

## Exam Questions ANS-C01

AWS Certified Advanced Networking Specialty Exam

<https://www.2passeasy.com/dumps/ANS-C01/>



### NEW QUESTION 1

A company has deployed Amazon EC2 instances in private subnets in a VPC. The EC2 instances must initiate any requests that leave the VPC, including requests to the company's on-premises data center over an AWS Direct Connect connection. No resources outside the VPC can be allowed to open communications directly to the EC2 instances.

The on-premises data center's customer gateway is configured with a stateful firewall device that filters for incoming and outgoing requests to and from multiple VPCs. In addition, the company wants to use a single IP match rule to allow all the communications from the EC2 instances to its data center from a single IP address.

Which solution will meet these requirements with the LEAST amount of operational overhead?

- A. Create a VPN connection over the Direct Connect connection by using the on-premises firewall
- B. Use the firewall to block all traffic from on premises to AW
- C. Allow a stateful connection from the EC2 instances to initiate the requests.
- D. Configure the on-premises firewall to filter all requests from the on-premises network to the EC2 instance
- E. Allow a stateful connection if the EC2 instances in the VPC initiate the traffic.
- F. Deploy a NAT gateway into a private subnet in the VPC where the EC2 instances are deployed
- G. Specify the NAT gateway type as private
- H. Configure the on-premises firewall to allow connections from the IP address that is assigned to the NAT gateway.
- I. Deploy a NAT instance into a private subnet in the VPC where the EC2 instances are deployed. Configure the on-premises firewall to allow connections from the IP address that is assigned to the NAT instance.

**Answer:** C

### NEW QUESTION 2

A company has deployed a web application on AWS. The web application uses an Application Load Balancer (ALB) across multiple Availability Zones. The targets of the ALB are AWS Lambda functions. The web application also uses Amazon CloudWatch metrics for monitoring.

Users report that parts of the web application are not loading properly. A network engineer needs to troubleshoot the problem. The network engineer enables access logging for the ALB.

What should the network engineer do next to determine which errors the ALB is receiving?

- A. Send the logs to Amazon CloudWatch Log
- B. Review the ALB logs in CloudWatch Insights to determine which error messages the ALB is receiving.
- C. Configure the Amazon S3 bucket destination
- D. Use Amazon Athena to determine which error messages the ALB is receiving.
- E. Configure the Amazon S3 bucket destination
- F. After Amazon CloudWatch Logs pulls the ALB logs from the S3 bucket automatically, review the logs in CloudWatch Logs to determine which error messages the ALB is receiving.
- G. Send the logs to Amazon CloudWatch Log
- H. Use the Amazon Athena CloudWatch Connector to determine which error messages the ALB is receiving.

**Answer:** B

#### Explanation:

Access logs is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logs for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logs at any time. <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

### NEW QUESTION 3

A company has hundreds of VPCs on AWS. All the VPCs access the public endpoints of Amazon S3 and AWS Systems Manager through NAT gateways. All the traffic from the VPCs to Amazon S3 and Systems Manager travels through the NAT gateways. The company's network engineer must centralize access to these services and must eliminate the need to use public endpoints.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a central egress VPC that has private NAT gateway
- B. Connect all the VPCs to the central egress VPC by using AWS Transit Gateway
- C. Use the private NAT gateways to connect to Amazon S3 and Systems Manager by using private IP addresses.
- D. Create a central shared services VPC
- E. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to access
- F. Ensure that private DNS is turned off
- G. Connect all the VPCs to the central shared services VPC by using AWS Transit Gateway
- H. Create an Amazon Route 53 forwarding rule for each interface VPC endpoint
- I. Associate the forwarding rules with all the VPC
- J. Forward DNS queries to the interface VPC endpoints in the shared services VPC.
- K. Create a central shared services VPC. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to access
- L. Ensure that private DNS is turned off
- M. Connect all the VPCs to the central shared services VPC by using AWS Transit Gateway
- N. Create an Amazon Route 53 private hosted zone with a full service endpoint name for Amazon S3 and Systems Manager
- O. Associate the private hosted zones with all the VPC
- P. Create an alias record in each private hosted zone with the full AWS service endpoint pointing to the interface VPC endpoint in the shared services VPC.
- Q. Create a central shared services VPC
- R. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to access
- S. Connect all the VPCs to the central shared services VPC by using AWS Transit Gateway
- T. Ensure that private DNS is turned on for the interface VPC endpoints and that the transit gateway is created with DNS support turned on.

**Answer:** B

#### Explanation:

Interface VPC endpoints enable private connectivity between VPCs and supported AWS services without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Interface VPC endpoints are powered by AWS PrivateLink, a technology that enables private access to AWS services. Amazon S3 and AWS Systems Manager support interface VPC endpoints. By turning off private DNS, the interface VPC endpoints can be accessed

by using their private IP addresses2. By using Amazon Route 53 forwarding rules, DNS queries can be resolved to the interface VPC endpoints in the shared services VPC3.

#### NEW QUESTION 4

A real estate company is building an internal application so that real estate agents can upload photos and videos of various properties. The application will store these photos and videos in an Amazon S3 bucket as objects and will use Amazon DynamoDB to store corresponding metadata. The S3 bucket will be configured to publish all PUT events for new object uploads to an Amazon Simple Queue Service (Amazon SQS) queue.

A compute cluster of Amazon EC2 instances will poll the SQS queue to find out about newly uploaded objects. The cluster will retrieve new objects, perform proprietary image and video recognition and classification update metadata in DynamoDB and replace the objects with new watermarked objects. The company does not want public IP addresses on the EC2 instances.

Which networking design solution will meet these requirements MOST cost-effectively as application usage increases?

- A. Place the EC2 instances in a public subne
- B. Disable the Auto-assign Public IP option while launching the EC2 instance
- C. Create an internet gatewa
- D. Attach the internet gateway to the VP
- E. In the public subnet's route table, add a default route that points to the internet gateway.
- F. Place the EC2 instances in a private subne
- G. Create a NAT gateway in a public subnet in the same Availability Zon
- H. Create an internet gatewa
- I. Attach the internet gateway to the VP
- J. In the public subnet's route table, add a default route that points to the internet gateway
- K. Place the EC2 instances in a private subne
- L. Create an interface VPC endpoint for Amazon SQ
- M. Create gateway VPC endpoints for Amazon S3 and DynamoDB.
- N. Place the EC2 instances in a private subne
- O. Create a gateway VPC endpoint for Amazon SQS.Create interface VPC endpoints for Amazon S3 and DynamoDB.

**Answer:** C

#### NEW QUESTION 5

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 6

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. Bi-directional 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?

