

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

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

Answer: A

NEW QUESTION 2

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 template 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 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

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 5

A company hosts several applications in the AWS Cloud across multiple VPCs that are connected to a transit gateway. Redundant AWS Direct Connect connections and a Direct Connect gateway provide private network connectivity to the company's on-premises environment.

During a maintenance window, the networking team adds eight VPCs. The application management team notices that there is no reachability between the newly created VPCs and the on-premises environment. Connectivity between all VPCs through the transit gateway is working as expected.

Which of the following are possible causes of the connectivity issues? (Choose TWO)

- A. The prefixes that are advertised from the Direct Connect gateway to the on-premises router are shorter than the CIDR blocks of the newly created VPCs
- B. The route tables for the newly created
- C. VPCs do not have the routes to the on-premises environment that point to the transit gateway attachment
- D. The on-premises route tables do not contain the exact CIDR blocks of the newly created VPCs
- E. The route tables (or the newly created VPCs have only summary routes for the on-premises environment (that point to the transit gateway attachment.
- F. The prefixes that are advertised from the Direct Connect gateway to the on-premises router do not contain the CIDR blocks of the newly created VPCs

Answer: AD

NEW QUESTION 6

You have to set up an AWS Direct Connect connection to connect your on-premises to an AWS VPC. Due to budget requirements, you can only provision a single Direct Connect port. You have two border gateway routers at your on-premises data center that can peer with the Direct Connect routers for redundancy. Which two design methodologies, in combination, will achieve this connectivity? (Select two.)

- A. Terminate the Direct Connect circuit on a L2 border switch, which in turn has trunk connections to the two routers.
- B. Create two Direct Connect private VIFs for the same VPC, each with a different peer IP.
- C. Terminate the Direct Connect circuit on any of the one routers, which in turn will have an IBGP session with the other router.
- D. Create one Direct Connect private VIF for the VPC with two customer peer IPs.
- E. Provision two VGWs for the VPC and create one Direct Connect private VIF per VGW.

Answer: AD

Explanation:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/add-peer-to-vif.html> (Adding a BGP Peer)

NEW QUESTION 7

A manufacturing company has a hybrid environment that includes an AWS Direct Connect gateway that is associated with an AWS Transit Gateway. The company wants to extend a third-party application that is hosted in its on-premises data center into one of its VPCs.

The application vendor has stated that it must use an overlay IP address to meet the company's requirement for high availability. The DHCP administrator has assigned a non-overlapping RFC1918 private address for use as the overlay IP address. The security team requires connectivity to remain private. Which solution meets these requirements with the LEAST management overhead?

- A. Create a layer 2 VPN across a public VIF by using a software-based VPN on a pair of Amazon EC2 instances. Use BGP to advertise the routes over the VPN.
- B. Create a transit VIF with automatically propagated routes in the transit gateway route table. Create a new subnet in the VPC for the overlay IP address, and propagate the route to the VPC route table.
- C. Update the route tables on premises as needed.
- D. Create an external Network Load Balancer by using Amazon Route 53 to create records that point to the target application's overlay IP address.
- E. Create static entries in the VPC route table.
- F. Create a transit VIF. Then create static routes in the transit gateway route table to point to the VPC that contains the overlay IP address. Create static routes in the VPC route table that point to the transit gateway. Update the route tables on premises as needed.

Answer: D

NEW QUESTION 8

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 9

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 10

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

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

Answer: A

NEW QUESTION 10

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 12

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

- A. Ensure that Bidirectional Forwarding Detection is enabled on the Direct Connect connection.
- B. Confirm that the same routes are being advertised over both the VPN and Direct Connect.
- C. Reconfigure the Direct Connect session from static routes to Border Gateway Protocol (BGP) peering.
- D. Configure a virtual private gateway for the VPN and another virtual private gateway for Direct Connect.

Answer: B

NEW QUESTION 13

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.com.
- C. Create a CNAME record to the DNS name of the SQS endpoint. Share the private hosted zone with all other VPCs.
- D. Disable the private DNS name for the S3 endpoint.
- E. Create an Amazon Route 53 private hosted zone for the domain sqs.us-east-1.amazonaws.com.
- F. Create an alias record to the DNS name of the S3 endpoint.
- G. Share the private hosted zone with all other VPCs.
- H. Enable the private DNS name for the S3 endpoint. Create an Amazon Route 53 private hosted zone for the domain sqs.us-east-1.amazonaws.com.
- 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.com.
- 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 18

Your organization's corporate website must be available on www.acme.com and acme.com. How should you configure Amazon Route 53 to meet this requirement?

