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.passapply.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 company runs an application on Amazon EC2 instances. A network engineer implements a NAT gateway in the application\\'s VPC to replaceself-managed NAT instances. After the network engineer shifts traffic from the self-managed NAT instances to the NAT gateway, users begin toreport issues.During troubleshooting, the network engineer discovers that the connection to the application is closing after approximately 6 minutes ofinactivity.What should the network engineer do to resolve this issue?

A. Check for increases in the IdleTimeoutCount Amazon CloudWatch metric for the NAT gateway. Configure TCP keepalive on theapplication EC2 instances.

B. Check for increases in the ErrorPortAllocation Amazon CloudWatch metric for the NAT gateway. Configure an HTTP timeout value on theapplication EC2 instances.

C. Check for increases in the PacketsDropCount Amazon CloudWatch metric for the NAT gateway. Configure an HTTPS timeout value onthe application EC2 instances.

D. Check for decreases in the ActiveConnectionCount Amazon CloudWatch metric for the NAT gateway. Configure UDP keepalive on theapplication EC2 instances.

Correct Answer: A

Internet connection drops after 350 seconds

Problem

Your instances can access the internet, but the connection drops after 350 seconds.

Cause

If a connection that\\'s using a NAT gateway is idle for 350 seconds or more, the connection times out.

When a connection times out, a NAT gateway returns an RST packet to any resources behind the NAT gateway that attempt to continue the connection (it does not send a FIN packet).

Solution

To prevent the connection from being dropped, you can initiate more traffic over the connection. Alternatively, you can enable TCP keepalive on the instance with a value less than 350 seconds.

QUESTION 2

A financial trading company is using Amazon EC2 instances to run its trading platform. Part of the company\\'s trading platform includes athird-party pricing service that the EC2 instances communicate with over UDP on port 50000.Recently, the company has had problems with the pricing service. Some of the responses from the pricing service appear to be incorrectlyformatted and are not being processed successfully. The third-party vendor requests access to the data that the pricing service is returning.The third-party vendor wants to capture request and response data for debugging by logging in to an EC2 instance that accesses the pricingservice. The company prohibits direct access to production systems and requires all log analysis to be performed in a dedicated monitoringaccount.Which set of steps should a network engineer take to capture the data and meet these requirements?

A. 1. Configure VPC flow logs to capture the data that flows in the VPC.2. Send the data to an Amazon S3 bucket.3. In the monitoring account, extract the data that flows to the EC2 instance\\'s IP address and filter the traffic for the UDP

data.4. Provide the data to the third-party vendor.

B. 1. Configure a traffic mirror filter to capture the UDP data.2. Configure Traffic Mirroring to capture the traffic for the EC2 instance\\'s elastic network interface.3. Configure a packet inspection package on a new EC2 instance in the production environment. Use the elastic network interface of thenew EC2 instance as the target for the traffic mirror.4. Extract the data by using the packet inspection package.5. Provide the data to the third-party vendor.

C. 1. Configure a traffic mirror filter to capture the UDP data.2. Configure Traffic Mirroring to capture the traffic for the EC2 instance\\'s elastic network interface.3. Configure a packet inspection package on a new EC2 instance in the monitoring account. Use the elastic network interface of the newEC2 instance as the target for the traffic mirror.4. Extract the data by using the packet inspection package.5. Provide the data to the third-party vendor.

D. 1. Create a new Amazon Elastic Block Store (Amazon EBS) volume. Attach the EBS volume to the EC2 instance.2. Log in to the EC2 instance in the production environment. Run the tcpdump command to capture the UDP data on the EBS volume.3. Export the data from the EBS volume to Amazon S3.4. Provide the data to the third-party vendor.

Correct Answer: C

https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html

QUESTION 3

A company uses a 4 Gbps AWS Direct Connect dedicated connection with a link aggregation group (LAG) bundle to connect to five VPCs thatare deployed in the us-east-1 Region. Each VPC serves a different business unit and uses its own private VIF for connectivity to the on-premises environment. Users are reporting slowness when they access resources that are hosted on AWS.A network engineer finds that there are sudden increases in throughput and that the Direct Connect connection becomes saturated at thesame time for about an hour each business day. The company wants to know which business unit is causing the sudden increase inthroughput. The network engineer must find out this information and implement a solution to resolve the problem.Which solution will meet these requirements?