- A. Configure a private hosted zone for each application VPC, and create the requisite record
- B. Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VP
- C. Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolve
- D. 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
- E. Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inboundendpoints.
- F. Configure a public hosted zone for each application VPC, and create the requisite record
- G. Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VP
- H. Define Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolve
- I. Associate the application VPC private hosted zones with the egress VP
- J. and share the Route 53 Resolver rules with the application accounts by using AWS Resource Access Manage
- K. Configure the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoints.
- L. Configure a private hosted zone for each application VPC, and create the requisite record
- M. Create a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPDefine Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolve
- N. Associate the application VPC private hosted zones with the egress VPand s

**Answer:** A

#### Explanation:

Creating a private hosted zone for each application VPC and creating the requisite records would enable end-to-end domain name resolution for the resources. Creating a set of Amazon Route 53 Resolver inbound and outbound endpoints in an egress VPC would enable bi-directional DNS resolution between AWS and the existing on-premises environments. Defining Route 53 Resolver rules to forward requests for the on-premises domains to the on-premises DNS resolver would enable DNS queries from AWS resources to on-premises resources. Associating the application VPC private hosted zones with the egress VPC and sharing the



Route 53 Resolver rules with the application accounts by using AWS Resource Access Manager would enable DNS queries among different VPCs and accounts. Configuring the on-premises DNS servers to forward the cloud domains to the Route 53 inbound endpoints would enable DNS queries from on-premises resources to AWS resources<sup>1</sup>.

#### NEW QUESTION 7

A company is deploying third-party firewall appliances for traffic inspection and NAT capabilities in its VPC. The VPC is configured with private subnets and public subnets. The company needs to deploy the firewall appliances behind a load balancer. Which architecture will meet these requirements MOST cost-effectively?

- A. Deploy a Gateway Load Balancer with the firewall appliances as target
- B. Configure the firewall appliances with a single network interface in a private subnet
- C. Use a NAT gateway to send the traffic to the internet after inspection.
- D. Deploy a Gateway Load Balancer with the firewall appliances as target
- E. Configure the firewall appliances with two network interfaces: one network interface in a private subnet and another network interface in a public subnet
- F. Use the NAT functionality on the firewall appliances to send the traffic to the internet after inspection.
- G. Deploy a Network Load Balancer with the firewall appliances as target
- H. Configure the firewall appliances with a single network interface in a private subnet
- I. Use a NAT gateway to send the traffic to the internet after inspection.
- J. Deploy a Network Load Balancer with the firewall appliances as target
- K. Configure the firewall appliances with two network interfaces: one network interface in a private subnet and another network interface in a public subnet
- L. Use the NAT functionality on the firewall appliances to send the traffic to the internet after inspection.

**Answer:** B

#### NEW QUESTION 8

A company's network engineer is designing a hybrid DNS solution for an AWS Cloud workload. Individual teams want to manage their own DNS hostnames for their applications in their development environment. The solution must integrate the application-specific hostnames with the centrally managed DNS hostnames from the on-premises network and must provide bidirectional name resolution. The solution also must minimize management overhead. Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

- A. Use an Amazon Route 53 Resolver inbound endpoint.
- B. Modify the DHCP options set by setting a custom DNS server value.
- C. Use an Amazon Route 53 Resolver outbound endpoint.
- D. Create DNS proxy servers.
- E. Create Amazon Route 53 private hosted zones.
- F. Set up a zone transfer between Amazon Route 53 and the on-premises DNS.

**Answer:** ABE

#### NEW QUESTION 9

A network engineer needs to set up an Amazon EC2 Auto Scaling group to run a Linux-based network appliance in a highly available architecture. The network engineer is configuring the new launch template for the Auto Scaling group. In addition to the primary network interface the network appliance requires a second network interface that will be used exclusively by the application to exchange traffic with hosts over the internet. The company has set up a Bring Your Own IP (BYOIP) pool that includes an Elastic IP address that should be used as the public IP address for the second network interface. How can the network engineer implement the required architecture?

- A. Configure the two network interfaces in the launch template
- B. Define the primary network interface to be created in one of the private subnets
- C. For the second network interface, select one of the public subnets
- D. Choose the BYOIP pool ID as the source of public IP addresses.
- E. Configure the primary network interface in a private subnet in the launch template
- F. Use the user data option to run a cloud-init script after boot to attach the second network interface from a subnet with auto-assign public IP addressing enabled.
- G. Create an AWS Lambda function to run as a lifecycle hook of the Auto Scaling group when an instance is launched
- H. In the Lambda function, assign a network interface to an AWS Global Accelerator endpoint.
- I. During creation of the Auto Scaling group, select subnets for the primary network interface
- J. Use the user data option to run a cloud-init script to allocate a second network interface and to associate an Elastic IP address from the BYOIP pool.

**Answer:** D

#### Explanation:

During creation of the Auto Scaling group, select subnets for the primary network interface. Use the user data option to run a cloud-init script to allocate a second network interface and to associate an Elastic IP address from the BYOIP pool.

This solution meets all of the requirements stated in the question. The primary network interface can be configured in a private subnet during creation of the Auto Scaling group. The user data option can be used to run a cloud-init script that will allocate a second network interface and associate an Elastic IP address from the BYOIP pool with it.

#### NEW QUESTION 10

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 10

A customer has set up multiple VPCs for Dev, Test, Prod, and Management. You need to set up AWS Direct Connect to enable data flow from on-premises to each VPC. The customer has monitoring software running in the Management VPC that collects metrics from the instances in all the other VPCs. Due to budget requirements, data transfer charges should be kept at minimum. Which design should be recommended?

- A. Create a total of four private VIFs, one for each VPC owned by the customer, and route traffic between VPCs using the Direct Connect link.
- B. Create a private VIF to the Management VPC, and peer this VPC to all other VPCs.
- C. Create a private VIF to the Management VPC, and peer this VPC to all other VPCs, enable source/destination NAT in the Management VPC.
- D. Create a total of four private VIFs, and enable VPC peering between all VPCs.

**Answer:** D

#### Explanation:

- creating VPC peering is free of charge - traffic costs ~0.01€/GB for VPC peering (IN + OUT) and ~0.02€/GB for direct connect (OUT only). As the communication involved in monitoring will never have IN == OUT, then 0.01 \* (IN + OUT) will always be lower than 0.02 \* OUT, ergo VPC peering will be cheaper

#### NEW QUESTION 11

A network engineer needs to update a company's hybrid network to support IPv6 for the upcoming release of a new application. The application is hosted in a VPC in the AWS Cloud. The company's current AWS infrastructure includes VPCs that are connected by a transit gateway. The transit gateway is connected to the on-premises network by AWS Direct Connect and AWS Site-to-Site VPN. The company's on-premises devices have been updated to support the new IPv6 requirements.