- A. Configure acme.com with an ALIAS record targeting the ELB.
- B. www.acme.com with an ALIAS record targeting the ELB.
- C. Configure acme.com with an A record targeting the EL.
- D. www.acme.com with a CNAME record targeting the acme.com record.
- E. Configure acme.com with a CNAME record targeting the EL.
- F. www.acme.com with a CNAME record targeting the acme.com record.

- G. Configure acme.com using a second ALIAS record with the ELB target
H. www.acme.com using a PTR record with the acme.com record target.

Answer: A

Explanation:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html>

NEW QUESTION 20

You run a well-architected, multi-AZ application in the eu-central-1 (Frankfurt) AWS region. The application is hosted in a VPC and is only accessed from the corporate network. To support large volumes of data transfer and administration of the application, you use a single 10-Gbps AWS Direct Connect connection with multiple private virtual interfaces. As part of a review, you decide to improve the resilience of your connection to AWS and make sure that any additional connectivity does not share the same Direct Connect routers at AWS. You need to provide the best levels of resilience to meet the application's needs. Which two options should you consider? (Select two.)

- A. Install a second 10-Gbps Direct Connect connection to the same Direct Connection location.
- B. Deploy an IPsec VPN over a public virtual interface on a new 10-Gbps Direct Connect connection.
- C. Install a second 10-Gbps Direct Connect connection to a Direct Connect location in eu-west-1.
- D. Deploy an IPsec VPN over the Internet to the eu-west-1 region for diversity.
- E. Install a second 10-Gbps Direct Connect connection to a second Direct Connect location for eu-central-1.

Answer: AE

Explanation:

<https://aws.amazon.com/directconnect/resiliency-recommendation/>

NEW QUESTION 21

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 26

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

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

The Engineer notices that the command output does not contain a public IP address. In the AWS Management Console, the public subnet has a route to the internet gateway. The instance also has a public IP address associated with it. What should the Engineer do next to troubleshoot this situation?

- A. Configure the public IP on the interface.
- B. Disable source/destination checking for the instance.
- C. Associate an Elastic IP address to the interface.
- D. Evaluate the security groups and the network access control list.

Answer: D

NEW QUESTION 29

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

- A. Configure a prefix list on the customer router containing the AWS IP address ranges for the specific region.
- B. Configure a filter on the company's router to only import routes with the 7224:8100 BGP community attribute.
- C. Configure a filter on the company's router to only import routes without a BGP community attribute and a maximum path length of 3.
- D. Configure a filter in the console and only allow routes advertised by AWS without a BGP community attribute and a maximum path length of 3.

Answer: B

NEW QUESTION 30

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 Identity 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 35

A department in your company has created a new account that is not part of the organization's consolidated billing family. The department has also created a VPC for its workload. Access is restricted by network access control lists to the department's on-premises private IP allocation. An AWS Direct Connect private virtual interface for this VPC advertises a default route to the company network. When the department downloads data from an Amazon Elastic Compute Cloud(EC2) instance in its new VPC, what are the associated charges?

- A. The company pays Internet Data Out charges.
- B. The company pays AWS Direct Connect Data Out charges.
- C. The department pays Internet Data Out charges.
- D. The department pays AWS Direct Connect Data Out charges.

Answer: D

NEW QUESTION 39

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 43

Your company's policy requires that all VPCs peer with a "common services: VPC. This VPC contains a fleet of layer 7 proxies and an Internet gateway. No other VPC is allowed to provision an Internet gateway. You configure a new VPC and peer with the common service VPC as required by policy. You launch an Amazon EC2. Windows instance configured to forward all traffic to the layer 7 proxies in the common services VPC. The application on this server should successfully interact with Amazon S3 using its properly configured AWS Identity and Access Management (IAM) role. However, Amazon S3 is returning 403 errors to the application.

Which step should you take to enable access to Amazon S3?

- A. Update the S3 bucket policy with the private IP address of the instance.
- B. Exclude 169.254.169.0/24 from the instance's proxy configuration.
- C. Configure a VPC endpoint for Amazon S3 in the same subnet as the instance.
- D. Update the CORS configuration for Amazon S3 to allow traffic from the proxy.

Answer: B

NEW QUESTION 45

The Web Application Development team is worried about malicious activity from 200 random IP addresses. Which action will ensure security and scalability from this type of threat?

- A. Use inbound security group rules to block the IP addresses.
- B. Use inbound network ACL rules to block the IP addresses.
- C. Use AWS WAF to block the IP addresses.
- D. Write iptables rules on the instance to block the IP addresses.

Answer: C

Explanation:

<https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html>

NEW QUESTION 48

You have multiple Amazon Elastic Compute Cloud (EC2) instances running a web server in a VPC configured with security groups and NACL. You need to ensure layer 7 protocol level logging of all network traffic (ACCEPT/REJECT) on the instances. What should be enabled to complete this task?

