

Exam Questions AWS-Certified-Advanced-Networking-Specialty

Amazon AWS Certified Advanced Networking - Specialty

<https://www.2passeasy.com/dumps/AWS-Certified-Advanced-Networking-Specialty/>



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 set of steps 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 the feature 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 attachment
- 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 with 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 to 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 attachment
- G. Associate a route table with the 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 wants to enforce a compliance requirement that its Amazon EC2 instances use only on-premises DNS servers for name resolution Outbound DNS requests to 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 failing to meet the compliance requirement?

- 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 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

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 6

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 7

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 8

A company is migrating a legacy storefront web application to the AWS Cloud. The application is complex and will take several months to refactor. A solutions architect recommended an interim solution of using Amazon CloudFront with a custom origin pointing to the SSL endpoint URL for the legacy web application until the replacement is ready and deployed. The interim solution has worked for several weeks. However, all browser connections recently began showing an HTTP 502 Bad Gateway error with the header "X-Cache-Error from cloudfront". Monitoring services show that the HTTPS port 443 on the legacy web application is open and responding to requests. What is the likely cause of the error and what is the solution?

- A. The origin access identity is not correct. Edit the CloudFront distribution and update the identity in the origins settings.
- B. The SSL certificate on the CloudFront distribution has expired. Use AWS Certificate Manager (ACM) in the us-east-1 Region to replace the SSL certificate in the CloudFront distribution with a new certificate.
- C. The SSL certificate on the legacy web application server has expired. Use AWS Certificate Manager (ACM) in the us-east-1 Region to create a new SSL certificate. Export the public and private keys and install the certificate on the legacy web application.
- D. The SSL certificate on the legacy web application server has expired. Replace the SSL certificate on the web server with one signed by a globally recognized certificate authority (CA). Install the full certificate chain onto the legacy web application server.

Answer: A

NEW QUESTION 9

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 10

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 VPC 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 10

An insurance company is planning the migration of workloads from its on-premises data center to the AWS Cloud The company requires end-to-end domain name resolution Bidirectional DNS resolution between AWS

and the existing on-premises environments must be established The workloads will be migrated into multiple VPCs. The workloads also have dependencies on each other, and not all the workloads will be migrated at the same time

Which solution meets these requirements? Which solution meets these requirements?

- A. Configure a private hosted zone for each application VPC, and create the requisite records Create a set of Amazon Route 53 Resolver inbound and outbound endpoint In an egress VPC Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver Associate the application VPC private hosted zones with the egress VPC and share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manage
- B. Configure the on premises DNS servers to forward the cloud domains to the Route 53 inbound endpoint.
- C. Configure a public hosted zone for each application VPC and create the requisite records Create a set of Amazon Route 53 Resolver Inbound and outbound endpoints in an egress VP
- D. Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver Associate the application VPC private hosted zones with the egress VPC and share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manager Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoints.
- E. Configure a private hosted zone for each application VPC, and create the requisite records Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPC Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolve
- F. Associate the application VPC private hosted zones with the egress VPC and share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manage
- G. Configure the on-premises DNS servers to forward the cloud domains to the Route 53 outbound endpoint.
- H. Configure a private hosted zone for each application VPC, and create the requisite records Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPC Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver Associate the Route 53 outbound rules with the application VPCs and share the private hosted zones with the application accounts by using AWS Resource Access Manager Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoint.

Answer: B

NEW QUESTION 15

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 20

A company uses AWS Direct Connect to connect its corporate network to multiple VPCs in the same AWS account and the same AVVS Region Each VPC uses its own private VIF and its own virtual LAN on the Direct Connect connection The company has grown and will soon surpass the limit of VPCs and private VIFs for each connection

What is the MOST scalable way to add VPCs with on-premises connectivity?

