ANS-C01 Q&As

AWS Certified Advanced Networking Specialty

Pass Amazon ANS-C01 Exam with 100% Guarantee

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

https://www.leads4pass.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 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 connectivityinitiated over an SSL connection. Traffic must be able to flow to the application from other AWS accounts over private connectivity. Theapplication 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. Create a lifecycle hook to add new tasks to thetarget group from Amazon ECS as required to handle scaling. Specify the GLB in the service definition. Create a VPC peer for external AWSaccounts. Update the route tables so that the AWS accounts can reach the GLB.

B. Choose an Application Load Balancer (ALB) as the type of load balancer for the ECS service. Create path-based routing rules to allowthe application to target the containers that are registered in the target group. Specify the ALB in the service definition. Create a VPCendpoint service for the ALB Share the VPC endpoint service with other AWS accounts.

C. Choose an Application Load Balancer (ALB) as the type of load balancer for the ECS service. Create path-based routing rules to allowthe application to target the containers that are registered in the target group. Specify the ALB in the service definition. Create a VPCpeer for the external AWS accounts. Update the route tables so that the AWS accounts can reach the ALB.

D. Choose a Network Load Balancer (NLB) as the type of load balancer for the ECS service. Specify the NLB in the service definition.Create a VPC endpoint service for the NLB. Share the VPC endpoint service with other AWS accounts.

Correct Answer: D

Path based routing is not required here. Requirement is "Traffic must be able to flow to the application from other AWS accounts over private connectivity. " - which is a case for PrivateLink.

QUESTION 2

A company is migrating its containerized application to AWS. For the architecture the company will have an ingress VPC with a Network LoadBalancer (NLB) to distribute the traffic to front-end pods in an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The front end of theapplication will determine which user is requesting access and will send traffic to 1 of 10 services VPCs. Each services VPC will include anNLB that distributes traffic to the services pods in an EKS cluster.The company is concerned about overall cost. User traffic will be responsible for more than 10 TB of data transfer from the ingress VPC toservices VPCs every month. A network engineer needs to recommend how to design the communication between the VPCs.Which solution will meet these requirements at the LOWEST cost?

A. Create a transit gateway. Peer each VPC to the transit gateway. Use zonal DNS names for the NLB in the services VPCs to minimizecross-AZ traffic from the ingress VPC to the services VPCs.

B. Create an AWS PrivateLink endpoint in every Availability Zone in the ingress VPC. Each PrivateLink endpoint will point to the zonal DNSentry of the NLB in the services VPCs.

C. Create a VPC peering connection between the ingress VPC and each of the 10 services VPCs. Use zonal DNS names for the NLB in theservices VPCs to minimize cross-AZ traffic from the ingress VPC to the services VPCs.

D. Create a transit gateway. Peer each VPC to the transit gateway. Turn off cross-AZ load balancing on the transit gateway. Use RegionalDNS names for the NLB in the services VPCs.

Correct Answer: C

VPC peering offers the lowest overall cost when compared to other options for inter-VPC connectivity. https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/vpc-to-vpc-connectivity.html

There is no such thing as "TG peering"; there are VPC peering and TG attachments.

QUESTION 3

A company\\'s network engineer builds and tests network designs for VPCs in a development account. The company needs to monitor thechanges that are made to network resources and must ensure strict compliance with network security policies. The company also needsaccess to the historical configurations of network resources.Which solution will meet these requirements?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with a custom pattern to monitor the account for changes. Configurethe rule to invoke an AWS Lambda function to identify noncompliant resources. Update an Amazon DynamoDB table with the changes thatare identified.

B. Create custom metrics from Amazon CloudWatch logs. Use the metrics to invoke an AWS Lambda function to identify noncompliantresources. Update an Amazon DynamoDB table with the changes that are identified.

C. Record the current state of network resources by using AWS Config. Create rules that reflect the desired configuration settings. Setremediation for noncompliant resources.

D. Record the current state of network resources by using AWS Systems Manager Inventory. Use Systems Manager State Manager toenforce the desired configuration settings and to carry out remediation for noncompliant resources.

