



ANS-C01^{Q&As}

AWS Certified Advanced Networking Specialty Exam

Pass Amazon ANS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/ans-c01.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

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. Define the primary network interface to be created in one of the private subnets. For the second network interface, select one of the public subnets. Choose the BYOIP pool ID as the source of public IP addresses.
- B. Configure the primary network interface in a private subnet in the launch template. 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.
- C. Create an AWS Lambda function to run as a lifecycle hook of the Auto Scaling group when an instance is launching. In the Lambda function, assign a network interface to an AWS Global Accelerator endpoint.
- D. 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.

Correct Answer: D

RhinozD answer with links <https://aws.amazon.com/about-aws/whats-new/2020/11/amazon-ec2-auto-scaling-supports-attaching-multiple-network-interfaces-at-launch/>

<https://repost.aws/knowledge-center/ec2-auto-scaling-multiple-network-interfaces>

QUESTION 2

A company wants to use an AWS Network Firewall firewall to secure its workloads in the cloud through network traffic inspection. The company must record complete metadata information, such as source/destination IP addresses and protocol type. The company must also record all network traffic flows and any DROP or ALERT actions that the firewall takes for traffic that the firewall processes. The Network Firewall endpoints are placed in the correct subnets, and the VPC route tables direct traffic to the Network Firewall endpoints on the path to and from the internet.

How should a network engineer configure the firewall to meet these requirements?

- A. Create a firewall policy to ensure that traffic is processed by stateless or stateful rules according to needs. Select Amazon CloudWatch Logs as the destination for the flow logs.
- B. Create a firewall policy to ensure that traffic is processed by stateless or stateful rules according to needs. Configure Network Firewall logging for alert logs and flow logs. Select a destination for logs separately for stateful and stateless engines.
- C. Create a firewall policy to ensure that a stateful engine processes all the traffic. Configure Network Firewall logging for alert logs and flow logs. Select a destination for alert logs and flow logs.
- D. Create a firewall policy to ensure that a stateful engine processes all the traffic. Configure VPC flow logs for the subnets that the firewall protects. Select a destination for the flow logs.



Correct Answer: B

QUESTION 3

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.com`. Add necessary records that point to the interface endpoint. Associate the private hosted zones with other VPCs.
- D. 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. Associate the private hosted zones with other VPCs.
- E. Access the SQS endpoint by using the public DNS name `sqs.us-east-1.amazonaws.com` in VPCs and on premises.
- F. Access the SQS endpoint by using the private DNS name of the interface endpoint `.sqs.us-east-1.vpce.amazonaws.com` in VPCs and on premises.

Correct Answer: BCE

To access interface endpoints through other VPCs, we need to

1.
Disable private DNS for VPC endpoints
 2.
Create PHZ e.g. `sqs.us-east-1.amazonaws.com`
 3.
Create Alias record pointing to VPC endpoint DNS
 4.
Associate PHZ with all the spoke VPCs
-

QUESTION 4

A company has deployed a multi-VPC environment in the AWS Cloud. The company uses a transit gateway to connect



all the VPCs together. In the past, the company has experienced a loss of connectivity between applications after changes to security groups, network ACLs, and route tables in a VPC. When these changes occur, the company wants to automatically verify that connectivity still exists between different resources in a single VPC.

- A. Create a list of paths between different resources to check in VPC Reachability Analyzer. Create an Amazon EventBridge rule to monitor when a change is made and logged in Amazon CloudWatch. Configure the rule to invoke an AWS Lambda function to test the different paths in Reachability Analyzer.
- B. Create a list of paths between different resources to check in VPC Reachability Analyzer. Create an Amazon EventBridge rule to monitor when a change is made and logged in AWS CloudTrail. Configure the rule to invoke an AWS Lambda function to test the different paths in Reachability Analyzer.
- C. Create a list of paths to check in AWS Transit Gateway Network Manager Route Analyzer. Create an Amazon EventBridge rule to monitor when a change is made and logged in Amazon CloudWatch. Configure the rule to invoke an AWS Lambda function to test the different paths in Route Analyzer.
- D. Create a list of paths to check in AWS Transit Gateway Network Manager Route Analyzer. Create an Amazon EventBridge rule to monitor when a change is made and logged in AWS CloudTrail. Configure the rule to invoke an AWS Lambda function to test the different paths in Route Analyzer.

Correct Answer: B

<https://docs.aws.amazon.com/vpc/latest/reachability/what-is-reachability-analyzer.html>

QUESTION 5

A company has deployed a software-defined WAN (SD-WAN) solution to interconnect all of its offices. The company is migrating workloads to AWS and needs to extend its SD-WAN solution to support connectivity to these workloads. A network engineer plans to deploy AWS Transit Gateway Connect and two SD-WAN virtual appliances to provide this connectivity. According to company policies, only a single SD-WAN virtual appliance can handle traffic from AWS workloads at a given time. How should the network engineer configure routing to meet these requirements?

- A. Add a static default route in the transit gateway route table to point to the secondary SD-WAN virtual appliance. Add routes that are more specific to point to the primary SD-WAN virtual appliance.
- B. Configure the BGP community tag 7224:7300 on the primary SD-WAN virtual appliance for BGP routes toward the transit gateway.
- C. Configure the AS_PATH prepend attribute on the secondary SD-WAN virtual appliance for BGP routes toward the transit gateway.
- D. Disable equal-cost multi-path (ECMP) routing on the transit gateway for Transit Gateway Connect.

Correct Answer: C

A - incorrect, static routes are not possible in TGW B - incorrect, these BGP communities are used for BGP over DX C - correct, AS_PATH prepending is a standard BGP way of influencing return traffic for advertised prefixes and SDWAN supports this. D - incorrect, disabling ECMP will make sure the SDWAN>TGW traffic is not load shared, but the return traffic TGW>SDWAN is not affected and therefore both appliances will process traffic.

[Latest ANS-C01 Dumps](#)

[ANS-C01 VCE Dumps](#)

[ANS-C01 Practice Test](#)