- A. Provision a new Direct Connect connection to handle the additional VPCs Use the new connection to connect additional VPCs.
- B. Create virtual private gateways for each VPC that is over the service quota Use AWS Site-to-Site VPN to connect the virtual private gateways to the corporate network
- C. Create a Direct Connect gateway, and add virtual private gateway associations to the VPC
- D. Configure a private VIF to connect to the corporate network
- E. Create a transit gateway and attach the VPCs Create a Direct Connect gateway, and associate it with the transit gateway Create a transit VIF to the Direct Connect gateway

Answer: D

NEW QUESTION 23

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 endpoint
- 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 endpoint
- 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 endpoint

- 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 endpoint
- J. Share the private hosted zone with all other VPCs.
- K. Enable the private DNS name for the SQS endpoint
- 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 endpoint
- N. Share the private hosted zone with all other VPCs.

Answer: A

NEW QUESTION 28

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 31

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 36

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 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 42

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

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

- C. Use the VPC wizard in the AWS Management Console
- 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 43

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 47

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 issue?

- 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 50

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 VPC's 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 55

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

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

- A. The VGW is not advertising the correct CIDR range back on-premises.
- B. The instance security group does not allow ICMP traffic.
- C. A public virtual interface must be configured for Amazon EC2 connectivity.
- D. The on-premises router is not advertising the correct CIDR range to AWS.
- E. There is a misconfiguration of the bi-directional forwarding detection.

Answer: BD

NEW QUESTION 56

A financial company is designing a secure AWS network architecture to support a hybrid cloud strategy. Systems deployed in the AWS Cloud are mission critical and have strict availability requirements. The

company anticipates the need for hundreds of VPCs. Instances will be transient and rely heavily on DNS resolution. The applications must be designed to have Availability Zone isolation and tolerate the loss of an Availability Zone.

What is the MOST reliable way to implement DNS in this scenario?

- A. Create a new DHCP options set with DNS settings with on-premises DNS servers that traverse an AWS Direct Connect connection.
- B. Create private hosted zones and share them with each VPC.
- C. Use Amazon Route 53 Resolver for hybrid DNS.
- D. Modify the default DHCP options set with a fleet of proxy DNS servers that are deployed in each VPC.
- E. Create a fleet of DNS proxy servers in a central VPC.
- F. Share the proxy fleet with each VPC using AWS PrivateLink.

Answer: C

NEW QUESTION 59

A company's developers wrote an AWS Lambda function to modify existing private route tables in response to a security appliance's auto scaling events. The Lambda function will be invoked on lifecycle hooks for an Auto Scaling group and is configured to run in a VPC. The developers are unsure if the following IAM