Correct Answer: C

AWS Config = Compliance

QUESTION 4

A company recently experienced an IP address exhaustion event in its VPCs. The event affected service capacity. The VPCs hold two or moresubnets in different Availability Zones.A network engineer needs to develop a solution that monitors IP address usage across resources in the VPCs. The company needs to receivenotification about possible issues so that the company can act before an incident happens.Which solution will meet these requirements with the LEAST operational overhead?

A. Set up Amazon VPC IP Address Manager (IPAM) with a new top-level pool. In the top-level pool, create a pool for each VPC. In each VPCpool, create a pool for each subnet in that VPC. Turn on the auto-import option for the VPC pools and the subnet pools. Configure anAmazon CloudWatch alarm to send an Amazon Simple Notification Service (Amazon SNS) notification if the availability limit threshold isreached.

B. Set up a log group in Amazon CloudWatch Logs for each subnet. Create an AWS Lambda function that reads each subnet\\'s IP addressusage and publishes metrics to the log group. Configure an Amazon CloudWatch alarm to send an Amazon Simple Notification Service(Amazon SNS) notification if the availability limit threshold is reached.

C. Set up a custom Amazon CloudWatch metric for IP address usage for each subnet. Create an AWS Lambda function that reads eachsubnet\\'s IP address usage and publishes a CloudWatch metric dimension. Schedule the Lambda function to run every 5 minutes. Configurea CloudWatch alarm to send an Amazon Simple Notification Service (Amazon SNS) notification if the availability limit threshold is reached.

D. Set up Amazon VPC IP Address Manager (IPAM) with a new top-level pool. In the top-level pool, create a pool for each VPC. In each VPCpool, create a pool for each subnet in that VPC. Turn on the auto-import option for the VPC pools and the subnet pools. Configure anAmazon EventBridge rule that monitors each pool availability limit threshold and sends an Amazon Simple Notification Service (AmazonSNS) notification if the limit threshold is reached.

Correct Answer: A

https://docs.aws.amazon.com/vpc/latest/ipam/cloudwatch-ipam.html

QUESTION 5

A data analytics company has a 100-node high performance computing (HPC) cluster. The HPC cluster is for parallel data processing and ishosted in a VPC in the AWS Cloud. As part of the data processing workflow, the HPC cluster needs to perform several DNS queries to resolveand connect to Amazon RDS databases, Amazon S3 buckets, and on-premises data stores that are accessible through AWS Direct Connect. TheHPC cluster can increase in size by five to seven times during the company\\'s peak event at the end of the year.The company is using two Amazon EC2 instances as primary DNS servers for the VPC. The EC2 instances are configured to forward queries tothe default VPC resolver for Amazon Route 53 hosted domains and to the on-premises DNS servers for other on-premises hosted domainnames. The company notices job failures and finds that DNS queries from the HPC cluster nodes failed when the nodes tried to resolve RDSand S3 bucket endpoints.Which architectural change should a network engineer implement to provide the DNS service in the MOST scalable way?

A. Scale out the DNS service by adding two additional EC2 instances in the VPC. Reconfigure half of the HPC cluster nodes to use thesenew DNS servers. Plan to scale out by adding additional EC2 instance-based DNS servers in the future as the HPC cluster size grows.

B. Scale up the existing EC2 instances that the company is using as DNS servers. Change the instance size to the largest possibleinstance size to accommodate the current DNS load and the anticipated load in the future.

C. Create Route 53 Resolver outbound endpoints. Create Route 53 Resolver rules to forward queries to on-premises DNS servers for onpremises hosted domain names. Reconfigure the HPC cluster nodes to use the default VPC resolver instead of the EC2 instance-basedDNS servers. Terminate the EC2 instances.

D. Create Route 53 Resolver inbound endpoints. Create rules on the on-premises DNS servers to forward queries to the default VPCresolver. Reconfigure the HPC cluster nodes to forward all DNS queries to the on-premises DNS servers. Terminate the EC2 instances.

Correct Answer: C

The VPC+2 addresses that those two EC2-based DNS use have a limit of 1024 queries per second. So we must get rid of them. We use the route 53 resolver, and for that we need an outgoing endpoint that can forwards queries to the ompprem zones.