The company has enabled IPv6 for the existing VPC by assigning a new IPv6 CIDR block to the VPC and by assigning IPv6 to the subnets for dual-stack support. The company has launched new Amazon EC2 instances for the new application in the updated subnets.

When updating the hybrid network to support IPv6 the network engineer must avoid making any changes to the current infrastructure. The network engineer also must block direct access to the instances' new IPv6 addresses from the internet. However, the network engineer must allow outbound internet access from the instances.

What is the MOST operationally efficient solution that meets these requirements?

- A. Update the Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address
- B. Create a new VPN connection that supports IPv6 connectivity
- C. Add an egress-only internet gateway
- D. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices
- E. Update the Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address
- F. Update the existing VPN connection to support IPv6 connectivity
- G. Add an egress-only internet gateway
- H. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices.
- I. Create a Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address
- J. Create a new VPN connection that supports IPv6 connectivity
- K. Add an egress-only internet gateway
- L. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices.
- M. Create a Direct Connect transit VIF and configure BGP peering with the AWS assigned IPv6 peering address
- N. Create a new VPN connection that supports IPv6 connectivity
- O. Add a NAT gateway
- P. Update any affected VPC security groups and route tables to provide connectivity within the VPC and between the VPC and the on-premises devices.

**Answer:** B

#### NEW QUESTION 12

You deploy an Amazon EC2 instance that runs a web server into a subnet in a VPC. An Internet gateway is attached, and the main route table has a default route (0.0.0.0/0) configured with a target of the Internet gateway.

The instance has a security group configured to allow as follows:

- > Protocol: TCP
- > Port: 80 inbound, nothing outbound

The Network ACL for the subnet is configured to allow as follows:

- > Protocol: TCP
- > Port: 80 inbound, nothing outbound

When you try to browse to the web server, you receive no response. Which additional step should you take to receive a successful response?

- A. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 80
- B. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 1024-65535
- C. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 80
- D. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 1024-65535

**Answer:** D

#### Explanation:

To enable the connection to a service running on an instance, the associated network ACL must allow both inbound traffic on the port that the service is listening on as well as allow outbound traffic from ephemeral ports. When a client connects to a server, a random port from the ephemeral port range (1024-65535) becomes the client's source port. The designated ephemeral port then becomes the destination port for return traffic from the service, so outbound traffic from the ephemeral port must be allowed in the network ACL. <https://aws.amazon.com/premiumsupport/knowledge-center/resolve-connection-sg-acl-inbound/>

### NEW QUESTION 13

A company is building its website on AWS in a single VPC. The VPC has public subnets and private subnets in two Availability Zones. The website has static content such as images. The company is using Amazon S3 to store the content.

The company has deployed a fleet of Amazon EC2 instances as web servers in a private subnet. The EC2 instances are in an Auto Scaling group behind an Application Load Balancer. The EC2 instances will serve traffic, and they must pull content from an S3 bucket to render the webpages. The company is using AWS Direct Connect with a public VIF for on-premises connectivity to the S3 bucket.

A network engineer notices that traffic between the EC2 instances and Amazon S3 is routing through a NAT gateway. As traffic increases, the company's costs are increasing. The network engineer needs to change the connectivity to reduce the NAT gateway costs that result from the traffic between the EC2 instances and Amazon S3.

Which solution will meet these requirements?

- A. Create a Direct Connect private VIF
- B. Migrate the traffic from the public VIF to the private VIF.
- C. Create an AWS Site-to-Site VPN tunnel over the existing public VIF.
- D. Implement interface VPC endpoints for Amazon S3. Update the VPC route table.
- E. Implement gateway VPC endpoints for Amazon S3. Update the VPC route table.

**Answer:** D

### NEW QUESTION 18

An AWS CloudFormation template is being used to create a VPC peering connection between two existing operational VPCs, each belonging to a different AWS account. All necessary components in the 'Remote' (receiving) account are already in place.

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

AWSTemplateFormation Version: 2010-09-09 Parameters:

Originating VPCId: Type: String RemoteVPCId: Type: String

RemoteVPCAccountId: Type: String Resources:

newVPCPeeringConnection:

Type: 'AWS::EC2::VPCPeeringConnection'

Properties:

VpcId: !Ref OriginatingVPCId PeerVpcId: !Ref RemoteVPCId PeerOwnerId: !Ref RemoteVPCAccountId

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

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

**Answer:** CE

### Explanation:

[https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/AWS\\_EC2.html](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/AWS_EC2.html)

### NEW QUESTION 22

A company is deploying an application. The application is implemented in a series of containers in an Amazon Elastic Container Service (Amazon ECS) cluster.

The company will use the Fargate launch type for its tasks. The containers will run workloads that require connectivity initiated over an SSL connection. Traffic must be able to flow to the application from other AWS accounts over private connectivity. The application must scale in a manageable way as more consumers use the application.

Which solution will meet these requirements?

- A. Choose a Gateway Load Balancer (GLB) as the type of load balancer for the ECS service
- B. Create a lifecycle hook to add new tasks to the target group from Amazon ECS as required to handle scaling
- C. Specify the GLB in the service definition
- D. Create a VPC peer for external AWS account
- E. Update the route tables so that the AWS accounts can reach the GLB.
- F. Choose an Application Load Balancer (ALB) as the type of load balancer for the ECS service
- G. Create path-based routing rules to allow the application to target the containers that are registered in the target group
- H. Specify the ALB in the service definition
- I. Create a VPC endpoint service for the ALB. Share the VPC endpoint service with other AWS accounts.
- J. Choose an Application Load Balancer (ALB) as the type of load balancer for the ECS service
- K. Create path-based routing rules to allow the application to target the containers that are registered in the target group
- L. Specify the ALB in the service definition
- M. Create a VPC peer for the external AWS account
- N. Update the route tables so that the AWS accounts can reach the ALB.
- O. Choose a Network Load Balancer (NLB) as the type of load balancer for the ECS service
- P. Specify the NLB in the service definition
- Q. Create a VPC endpoint service for the NLB
- R. Share the VPC endpoint service with other AWS accounts.

**Answer:** D

### NEW QUESTION 26

A company plans to deploy a two-tier web application to a new VPC in a single AWS Region. The company has configured the VPC with an internet gateway and four subnets. Two of the subnets are public and have default routes that point to the internet gateway. Two of the subnets are private and share a route table that does not have a default route.

The application will run on a set of Amazon EC2 instances that will be deployed behind an external Application Load Balancer. The EC2 instances must not be directly accessible from the internet. The application will use an Amazon S3 bucket in the same Region to store data. The application will invoke S3 GET API operations and S3 PUT API operations from the EC2 instances. A network engineer must design a VPC architecture that minimizes data transfer cost.

Which solution will meet these requirements?