A. Review the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF issending the highest throughput during the period in which slowness is observed. Create a new 10 Gbps dedicated connection. Shift trafficfrom the existing dedicated connection to the new dedicated connection.

B. Review the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF issending the highest throughput during the period in which slowness is observed. Upgrade the bandwidth of the existing dedicatedconnection to 10 Gbps.

C. Review the Amazon CloudWatch metrics for ConnectionBpsIngress and ConnectionPpsEgress to determine which VIF is sending thehighest throughput during the period in which slowness is observed. Upgrade the existing dedicated connection to a 5 Gbps hostedconnection.

D. Review the Amazon CloudWatch metrics for ConnectionBpsIngress and ConnectionPpsEgress to determine which VIF is sending thehighest throughput during the period in which slowness is observed. Create a new 10 Gbps dedicated connection. Shift traffic from theexisting dedicated connection to the new dedicated connection.

Correct Answer: A

https://docs.aws.amazon.com/directconnect/latest/UserGuide/dedicated_connection.html

> "You cannot change the port speed after you create the connection request. To change the port speed, you must create and configure a new connection."

QUESTION 4

A company has an application that runs on a fleet of Amazon EC2 instances. A new company regulation mandates that all network traffic toand from the EC2 instances must be sent to a centralized third-party EC2 appliance for content inspection.Which solution will meet these requirements?

A. Configure VPC flow logs on each EC2 network interface. Publish the flow logs to an Amazon S3 bucket. Create a third-party EC2appliance to acquire flow logs from the S3 bucket. Log in to the appliance to monitor network content.

B. Create a third-party EC2 appliance in an Auto Scaling group fronted by a Network Load Balancer (NLB). Configure a mirror session.Specify the NLB as the mirror target. Specify a mirror filter to capture inbound and outbound traffic. For the source of the mirror session,specify the EC2 elastic network interfaces for all the instances that host the application.

C. Configure a mirror session. Specify an Amazon Kinesis Data Firehose delivery stream as the mirror target. Specify a mirror filter tocapture inbound and outbound traffic. For the source of the mirror session, specify the EC2 elastic network interfaces for all the instancesthat host the application. Create a third-party EC2 appliance. Send all traffic to the appliance through the Kinesis Data Firehose deliverystream for content inspection.

D. Configure VPC flow logs on each EC2 network interface. Send the logs to Amazon CloudWatch. Create a third-party EC2 appliance.Configure a CloudWatch filter to send the flow logs to Amazon Kinesis Data Firehose to load the logs into the appliance.

Correct Answer: B

You can use the following resources as traffic mirror targets: Network interfaces of type interface Network Load Balancers Gateway Load Balancer endpoints https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-targets.html

QUESTION 5

A company has deployed a critical application on a fleet of Amazon EC2 instances behind an Application Load Balancer. The application mustalways be reachable on port 443 from the public internet. The application recently had an outage that resulted from an incorrect change tothe EC2 security group.A network engineer needs to automate a way to verify the network connectivity between the public internet and the EC2 instances whenever achange is made to the security group. The solution also must notify the network engineer when the change affects the connection.Which solution will meet these requirements?

A. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture REJECT traffic on port 443. Publish the flow logrecords to a log group in Amazon CloudWatch Logs. Create a CloudWatch Logs metric filter for the log group for rejected traffic. Create analarm to notify the network engineer.

B. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture all traffic on port 443. Publish the flow logrecords to a log group in Amazon CloudWatch Logs. Create a CloudWatch Logs metric filter for the log group for all traffic. Create an alarmto notify the network engineer

C. Create a VPC Reachability Analyzer path on port 443. Specify the security group as the source. Specify the EC2 instances as thedestination. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change to thesecurity group affects the connection. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to the SNStopic in case the analyses fail Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function when achange to the security group occurs.

D. Create a VPC Reachability Analyzer path on port 443. Specify the internet gateway of the VPC as the source. Specify the EC2 instancesas the destination. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change tothe security group affects the connection. Create an AWS Lambda

function to start Reachability Analyzer and to publish a message to theSNS topic in case the analyses fail. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function whena change to the security group occurs.

Correct Answer: D

https://aws.amazon.com/blogs/networking-and-content-delivery/automating-connectivity-assessments-with-vpc-reachability-analyzer/