QUESTION 6

A government contractor is designing a multi-account environment with multiple VPCs for a customer. A network security policy requires alltraffic between any two VPCs to be transparently inspected by a third-party appliance.The customer wants a solution that features AWS Transit Gateway. The setup must be highly available across multiple Availability Zones, andthe solution needs to support automated failover. Furthermore, asymmetric routing is not supported by the inspection appliances.Which combination of steps is part of a solution that meets these requirements? (Choose two.)

A. Deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection

VPC. Connect theinspection VPC to the transit gateway by using a VPC attachment. Create a target group, and register the appliances with the targetgroup. Create a Network Load Balancer (NLB), and set it up to forward to the newly created target group. Configure a default route in theinspection VPCs transit gateway subnet toward the NLB.

B. Deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection VPC. Connect theinspection VPC to the transit gateway by using a VPC attachment. Create a target group, and register the appliances with the targetgroup. Create a Gateway Load Balancer, and set it up to forward to the newly created target group. Configure a default route in theinspection VPC\\'s transit gateway subnet toward the Gateway Load Balancer endpoint.

C. Configure two route tables on the transit gateway. Associate one route table with all the attachments of the application VPCs.Associate the other route table with the inspection VPC\\'s attachment. Propagate all VPC attachments into the inspection route table.Define a static default route in the application route table. Enable appliance mode on the attachment that connects the inspection VPC.

D. Configure two route tables on the transit gateway. Associate one route table with all the attachments of the application VPCs.Associate the other route table with the inspection VPCs attachment. Propagate all VPC attachments into the application route table.Define a static default route in the inspection route table. Enable appliance mode on the attachment that connects the inspection VPC.

E. Configure one route table on the transit gateway. Associate the route table with all the VPCs. Propagate all VPC attachments into theroute table. Define a static default route in the route table.

Correct Answer: BC

B and C, GLB better for 3rd party appliance, TGW RT associated to APP VPCs has a single route to the Inspection VPC and second TGW RT for the inspection VPC has all APP VPC CIDRs propagated to it.

QUESTION 7

A network engineer needs to build an encrypted connection between an on-premises data center and a VPC. The network engineer attachesthe VPC to a virtual private gateway and sets up an AWS Site-to-Site VPN connection. The VPN tunnel is UP after configuration and is working.However, during rekey for phase 2 of the VPN negotiation, the customer gateway device is receiving different parameters than the parametersthat the device is configured to support.The network engineer checks the IPsec configuration of the VPN tunnel. The network engineer notices that the customer gateway device isconfigured with the most secure encryption algorithms that the AWS Site-to-Site VPN configuration file provides.What should the network engineer do to troubleshoot and correct the issue?

A. Check the native virtual private gateway logs. Restrict the VPN tunnel options to the specific VPN parameters that the virtual privategateway requires.

B. Check the native customer gateway logs. Restrict the VPN tunnel options to the specific VPN parameters that the customer gatewayrequires.

C. Check Amazon CloudWatch logs of the virtual private gateway. Restrict the VPN tunnel options to the specific VPN parameters that thevirtual private gateway requires.

D. Check Amazon CloudWatch logs of the customer gateway. Restrict the VPN tunnel options to the specific VPN parameters that thecustomer gateway requires.

Correct Answer: B

You check Cloudwatch for AWS resources or your native/on-prem logs for your on prem resource. AandD is out.

The problem statement indicates that customer gateway is misconfigured. So you need to work on Customer gateway.

QUESTION 8

A company has its production VPC (VPC-A) in the eu-west-1 Region in Account 1. VPC-A is attached to a transit gateway (TGW-A) that isconnected to an on-premises data center in Dublin, Ireland, by an AWS Direct Connect transit VIF that is configured for an AWS Direct Connectgateway. The company also has a staging VPC (VPC-B) that is attached to another transit gateway (TGW-B) in the eu-west-2 Region in Account2.A network engineer must implement connectivity between VPC-B and the on-premises data center in Dublin.Which solutions will meet these requirements? (Choose two.)

A. Configure inter-Region VPC peering between VPC-A and VPC-B. Add the required VPC peering routes. Add the VPC-B CIDR block in theallowed prefixes on the Direct Connect gateway association.

B. Associate TGW-B with the Direct Connect gateway. Advertise the VPC-B CIDR block under the allowed prefixes.

C. Configure another transit VIF on the Direct Connect connection and associate TGW-B. Advertise the VPC-B CIDR block under the allowedprefixes.

