both tunnels last changed at the same time the ping responses were successfully received
Which steps should the network engineer take to resolve the instability*? (Select TWO )

A. Enable dead peer detection (DPD) on the customer gateway device
B. Change the tunnel configuration to active/standby on the virtual private gateway
C. Use AS PATH prepending on one path to cause all traffic to prefer that tunnel
D. Send ICMP requests to an instance in the VPC every 5 seconds from the on-premises network
E. Use a higher multi-exit discriminator (MED) value on the preferred path to prefer that tunnel

**Answer:** CE

**NEW QUESTION 131**
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 133**
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 136**
A company recently migrated its Amazon EC2 instances to VPC private subnets to satisfy a security compliance requirement. The EC2 instances now use a NAT gateway tor internet access After the migration, some long-running database queries from private EC2 instances to a publicly accessible third-party database no longer receive responses The database query logs reveal that the queries successfully completed after 7 minutes but that the client EC2 instances never received the response.
Which configuration change should a network engineer implement to resolve this issue''

A. Configure the NAT gateway timeout to allow connections for up to 600 seconds
B. Enable enhanced networking on the client EC2 instances
C. Enable TCP keepalive on the client EC2 instances with a value of less than 300 seconds
D. Close idle TCP connections though the NAT gateway

**Answer:** C

**NEW QUESTION 141**
An organization delivers high-resolution, dynamic web content. Internet users access the content from a variety of platforms, including mobile, tablet and desktop. Each platform receives a customized experience to account for the differences in viewing modes. A dedicated, automatic-scaling fleet of Amazon EC2 instances is used for each platform to server content based on path-based headers.
Which combination of services will MINIMIZE cost and MAXIMIZE performance? (Select two.)

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

**Answer:** AE

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

**NEW QUESTION 143**
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 148**
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 149**
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:** B

**Explanation:**
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html#vpc-endpoints-policies-s3

**NEW QUESTION 150**
.....

# Thank You for Trying Our Product

## We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

## AWS-Certified-Advanced-Networking-Specialty Practice Exam Features:

* AWS-Certified-Advanced-Networking-Specialty Questions and Answers Updated Frequently

* AWS-Certified-Advanced-Networking-Specialty Practice Questions Verified by Expert Senior Certified Staff

* AWS-Certified-Advanced-Networking-Specialty Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AWS-Certified-Advanced-Networking-Specialty Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year