- A. Deploy the EC2 instances in the public subnet
- B. Create an S3 interface endpoint in the VP
- C. Modify the application configuration to use the S3 endpoint-specific DNS hostname.
- D. Deploy the EC2 instances in the private subnet
- E. Create a NAT gateway in the VP
- F. Create default routes in the private subnets to the NAT gatewa
- G. Connect to Amazon S3 by using the NAT gateway.
- H. Deploy the EC2 instances in the private subnet
- I. Create an S3 gateway endpoint in the VPSpecify die route table of the private subnets during endpoint creation to create routes to Amazon S3.
- J. Deploy the EC2 instances in the private subnet
- K. Create an S3 interface endpoint in the VP
- L. Modify the application configuration to use the S3 endpoint-specific DNS hostname.

**Answer: C**

**Explanation:**

Option C is the optimal solution as it involves deploying the EC2 instances in the private subnets, which provides additional security benefits. Additionally, creating an S3 gateway endpoint in the VPC will enable the EC2 instances to communicate with Amazon S3 directly, without incurring data transfer costs. This is because the S3 gateway endpoint uses Amazon's private network to transfer data between the VPC and S3, which is not charged for data transfer. Furthermore, specifying the route table of the private subnets during endpoint creation will create routes to Amazon S3, which is required for the EC2 instances to communicate with S3.

**NEW QUESTION 31**

A company has created three VPCs: a production VPC, a nonproduction VPC, and a shared services VPC. The production VPC and the nonproduction VPC must each have communication with the shared services VPC. There must be no communication between the production VPC and the nonproduction VPC. A transit gateway is deployed to facilitate communication between VPCs.

Which route table configurations on the transit gateway will meet these requirements?

- A. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes for only the shared services VP
- B. Create an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.
- C. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes for each VP
- D. Create an additional route table with only the shared services VPC attachment associated with propagated routes from each VPC.
- E. Configure a route table with all the VPC attachments associated with propagated routes for only the shared services VPCCreate an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.
- F. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes disable
- G. Create an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.

**Answer: A**

**NEW QUESTION 36**

A company is using a NAT gateway to allow internet connectivity for private subnets in a VPC in the us-west-2 Region. After a security audit, the company needs to remove the NAT gateway.

In the private subnets, the company has resources that use the unified Amazon CloudWatch agent. A network engineer must create a solution to ensure that the unified CloudWatch agent continues to work after the removal of the NAT gateway.

Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

- A. Validate that private DNS is enabled on the VPC by setting the enableDnsHostnames VPC attribute and the enableDnsSupport VPC attribute to true.
- B. Create a new security group with an entry to allow outbound traffic that uses the TCP protocol on port 443 to destination 0.0.0.0/0
- C. Create a new security group with entries to allow inbound traffic that uses the TCP protocol on port 443 from the IP prefixes of the private subnets.
- D. Create the following interface VPC endpoints in the VPC: com.amazonaws.us-west-2.logs and com.amazonaws.us-west-2.monitorin
- E. Associate the new security group with the endpoint network interfaces.
- F. Create the following interface VPC endpoint in the VPC: com.amazonaws.us-west-2.cloudwatch.Associate the new security group with the endpoint network interfaces.
- G. Associate the VPC endpoint or endpoints with route tables that the private subnets use.

**Answer: BDF**

**NEW QUESTION 39**

A global company operates all its non-production environments out of three AWS Regions: eu-west-1, us-east-1, and us-west-1. The company hosts all its production workloads in two on-premises data centers. The company has 60 AWS accounts and each account has two VPCs in each Region. Each VPC has a virtual private gateway where two VPN connections terminate for resilient connectivity to the data centers. The company has 360 VPN tunnels to each data center, resulting in high management overhead. The total VPN throughput for each Region is 500 Mbps.

The company wants to migrate the production environments to AWS. The company needs a solution that will simplify the network architecture and allow for future growth. The production environments will generate an additional 2 Gbps of traffic per Region back to the data centers. This traffic will increase over time.

Which solution will meet these requirements?

- A. Set up an AWS Direct Connect connection from each data center to AWS in each Regio
- B. Create and attach private VIFs to a single Direct Connect gatewa
- C. Attach the Direct Connect gateway to all the VPC
- D. Remove the existing VPN connections that are attached directly to the virtual private gateways.
- E. Create a single transit gateway with VPN connections from each data cente
- F. Share the transit gateway with each account by using AWS Resource Access Manager (AWS RAM). Attach the transit gateway to each VP
- G. Remove the existing VPN connections that are attached directly to the virtual private gateways.
- H. Create a transit gateway in each Region with multiple newly commissioned VPN connections from each data cente
- I. Share the transit gateways with each account by using AWS Resource Access Manager (AWS RAM). In each Region, attach the transit gateway to each VPRemove the existing VPN connections that are attached directly to the virtual private gateways.
- J. Peer all the VPCs in each Region to a new VPC in each Region that will function as a centralized transit VP
- K. Create new VPN connections from each data center to the transit VPC
- L. Terminate the original VPN connections that are attached to all the original VPC
- M. Retain the new VPN connection to the new transit VPC in each Region.

Answer: C

#### NEW QUESTION 44

A company has a hybrid cloud environment. The company's data center is connected to the AWS Cloud by an AWS Direct Connect connection. The AWS environment includes VPCs that are connected together in a hub-and-spoke model by a transit gateway. The AWS environment has a transit VIF with a Direct Connect gateway for on-premises connectivity.

The company has a hybrid DNS model. The company has configured Amazon Route 53 Resolver endpoints in the hub VPC to allow bidirectional DNS traffic flow. The company is running a backend application in one of the VPCs.

The company uses a message-oriented architecture and employs Amazon Simple Queue Service (Amazon SQS) to receive messages from other applications over a private network. A network engineer wants to use an interface VPC endpoint for Amazon SQS for this architecture. Client services must be able to access the endpoint service from on premises and from multiple VPCs within the company's AWS infrastructure.

Which combination of steps should the network engineer take to ensure that the client applications can resolve DNS for the interface endpoint? (Choose three.)

- A. Create the interface endpoint for Amazon SQS with the option for private DNS names turned on.
- B. Create the interface endpoint for Amazon SQS with the option for private DNS names turned off.
- C. Manually create a private hosted zone for sqs.us-east-1.amazonaws.co
- D. Add necessary records that point to the interface endpoint
- E. Associate the private hosted zones with other VPCs.
- F. Use the automatically created private hosted zone for sqs.us-east-1.amazonaws.com with previously created necessary records that point to the interface endpoint
- G. Associate the private hosted zones with other VPCs.
- H. Access the SQS endpoint by using the public DNS name sqs.us-east-1.amazonaws.com in VPCs and on premises.
- I. Access the SQS endpoint by using the private DNS name of the interface endpoint.sqs.us-east-1.vpc.amazonaws.com in VPCs and on premises.