policy provides sufficient permissions to be used as an execution role for this Lambda function.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "ec2:CreateRoute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource": "*"
    }
  ]
}
```

The developers ask a network engineer to review the permissions.
 Which set of permissions should the network engineer add to the policy?

- A. lambda
- B. ListFunctions, lambda:GetPolicy, and ec2 Delete RouteTable
- C. ec2:AssociateAddress, ec2 ModifyInstanceAttribut
- D. and ec2 AssociateRouteTable
- E. ec2:CreateNetworkIntertace ec2 DeleteNetworkInterface, and ec2 ReplaceRoute
- F. ec2:Describei.ifecydoHooks, ec2 DescribeScalingActivities, and ec2 DescribePolicies

Answer: C

NEW QUESTION 61

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. 10.0.0.2
- C. 10.1.0.2
- D. 169.254.169.253
- E. 169.254.169.254

Answer: BE

NEW QUESTION 65

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 70

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 71

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

- A. Configure IAM user policies to lock down permissions for specific user
- B. Enable AWS CloudTrail to identify API calls from user
- C. Use AWS Config to audit any changes, and configure Amazon SNS to send notifications.
- D. Configure IAM user policies to lock down permissions for specific user
- E. Enable AWS CloudTrail to identify the API calls from user
- F. Configure AWS CodeCommit to audit any changes in configurations, and configure Amazon SNS to send notifications.

- G. Configure IAM user policies to lock down permissions for specific user
- H. Enable AWS CloudTrail to identify the API calls from user
- I. Configure Amazon Macie to use machine learning to identify any configuration changes, and configure Amazon SNS to send notifications.
- J. Configure IAM role policies to lock down permissions for specific user
- K. Configure Amazon GuardDuty to audit and monitor configuration changes, and configure Amazon SNS to send notifications.

Answer: A

NEW QUESTION 73

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 to the 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 74

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 78

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

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

- A. 33.17.0.0/16
- B. 172.16.0.0/18
- C. 100.70.0.0/17
- D. 192.168.1.0/24
- E. 10.0.0.0/8

Answer: AC

NEW QUESTION 79

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 83

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 connect 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 87

A Network Engineer needs to be automatically notified when a certain TCP port is accessed on a fleet of Amazon EC2 instances running in an Amazon VPC. Which of the following is the MOST reliable solution?

- A. Create an inbound rule in the VPC's network ACL that matches the TCP port.
- B. Create an Amazon CloudWatch alarm on the NetworkPackets metric for the ACL that uses Amazon SNS to notify the Administrator when the metric is greater than zero.
- C. Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to notify the Administrator with Amazon SNS each time the TCP port is accessed.
- D. Create VPC Flow Logs that write to Amazon CloudWatch Logs, with a metric filter matching connections on the required port.
- E. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.
- F. Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to publish to a custom Amazon CloudWatch metric each time the TCP port is accessed.
- G. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.

Answer: A

NEW QUESTION 88

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

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

- A. Attach the virtual private gateway to a VPC and enable route propagation.
- B. Filter the public IP prefixes 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 92

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 95

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

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

Answer: AE

Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/active-passive-direct-connect/>

NEW QUESTION 99

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

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

Which configuration change should you make to address this issue?

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

Answer: A

Explanation:

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

NEW QUESTION 102

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

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

Answer: D

NEW QUESTION 104

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

- A. Use a Classic Load Balancer and upload the client certificate private keys to it
- B. Perform SSL mutual authentication of the client-side certificate there.
- C. Use a Network Load Balancer with a TCP listener on port 443, and pass the request through for the SSL mutual authentication to be handled by a backend instance.
- D. Use an Application Load Balancer and upload the client certificate private keys to it by using the native server name indication (SNI) features with smart certificate selection to handle multiple calling applications.
- E. Front the application with Amazon API Gateway, and use its client-side SSL mutual authentication feature that uses the backend instances to verify the source of the request.

Answer: B

NEW QUESTION 105

A network architect is designing an internet website. It has web, application, and database tiers that will run in AWS. The website uses Amazon DynamoDB. Which architecture will minimize public exposure of the back-end instances?

- A. A VPC with public subnets for the NLB, public subnets for the web tier, private subnets for the application tier, and private subnets for DynamoDB.
- B. A VPC with public subnets for the ALB, private subnets for the web tier, and private subnets for the application tier
- C. The application tier connects DynamoDB through a VPC endpoint.
- D. A VPC with public subnets for the ALB, public subnets for the web tier, private subnets for the application tier, and private subnets for DynamoDB.
- E. A VPC with public subnets for the NLB, private subnets for the web tier, and public subnets for the application tier
- F. The application tier connects DynamoDB through a VPC endpoint.

Answer: B

NEW QUESTION 107

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 for 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 through the NAT gateway

Answer: C

NEW QUESTION 111

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 116

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

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

Answer: BE

Explanation:

References: <https://aws.amazon.com/directconnect/faqs/>

NEW QUESTION 118

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AWS-Certified-Advanced-Networking-Specialty Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AWS-Certified-Advanced-Networking-Specialty Product From:

<https://www.2passeasy.com/dumps/AWS-Certified-Advanced-Networking-Specialty/>

Money Back Guarantee

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