D. Configure inter-Region transit gateway peering between TGW-A and TGW-B. Add the peering routes in the transit gateway route tables.Add both the VPC-A and the VPC-B CIDR block under the allowed prefix list in the Direct Connect gateway association.

E. Configure an AWS Site-to-Site VPN connection over the transit VIF to TGW-B as a VPN attachment.

Correct Answer: BD

Only one Transit VIF is possible with one Direct connection. With DX gateway, 3 Transit Gateways (same or different regions) can be added. Option B) and D) are correct, though B) itself fulfils the requirement in the question.

QUESTION 9

A network engineer has deployed an Amazon EC2 instance in a private subnet in a VPC. The VPC has no public subnet. The EC2 instancehosts application code that sends messages to an Amazon Simple Queue Service (Amazon SQS) queue. The subnet has the default networkACL 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

Correct Answer: AC

A - EC2 requires IAM role that allows write operations to Amazon SQS C - Being in private subnet, interface endpoint is required to access SQS

QUESTION 10

A company is planning to deploy many software-defined WAN (SD-WAN) sites. The company is using AWS Transit Gateway and has deployed atransit gateway in the required AWS Region. A network engineer needs to deploy the SD-WAN hub virtual appliance into a VPC that isconnected to the transit gateway. The solution must support at least 5 Gbps of throughput from the SD-WAN hub virtual appliance to otherVPCs 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. Create two IPsec VPN connections between the SD-WAN hub virtual applianceand the transit gateway. Configure BGP over the IPsec VPN connections

B. Assign a new CIDR block to the transit gateway. Create a new VPC for the SD-WAN hub virtual appliance. Attach the new VPC to thetransit gateway with a VPC attachment. Add a transit gateway Connect attachment. Create a Connect peer and specify the GRE and BGPparameters. Create a route in the appropriate VPC for the SD-WAN hub virtual appliance to route to the transit gateway.

C. Create a new VPC for the SD-WAN hub virtual appliance. Attach the new VPC to the transit gateway with a VPC attachment. Create twoIPsec VPN connections between the SD-WAN hub virtual appliance and the transit gateway. Configure BGP over the IPsec VPNconnections.

D. Assign a new CIDR block to the transit gateway. Create a new VPC for the SD-WAN hub virtual appliance. Attach the new VPC to thetransit gateway with a VPC attachment. Add a transit gateway Connect attachment. Create a Connect peer and specify the VXLAN andBGP parameters. Create a route in the appropriate VPC for the SD-WAN hub virtual appliance to route to the transit gateway.

Correct Answer: B

TGW Connect is setup with GRE and BGP no mention of VXLAN: https://aws.amazon.com/transit-gateway/faqs/

QUESTION 11

A company\\'s network engineer is designing a hybrid DNS solution for an AWS Cloud workload. Individual teams want to manage their own DNShostnames for their applications in their development environment. The solution must integrate the application-specific hostnames with thecentrally managed DNS hostnames from the on-premises network and must provide bidirectional name resolution. The solution also mustminimize 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.

Correct Answer: ACE

For bidirectional name resolution, both Route 53 Resolver inbound and outbound endpoint is required.

QUESTION 12

A network engineer is designing the DNS architecture for a new AWS environment. The environment must be able to resolve DNS names ofendpoints on premises, and the on-premises systems must be able to resolve the names of AWS endpoints. The DNS architecture must giveindividual accounts the ability to manage subdomains.The network engineer needs to create a single set of rules that will work across multiple accounts to control this behavior. In addition, thenetwork engineer must use AWS native services whenever possible.Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Create an Amazon Route 53 private hosted zone for the overall cloud domain. Plan to create subdomains that align to other AWSaccounts that are associated with the central Route 53 private hosted zone.

B. Create AWS Directory Service for Microsoft Active Directory server endpoints in the central AWS account that hosts the private hostedzone for the overall cloud domain. Create a conditional forwarding rule in Microsoft Active Directory DNS to forward traffic to a DNSresolver endpoint on premises. Create another rule to forward traffic between subdomains to the VPC resolver.

C. Create Amazon Route 53 Resolver inbound and outbound endpoints in the central AWS account that hosts the private hosted zone forthe overall cloud domain. Create a forwarding rule to forward traffic to a DNS resolver endpoint on premises. Create another rule toforward traffic between subdomains to the Resolver inbound endpoint.