Answer: ADF

#### NEW QUESTION 45

A company has deployed its AWS environment in a single AWS Region. The environment consists of a few hundred application VPCs, a shared services VPC, and a VPN connection to the company's on-premises environment. A network engineer needs to implement a transit gateway with the following requirements:

- Application VPCs must be isolated from each other.
- Bidirectional communication must be allowed between the application VPCs and the on-premises network.
- Bidirectional communication must be allowed between the application VPCs and the shared services VPC. The network engineer creates the transit gateway with options disabled for default route table association and default route table propagation. The network engineer also creates the VPN attachment for the on-premises network and creates the VPC attachments for the application VPCs and the shared services VPC.

The network engineer must meet all the requirements for the transit gateway by designing a solution that needs the least number of transit gateway route tables.

Which combination of actions should the network engineer perform to accomplish this goal?(Choose two.)

- A. Configure a separate transit gateway route table for on premise
- B. Associate the VPN attachment with this transit gateway route table
- C. Propagate all application VPC attachments to this transit gateway route table.
- D. Configure a separate transit gateway route table for each application VPC
- E. Associate each application VPC attachment with its respective transit gateway route table
- F. Propagate the shared services VPC attachment and the VPN attachment to this transit gateway route table.
- G. Configure a separate transit gateway route table for all application VPC
- H. Associate all application VPCs with this transit gateway route table
- I. Propagate the shared services VPC attachment and the VPN attachment to this transit gateway route table.
- J. Configure a separate transit gateway route table for the shared services VPC
- K. Associate the shared services VPC attachment with this transit gateway route table
- L. Propagate all application VPC attachments to this transit gateway route table.
- M. Configure a separate transit gateway route table for on premises and the shared services VPC
- N. Associate the VPN attachment and the shared services VPC attachment with this transit gateway route table
- O. Propagate all application VPC attachments to this transit gateway route table.

Answer: BD

#### NEW QUESTION 49

A software company offers a software-as-a-service (SaaS) accounting application that is hosted in the AWS Cloud. The application requires connectivity to the company's on-premises network. The company has two redundant 10 GB AWS Direct Connect connections between AWS and its on-premises network to accommodate the growing demand for the application.

The company already has encryption between its on-premises network and the colocation. The company needs to encrypt traffic between AWS and the edge routers in the colocation within the next few months. The company must maintain its current bandwidth.

What should a network engineer do to meet these requirements with the LEAST operational overhead?

- A. Deploy a new public VIF with encryption on the existing Direct Connect connection
- B. Reroute traffic through the new public VIF.
- C. Create a virtual private gateway. Deploy new AWS Site-to-Site VPN connections from on premises to the virtual private gateway. Reroute traffic from the Direct Connect private VIF to the new VPNs.
- D. Deploy a new pair of 10 GB Direct Connect connections with MACsec
- E. Configure MACsec on the edge router
- F. Reroute traffic to the new Direct Connect connection
- G. Decommission the original Direct Connect connections
- H. Deploy a new pair of 10 GB Direct Connect connections with MACsec
- I. Deploy a new public VIF on the new Direct Connect connection
- J. Deploy two AWS Site-to-Site VPN connections on top of the new public VIF
- K. Reroute traffic from the existing private VIF to the new Site-to-Site connection
- L. Decommission the original Direct Connect connections.

Answer: C



**NEW QUESTION 50**

A company is planning to deploy many software-defined WAN (SD-WAN) sites. The company is using AWS Transit Gateway and has deployed a transit gateway in the required AWS Region. A network engineer needs to deploy the SD-WAN hub virtual appliance into a VPC that is connected to the transit gateway. The solution must support at least 5 Gbps of throughput from the SD-WAN hub virtual appliance to other VPCs that are attached to the transit gateway. Which solution will meet these requirements?

- A. Create a new VPC for the SD-WAN hub virtual appliance
- B. Create two IPsec VPN connections between the SD-WAN hub virtual appliance and the transit gateway
- C. Configure BGP over the IPsec VPN connections
- D. Assign a new CIDR block to the transit gateway
- E. Create a new VPC for the SD-WAN hub virtual appliance
- F. Attach the new VPC to the transit gateway with a VPC attachment
- G. Add a transit gateway Connect attachment
- H. Create a Connect peer and specify the GRE and BGP parameter
- I. Create a route in the appropriate VPC for the SD-WAN hub virtual appliance to route to the transit gateway.
- J. Create a new VPC for the SD-WAN hub virtual appliance
- K. Attach the new VPC to the transit gateway with a VPC attachment
- L. Create two IPsec VPN connections between the SD-WAN hub virtual appliance and the transit gateway
- M. Configure BGP over the IPsec VPN connections.
- N. Assign a new CIDR block to the transit gateway
- O. Create a new VPC for the SD-WAN hub virtual appliance
- P. Attach the new VPC to the transit gateway with a VPC attachment
- Q. Add a transit gateway Connect attachment
- R. Create a Connect peer and specify the VXLAN and BGP parameter
- S. Create a route in the appropriate VPC for the SD-WAN hub virtual appliance to route to the transit gateway.

**Answer:** D

**NEW QUESTION 51**

A company hosts a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin in an Amazon CloudFront distribution. The company wants to implement a custom authentication system that will provide a token for its authenticated customers. The web application must ensure that the GET/POST requests come from authenticated customers before it delivers the content. A network engineer must design a solution that gives the web application the ability to identify authorized customers. What is the MOST operationally efficient solution that meets these requirements?

- A. Use the ALB to inspect the authorized token inside the GET/POST request payload
- B. Use an AWS Lambda function to insert a customized header to inform the web application of an authenticated customer request.
- C. Integrate AWS WAF with the ALB to inspect the authorized token inside the GET/POST request payload
- D. Configure the ALB listener to insert a customized header to inform the web application of an authenticated customer request.
- E. Use an AWS Lambda@Edge function to inspect the authorized token inside the GET/POST request payload
- F. Use the Lambda@Edge function also to insert a customized header to inform the web application of an authenticated customer request.
- G. Set up an EC2 instance that has a third-party packet inspection tool to inspect the authorized token inside the GET/POST request payload
- H. Configure the tool to insert a customized header to inform the web application of an authenticated customer request.

**Answer:** C

**NEW QUESTION 53**

A company operates its IT services through a multi-site hybrid infrastructure. The company deploys resources on AWS in the us-east-1 Region and in the eu-west-2 Region. The company also deploys resources in its own data centers that are located in the United States (US) and in the United Kingdom (UK). In both AWS Regions, the company uses a transit gateway to connect 15 VPCs to each other. The company has created a transit gateway peering connection between the two transit gateways. The VPC CIDR blocks do not overlap with each other or with IP addresses used within the data centers. The VPC CIDR prefixes can also be aggregated either on a Regional level or for the company's entire AWS environment.