- A. CloudWatch Logs at the VPC level
- B. Packet sniffing at the instance level
- C. VPC flow logs at the subnet level
- D. Packet sniffing at the VPC level

Answer: B

NEW QUESTION 50

A company has two on-premises data center locations. There is a company-managed router at each 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 for 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 52

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 VPC 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 55

A company uses an Application Load Balancer (ALB) to provide access to a multi-tenant web application for 25 customers. The company creates a unique hostname for each customer to use to access the application. Hostnames use the format customer-name.example.com.

Each customer has a dedicated group of Amazon EC2 instances that run their own version of the web application. When a customer visits customer-name.example.com, the ALB should route the request to the correct group of EC2 instances. The company requires a highly available solution that is easy to maintain. Which solution meets these requirements at the LOWEST cost?

- A. Create one ALB for all customers. Create a listener rule that includes an HTTP header condition to match the URL. Add a forward action to route the request to the customer target group. Use Amazon Route 53 to create an alias record for each customer-name.example.com hostname that points to the ALB.
- B. Create one ALB for each customer. Configure the listener to route requests to the customer target group. Configure an NGINX proxy server to manage connections to each ALB. Use Amazon Route 53 to create a CNAME record for each customer-name.example.com hostname that points to the NGINX proxy server.
- C. Create one ALB for all customers. Create a listener rule that includes a Host header condition to match the hostname. Add a forward action to route the request to the customer target group. Use Amazon Route 53 to create an alias record for each customer-name.example.com hostname that points to the ALB.
- D. Create one ALB for each customer. Configure the listener to route requests to the customer target group. Create an Amazon CloudFront distribution. Add each ALB to the distribution as a custom origin. Use Amazon Route 53 to create an alias for each customer-name.example.com hostname that points to the CloudFront distribution.

Answer: A

NEW QUESTION 57

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 61

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 65

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 69

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 routes 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 routes 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 72

A bank built a new version of its banking application in AWS using containers that connect 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 application
- 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 application
- 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 application
- 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 77

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 80

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

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

- A. The security group is denying inbound ICMP.
- B. The network ACL is denying inbound ICMP.
- C. The security group is denying outbound ICMP.
- D. The network ACL is denying outbound ICMP.

Answer: D

NEW QUESTION 81

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 86

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 91

A company has an AWS Direct Connect connection between its on-premises data center and Amazon VPC. An application running on an Amazon EC2 instance in the VPC needs to access confidential data stored in the on-premises data center with consistent performance. For compliance purposes, data encryption is required.

What should the network engineer do to meet these requirements?

- A. Configure a public virtual interface on the Direct Connect connection
- B. Set up an AWS Site-to-Site VPN between the customer gateway and the virtual private gateway in the VPC.
- C. Configure a private virtual interface on the Direct Connect connection
- D. Set up an AWS Site-to-Site VPN between the customer gateway and the virtual private gateway in the VPC.
- E. Configure an internet gateway in the VPC. Set up a software VPN between the customer gateway and an EC2 instance in the VPC.
- F. Configure an internet gateway in the VPC. Set up an AWS Site-to-Site VPN between the customer gateway and the virtual private gateway in the VPC.

Answer: D

NEW QUESTION 93

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 96

You currently use a single security group assigned to all nodes in a clustered NoSQL database. Only your cluster members in one region must be able to connect to each other. This security group uses a self-referencing rule using the cluster security group's group-id to make it easier to add or remove nodes from the cluster. You need to make this database comply with out-of-region disaster recovery requirements and ensure that the network traffic between the nodes is encrypted when travelling between regions. How should you enable secure cluster communication while deploying additional cluster members in another AWS region?

- A. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group rules that reference each other's security group-id in each region.
- B. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
- C. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
- D. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group rules that reference each other's security group-id in each region.

Answer: B**NEW QUESTION 100**

An organization is using a VPC endpoint for Amazon S3. When the security group rules for a set of instances were initially configured, access was restricted to allow traffic only to the IP addresses of the Amazon S3 API endpoints in the region from the published JSON file. The application was working properly, but now is logging a growing number of timeouts when connecting with Amazon S3. No internet gateway is configured for the VPC. Which solution will fix the connectivity failures with the LEAST amount of effort?

- A. Create a Lambda function to update the security group based on AmazonIPSpaceChanged notifications.
- B. Update the VPC routing to direct Amazon S3 prefix-list traffic to the VPC endpoint using the route table APIs.
- C. Update the application server's outbound security group to use the prefix-list for Amazon S3 in the same region.
- D. Create an additional VPC endpoint for Amazon S3 in the same route table to scale the concurrent connections to Amazon.