The data centers are connected to each other by a private WAN connection. IP routing information is exchanged dynamically through Interior BGP (iBGP) sessions. The data centers maintain connectivity to AWS through one AWS Direct Connect connection in the US and one Direct Connect connection in the UK. Each Direct Connect connection is terminated on a Direct Connect gateway and is associated with a local transit gateway through a transit VIF.

Traffic follows the shortest geographical path from source to destination. For example, packets from the UK data center that are targeted to resources in eu-west-2 travel across the local Direct Connect connection. In cases of cross-Region data transfers, such as from the UK data center to VPCs in us-east-1, the private WAN connection must be used to minimize costs on AWS. A network engineer has configured each transit gateway association on the Direct Connect gateway to advertise VPC-specific CIDR IP prefixes only from the local Region. The routes toward the other Region must be learned through BGP from the routers in the other data center in the original, non-aggregated form.

The company recently experienced a problem with cross-Region data transfers because of issues with its private WAN connection. The network engineer needs to modify the routing setup to prevent similar interruptions in the future. The solution cannot modify the original traffic routing goal when the network is operating normally.

Which modifications will meet these requirements? (Choose two.)

- A. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection
- B. Add the company's entire AWS environment aggregate route to the list of subnets advertised through the local Direct Connect connection.
- C. Add the CIDR prefixes from the other Region VPCs and the local VPC CIDR blocks to the list of subnets advertised through the local Direct Connect connection
- D. Configure data center routers to make routing decisions based on the BGP communities received.
- E. Add the aggregate IP prefix for the other Region and the local VPC CIDR blocks to the list of subnets advertised through the local Direct Connect connection.
- F. Add the aggregate IP prefix for the company's entire AWS environment and the local VPC CIDR blocks to the list of subnets advertised through the local Direct Connect connection.
- G. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection
- H. Add both Regional aggregate IP prefixes to the list of subnets advertised through the Direct Connect connection on both sides of the network
- I. Configure data center routers to make routing decisions based on the BGP communities received.

**Answer:** AD

**NEW QUESTION 54**

A company has been using an outdated application layer protocol for communication among applications. The company decides not to use this protocol anymore

and must migrate all applications to support a new protocol. The old protocol and the new protocol are TCP-based, but the protocols use different port numbers. After several months of work, the company has migrated dozens of applications that run on Amazon EC2 instances and in containers. The company believes that all the applications have been migrated, but the company wants to verify this belief. A network engineer needs to verify that no application is still using the old protocol.

Which solution will meet these requirements without causing any downtime?

- A. Use Amazon Inspector and its Network Reachability rules packag
- B. Wait until the analysis has finished running to find out which EC2 instances are still listening to the old port.
- C. Enable Amazon GuardDut
- D. Use the graphical visualizations to filter for traffic that uses the port of the old protoco
- E. Exclude all internet traffic to filter out occasions when the same port is used as an ephemeral port.
- F. Configure VPC flow logs to be delivered into an Amazon S3 bucke
- G. Use Amazon Athena to query the data and to filter for the port number that is used by the old protocol.
- H. Inspect all security groups that are assigned to the EC2 instances that host the application
- I. Remove the port of the old protocol if that port is in the list of allowed port
- J. Verify that the applications are operating properly after the port is removed from the security groups.

**Answer: C**

**Explanation:**

Configuring VPC flow logs to be delivered into an Amazon S3 bucket would enable capture of information about the IP traffic going to and from network interfaces within the VPC3. Using Amazon Athena to query the data and to filter for the port number that is used by the old protocol would enable identification of applications that are still using the old protocol.

**NEW QUESTION 59**

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 60**

A company is developing an application in which IoT devices will report measurements to the AWS Cloud. The application will have millions of end users. The company observes that the IoT devices cannot support DNS resolution. The company needs to implement an Amazon EC2 Auto Scaling solution so that the IoT devices can connect to an application endpoint without using DNS.

Which solution will meet these requirements MOST cost-effectively?

- A. Use an Application Load Balancer (ALB)-type target group for a Network Load Balancer (NLB). Create an EC2 Auto Scaling grou
- B. Attach the Auto Scaling group to the AL
- C. Set up the IoT devices to connect to the IP addresses of the NLB.
- D. Use an AWS Global Accelerator accelerator with an Application Load Balancer (ALB) endpoint
- E. Create an EC2 Auto Scaling grou
- F. Attach the Auto Scaling group to the ALSet up the IoT devices to connect to the IP addresses of the accelerator.
- G. Use a Network Load Balancer (NLB). Create an EC2 Auto Scaling grou
- H. Attach the Auto Scaling group to the NL
- I. Set up the IoT devices to connect to the IP addresses of the NLB.
- J. Use an AWS Global Accelerator accelerator with a Network Load Balancer (NLB) endpoint
- K. Create anEC2 Auto Scaling grou
- L. Attach the Auto Scaling group to the NL
- M. Set up the IoT devices to connect to the IP addresses of the accelerator.

**Answer: D**

**Explanation:**

AWS Global Accelerator can provide static IP addresses that the IoT devices can connect to without using DNS2. It can also route traffic over the AWS global network and improve performance and availability for the IoT devices2. An NLB can provide end-to-end encryption for HTTPS traffic by using TLS as a target group protocol and terminating SSL connections at the load balancer level1. An NLB can also support session affinity (sticky sessions) with TCP connections1.

**NEW QUESTION 63**

A bank built a new version of its banking application in AWS using containers that content to an on-premises database over VPN connection. This application version requires users to also update their client application. The bank plans to deprecate the earlier client version. However, the company wants to keep supporting earlier clients through their on-premises version of the application to serve a small portion of the customers who haven't yet upgraded.

What design will allow the company to serve both newer and earlier clients in the MOST efficient way?

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

I. Use header-based routing to route traffic based on the application version.

**Answer:** D

#### NEW QUESTION 65

A company has multiple AWS accounts. Each account contains one or more VPCs. A new security guideline requires the inspection of all traffic between VPCs. The company has deployed a transit gateway that provides connectivity between all VPCs. The company also has deployed a shared services VPC with Amazon EC2 instances that include IDS services for stateful inspection. The EC2 instances are deployed across three Availability Zones. The company has set up VPC associations and routing on the transit gateway. The company has migrated a few test VPCs to the new solution for traffic inspection. Soon after the configuration of routing, the company receives reports of intermittent connections for traffic that crosses Availability Zones. What should a network engineer do to resolve this issue?

- A. Modify the transit gateway VPC attachment on the shared services VPC by enabling cross-Availability Zone load balancing.
- B. Modify the transit gateway VPC attachment on the shared services VPC by enabling appliance mode support.
- C. Modify the transit gateway by selecting VPN equal-cost multi-path (ECMP) routing support.
- D. Modify the transit gateway by selecting multicast support.

**Answer:** B

#### Explanation:

To resolve the issue of intermittent connections for traffic that crosses Availability Zones after configuring routing for traffic inspection between VPCs using a transit gateway and EC2 instances with IDS services in a shared services VPC, a network engineer should modify the transit gateway VPC attachment on the shared services VPC by enabling appliance mode support (Option B). This will ensure that traffic is routed to the same EC2 instance for stateful inspection and prevent intermittent connections.

#### NEW QUESTION 67

An organization is replacing a tape backup system with a storage gateway. there is currently no connectivity to AWS. Initial testing is needed. What connection option should the organization use to get up and running at minimal cost?

- A. Use an internet connection.
- B. Set up an AWS VPN connection.
- C. Provision an AWS Direct Connection private virtual interface.
- D. Provision a Direct Connect public virtual interface.

**Answer:** A

#### NEW QUESTION 72

A media company is implementing a news website for a global audience. The website uses Amazon CloudFront as its content delivery network. The backend runs on Amazon EC2 Windows instances behind an Application Load Balancer (ALB). The instances are part of an Auto Scaling group. The company's customers access the website by using service.example.com as the CloudFront custom domain name. The CloudFront origin points to an ALB that uses service-alb.example.com as the domain name. The company's security policy requires the traffic to be encrypted in transit at all times between the users and the backend. Which combination of changes must the company make to meet this security requirement? (Choose three.)

- A. Create a self-signed certificate for service.example.co
- B. Import the certificate into AWS Certificate Manager (ACM). Configure CloudFront to use this imported SSL/TLS certificat
- C. Change the default behavior to redirect HTTP to HTTPS.
- D. Create a certificate for service.example.com by using AWS Certificate Manager (ACM). Configure CloudFront to use this custom SSL/TLS certificat
- E. Change the default behavior to redirect HTTP to HTTPS.
- F. Create a certificate with any domain name by using AWS Certificate Manager (ACM) for the EC2 instance
- G. Configure the backend to use this certificate for its HTTPS listene
- H. Specify the instance target type during the creation of a new target group that uses the HTTPS protocol for its target
- I. Attach the existing Auto Scaling group to this new target group.
- J. Create a public certificate from a third-party certificate provider with any domain name for the EC2 instance
- K. Configure the backend to use this certificate for its HTTPS listene
- L. Specify the instance target type during the creation of a new target group that uses the HTTPS protocol for its target
- M. Attach the existing Auto Scaling group to this new target group.
- N. Create a certificate for service-alb.example.com by using AWS Certificate Manager (ACM). On the ALB add a new HTTPS listener that uses the new target group and the service-alb.example.com ACM certificat
- O. Modify the CloudFront origin to use the HTTPS protocol onl
- P. Delete the HTTP listener on the ALB.
- Q. Create a self-signed certificate for service-alb.example.co
- R. Import the certificate into AWS Certificate Manager (ACM). On the ALB add a new HTTPS listener that uses the new target group and the imported service-alb.example.com ACM certificat
- S. Modify the CloudFront origin to use the HTTPS protocol onl
- T. Delete the HTTP listener on the ALB.

**Answer:** BDE

#### NEW QUESTION 76

A company has several production applications across different accounts in the AWS Cloud. The company operates from the us-east-1 Region only. Only certain partner companies can access the applications. The applications are running on Amazon EC2 instances that are in an Auto Scaling group behind an Application Load Balancer (ALB). The EC2 instances are in private subnets and allow traffic only from the ALB. The ALB is in a public subnet and allows inbound traffic only from partner network IP address ranges over port 80.

When the company adds a new partner, the company must allow the IP address range of the partner network in the security group that is associated with the ALB in each account. A network engineer must implement a solution to centrally manage the partner network IP address ranges. Which solution will meet these requirements in the MOST operationally efficient manner?

- A. Create an Amazon DynamoDB table to maintain all IP address ranges and security groups that need to be update



- B. Update the DynamoDB table with the new IP address range when the company adds a new partne
- C. Invoke an AWS Lambda function to read new IP address ranges and security groups from the DynamoDB table to update the security group
- D. Deploy this solution in all accounts.
- E. Create a new prefix lis
- F. Add all allowed IP address ranges to the prefix lis
- G. Use Amazon EventBridge (Amazon CloudWatch Events) rules to invoke an AWS Lambda function to update security groups whenever a new IP address range is added to the prefix lis
- H. Deploy this solution in all accounts.
- I. Create a new prefix lis
- J. Add all allowed IP address ranges to the prefix lis
- K. Share the prefix list across different accounts by using AWS Resource Access Manager (AWS RAM). Update security groups to use the prefix list instead of the partner IP address rang
- L. Update the prefix list with the new IP address range when the company adds a new partner.
- M. Create an Amazon S3 bucket to maintain all IP address ranges and security groups that need to be update
- N. Update the S3 bucket with the new IP address range when the company adds a new partne
- O. Invoke an AWS Lambda function to read new IP address ranges and security groups from the S3 bucket to update the security group
- P. Deploy this solution in all accounts.

**Answer:** C

**Explanation:**

Creating a new prefix list and adding all allowed IP address ranges to the prefix list would enable grouping of CIDR blocks that can be referenced in security group rules3. Sharing the prefix list across different accounts by using AWS Resource Access Manager (AWS RAM)would enable central management of the partner network IP address ranges5. Updating security groups to use the prefix list instead of the partner IP address range would enable simplification of security group rules3. Updating the prefix list with the new IP address range when the company adds a new partner would enable automatic propagation of the changes to all security groups that use the prefix list3.

**NEW QUESTION 79**

A security team is performing an audit of a company's AWS deployment. The security team is concerned that two applications might be accessing resources that should be blocked by network ACLs and security groups. The applications are deployed across two Amazon Elastic Kubernetes Service (Amazon EKS) clusters that use the Amazon VPC Container Network Interface (CNI) plugin for Kubernetes. The clusters are in separate subnets within the same VPC and have a Cluster Autoscaler configured.

The security team needs to determine which POD IP addresses are communicating with which services throughout the VPC. The security team wants to limit the number of flow logs and wants to examine the traffic from only the two applications.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create VPC flow logs in the default forma
- B. Create a filter to gather flow logs only from the EKS nodes.Include the srcaddr field and the dstaddr field in the flow logs.
- C. Create VPC flow logs in a custom forma
- D. Set the EKS nodes as the resource Include the pkt-srcaddr field and the pkt-dstaddr field in the flow logs.
- E. Create VPC flow logs in a custom forma
- F. Set the application subnets as resource
- G. Include the pkt-srcaddr field and the pkt-dstaddr field in the flow logs.
- H. Create VPC flow logs in a custom forma
- I. Create a filter to gather flow logs only from the EKS nodes.Include the pkt-srcaddr field and the pkt-dstaddr field in the flow logs.