Answer: C**Explanation:**

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

NEW QUESTION 103

A customer is using ABC Telecom as a network provider. The customer has 10 different offices connected to ABC Telecom's MPLS backbone. The customer is setting up an AWS Direct Connect connection to AWS and has provided the LOA-CFA to ABC Telecom. ABC Telecom has terminated the Direct Connect circuit into their MPLS backbone. To uniquely identify the customer's traffic over the MPLS backbone, the customer must encapsulate all traffic with VLAN tag 100. The customer wants to send traffic to multiple VPCs.

Which two steps should be taken to meet the customer's requirement? (Select two.)

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

Answer: AD**NEW QUESTION 108**

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

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

How should the engineer configure DNS to support these requirements?

- A. Use Amazon Route 53 to create a geo-based routing entry for the hostname 'app' in the DNS zone 'example.com'.
- B. Create two A record entries for 'app' in the DNS zone 'example.com' – one for the public IP and one for the private IP.
- C. Use Route 53 to create an ALIAS record to the public DNS name for the instance.
- D. Create a CNAME for 'app' in the DNS zone 'example.com' to the public DNS name for the Amazon EC2 instance.

Answer: D**NEW QUESTION 112**

Your organization needs to resolve DNS entries stored in an Amazon Route 53 private zone "awscloud:internal" from the corporate network. An AWS Direct Connect connection with a private virtual interface is configured to provide access to a VPC with the CIDR block 192.168.0.0/16. A DNS Resolver (BIND) is configured on an Amazon Elastic Compute Cloud (EC2) instance with the IP address 192.168.10.5 within the VPC. The DNS Resolver has standard root server hints configured and conditional forwarding for "awscloud.internal" to the IP address 192.168.0.2.

From your PC on the corporate network, you query the DNS server at 192.168.10.5 for www.amazon.com. The query is successful and returns the appropriate response. When you query for "server.awscloud.internal", the query times out. You receive no response.

How should you enable successful queries for "server.awscloud.internal"?

- A. Attach an internet gateway to the VPC and create a default route.
- B. Configure the VPC settings for enableDnsHostnames and enableDnsSupport as True
- C. Relocate the BIND DNS Resolver to the corporate network.
- D. Update the security group for the EC2 instance at 192.168.10.5 to allow UDP Port 53 outbound.

Answer: B

NEW QUESTION 117

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

- A. The NAT gateway does not support fragmented packets.
- B. The internet gateway only supports an MTU of 1500 bytes.
- C. An Amazon EC2 instance expects to communicate with an MTU of 9001.
- D. The security group on the instances does not allow PMTUD.

Answer: A

NEW QUESTION 118

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 121

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 124

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 128

A Network Engineer is provisioning a subnet for a load balancer that will sit in front of a fleet of application servers in a private subnet. There is limited IP space left in the VPC CIDR. The application has few users now but is expected to grow quickly to millions of users.

What design will use the LEAST amount of IP space, while allowing for this growth?

- A. Use two /29 subnets for an Application Load Balancer in different Availability Zones.
- B. Use one /29 subnet for the Network Load Balance
- C. Add another VPC CIDR to the VPC to allow for future growth.

- D. Use two /28 subnets for a Network Load Balancer in different Availability Zones.
- E. Use one /28 subnet for an Application Load Balance
- F. Add another VPC CIDR to the VPC to allow for future growth.

Answer: C

NEW QUESTION 133

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 134

You need to set up a VPN between AWS VPC and your on-premises network. You create a VPN connection in the AWS Management Console, download the configuration file, and install it on your on-premises router. The tunnel is not coming up because of firewall restrictions on your router. Which two network traffic options should you allow through the firewall? (Select two.)

- A. UDP port 500
- B. IP protocol 50
- C. IP protocol 5
- D. TCP port 50
- E. TCP port 500

Answer: AB

Explanation:

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

NEW QUESTION 136

Your security team implements a host-based firewall on all of your Amazon Elastic Compute Cloud (EC2) instances to block all outgoing traffic. Exceptions must be requested for each specific requirement. Until you request a new rule, you cannot access the instance metadata service. Which firewall rule should you request to be added to your instances to allow instance metadata access?

- A. Inbound; Protocol tcp; Source [Instance's EIP]; Destination 169.254.169.254
- B. Inbound; Protocol tcp; Destination 169.254.169.254; Destination port 80
- C. Outbound; Protocol tcp; Destination 169.254.169.254; Destination port 80
- D. Outbound; Protocol tcp; Destination 169.254.169.254; Destination port 443

Answer: C

NEW QUESTION 140

.....

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