**Answer:** D

**NEW QUESTION 81**

An Australian ecommerce company hosts all of its services in the AWS Cloud and wants to expand its customer base to the United States (US). The company is targeting the western US for the expansion.

The company's existing AWS architecture consists of four AWS accounts with multiple VPCs deployed in the ap-southeast-2 Region. All VPCs are attached to a transit gateway in ap-southeast-2. There are dedicated VPCs for each application service. The company also has VPCs for centralized security features such as proxies, firewalls, and logging.

The company plans to duplicate the infrastructure from ap-southeast-2 to the us-west-1 Region. A network engineer must establish connectivity between the various applications in the two Regions. The solution must maximize bandwidth, minimize latency and minimize operational overhead.

Which solution will meet these requirements?

- A. Create VPN attachments between the two transit gateway
- B. Configure the VPN attachments to use BGP routing between the two transit gateways.
- C. Peer the transit gateways in each Regio
- D. Configure routing between the two transit gateways for each Region's IP addresses.
- E. Create a VPN server in a VPC in each Regio
- F. Update the routing to point to the VPN servers for the IP addresses in alternate Regions.
- G. Attach the VPCs in us-west-1 to the transit gateway in ap-southeast-2.

**Answer:** B

**Explanation:**

Peering the transit gateways in each region would establish a private network connection between the two regions, allowing the company to route traffic between the VPCs in different regions without going over the public internet. This would help minimize latency and maximize bandwidth while reducing the operational overhead of managing multiple VPN connections.

**NEW QUESTION 83**

A retail company is running its service on AWS. The company's architecture includes Application Load Balancers (ALBs) in public subnets. The ALB target groups are configured to send traffic to backend Amazon EC2 instances in private subnets. These backend EC2 instances can call externally hosted services over the internet by using a NAT gateway.

The company has noticed in its billing that NAT gateway usage has increased significantly. A network engineer needs to find out the source of this increased usage.

Which options can the network engineer use to investigate the traffic through the NAT gateway? (Choose two.)

- A. Enable VPC flow logs on the NAT gateway's elastic network interface
- B. Publish the logs to a log group in Amazon CloudWatch Log
- C. Use CloudWatch Logs Insights to query and analyze the logs.
- D. Enable NAT gateway access log
- E. Publish the logs to a log group in Amazon CloudWatch Log
- F. Use CloudWatch Logs Insights to query and analyze the logs.
- G. Configure Traffic Mirroring on the NAT gateway's elastic network interface
- H. Send the traffic to an additional EC2 instance
- I. Use tools such as tcpdump and Wireshark to query and analyze the mirrored traffic.
- J. Enable VPC flow logs on the NAT gateway's elastic network interface
- K. Publish the logs to an Amazon S3 bucket
- L. Create a custom table for the S3 bucket in Amazon Athena to describe the log structure
- M. Use Athena to query and analyze the logs.
- N. Enable NAT gateway access log
- O. Publish the logs to an Amazon S3 bucket
- P. Create a custom table for the S3 bucket in Amazon Athena to describe the log structure
- Q. Use Athena to query and analyze the logs.

**Answer:** AD

**Explanation:**

To investigate the increased usage of a NAT gateway in a VPC architecture with ALBs and backend EC2 instances, a network engineer can use the following options:

➤ Enable VPC flow logs on the NAT gateway's elastic network interface and publish the logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query and analyze the logs.  
(Option A)

➤ Enable VPC flow logs on the NAT gateway's elastic network interface and publish the logs to an Amazon S3 bucket. Create a custom table for the S3 bucket in Amazon Athena to describe the log structure and use Athena to query and analyze the logs. (Option D)

These options allow for detailed analysis of traffic through the NAT gateway to identify the source of increased usage.

**NEW QUESTION 87**

A network engineer has deployed an Amazon EC2 instance in a private subnet in a VPC. The VPC has no public subnet. The EC2 instance hosts application code that sends messages to an Amazon Simple Queue Service (Amazon SQS) queue. The subnet has the default network ACL with no modification applied. The EC2 instance has the default security group with no modification applied.

The SQS queue is not receiving messages.

Which of the following are possible causes of this problem? (Choose two.)

- A. The EC2 instance is not attached to an IAM role that allows write operations to Amazon SQS.
- B. The security group is blocking traffic to the IP address range used by Amazon SQS
- C. There is no interface VPC endpoint configured for Amazon SQS
- D. The network ACL is blocking return traffic from Amazon SQS
- E. There is no route configured in the subnet route table for the IP address range used by Amazon SQS

**Answer:** CE

**NEW QUESTION 90**

A company is running multiple workloads on Amazon EC2 instances in public subnets. In a recent incident, an attacker exploited an application vulnerability on one of the EC2 instances to gain access to the instance. The company fixed the application and launched a replacement EC2 instance that contains the updated application.

The attacker used the compromised application to spread malware over the internet. The company became aware of the compromise through a notification from AWS. The company needs the ability to identify when an application that is deployed on an EC2 instance is spreading malware.

Which solution will meet this requirement with the LEAST operational effort?

- A. Use Amazon GuardDuty to analyze traffic patterns by inspecting DNS requests and VPC flow logs.
- B. Use Amazon GuardDuty to deploy AWS managed decoy systems that are equipped with the most recent malware signatures.
- C. Set up a Gateway Load Balance
- D. Run an intrusion detection system (IDS) appliance from AWS Marketplace on Amazon EC2 for traffic inspection.
- E. Configure Amazon Inspector to perform deep packet inspection of outgoing traffic.

**Answer:** A

**Explanation:**

This solution involves using Amazon GuardDuty to monitor network traffic and analyze DNS requests and VPC flow logs for suspicious activity. This will allow the company to identify when an application is spreading malware by monitoring the network traffic patterns associated with the instance. GuardDuty is a fully managed threat detection service that continuously monitors for malicious activity and unauthorized behavior in your AWS accounts and workloads. It requires minimal setup and configuration and can be integrated with other AWS services for automated remediation. This solution requires the least operational effort compared to the other options

**NEW QUESTION 93**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual ANS-C01 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the ANS-C01 Product From:

<https://www.2passeasy.com/dumps/ANS-C01/>

## Money Back Guarantee

### ANS-C01 Practice Exam Features:

- \* ANS-C01 Questions and Answers Updated Frequently
- \* ANS-C01 Practice Questions Verified by Expert Senior Certified Staff
- \* ANS-C01 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* ANS-C01 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year