D. Ensure that networking exists between the other accounts and the central account so that traffic can reach the AWS Directory Servicefor Microsoft Active Directory DNS endpoints.

E. Ensure that networking exists between the other accounts and the central account so that traffic can reach the Amazon Route 53Resolver endpoints.

F. Share the Amazon Route 53 Resolver rules between accounts by using AWS Resource Access Manager (AWS RAM). Ensure thatnetworking exists between the other accounts and the central account so that traffic can reach the Route 53 Resolver endpoints.

Correct Answer: ACF

C can\\'t be true. can\\'t create rules for the Resolver Inbound endpoint at the same time, E can\\'t be False if F is true. they state the same thing

QUESTION 13

A company operates its IT services through a multi-site hybrid infrastructure. The company deploys resources on AWS in the us-east-1 Regionand 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 theUnited Kingdom (UK). In both AWS Regions, the company uses a transit gateway to connect 15 VPCs to each other. The company has createda transit gateway peering connection between the two transit gateways. The VPC CIDR blocks do not overlap with each other or with IPaddresses used within the data centers. The VPC CIDR prefixes can also be aggregated either on a Regional level or for the company\\'s entireAWS environment.The data centers are connected to each other by a private WAN connection. IP routing information is exchanged dynamically through InteriorBGP (iBGP) sessions. The data centers maintain connectivity to AWS through one AWS Direct Connect connection in the US and one DirectConnect connection in the UK. Each Direct Connect connection is terminated on a Direct Connect gateway and is associated with a localtransit 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 toresources in eu-west-2 travel across the local Direct Connect connection. In cases of cross-Region data transfers, such as from the UK datacenter to VPCs in us-east-1, the private WAN connection must be used to minimize costs on AWS. A network engineer has configured eachtransit gateway association on the Direct Connect gateway to advertise VPC-specific CIDR IP prefixes only from the local Region. The routestoward 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. Thenetwork engineer needs to modify the routing setup to prevent similar interruptions in the future. The solution cannot modify the originaltraffic 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. Add the company\\'sentire AWS environment aggregate route to the list of subnets advertised through the local Direct Connect connection.

B. Add the CIDR prefixes from the other Region VPCs and the local VPC CIDR blocks to the list of subnets advertised through the localDirect Connect connection. Configure data center routers to make routing decisions based on the BGP communities received.

C. Add the aggregate IP prefix for the other Region and the local VPC CIDR blocks to the list of subnets advertised through the local DirectConnect connection.

D. Add the aggregate IP prefix for the company\\'s entire AWS environment and the local VPC CIDR blocks to the list of subnets advertisedthrough the local Direct Connect connection.

E. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection. Add both Regionalaggregate IP prefixes to the list of subnets advertised through the Direct Connect connection on both sides of the network. Configure datacenter routers to make routing decisions based on the BGP communities received.

Correct Answer: CE

If the private WAN failed, the network engineer would swing the traffic to the other region through the local Direct Connect and the Transit Gateways. That is the requirement. The solution is that the local DC has 2 kinds of route to the other

region VPCs. One is the existing CIDR-based routes via the private WAN, another is the advertised aggregated routes from the local Direct Connect connection. CIDR-based routes are prior to the aggregated routes advertised from Direct

Connect connection due to the longest prefix match routing algorithm.

The options which match this solution are C and E.

QUESTION 14

A company is replatforming a legacy data processing solution to AWS. The company deploys the solution on Amazon EC2 Instances in private subnets that are in one VPC.

The solution uses Amazon S3 for abject storage. Both the data that the solution processes and the data the solution produces are stored in Amazon S3. The solution uses Amazon DynamoDB to save its own state. The company collects flow logs for the VPC. The solution uses one NAT gateway to register its license through the internet. A software vendor provides a specific hostname so the solution can register its license.

The company notices that the AWS bill exceeds the projected budget for the solution. A network engineer uses AWS Cost Explorer to investigate the bill. The network engineer notices that the USE2-NatGateway-Bytes($) usage type is the root cause of the higher than expected bill.

What should the network engineer do to resolve the issue? (Choose two.)

A. Set up Amazon VPC Traffic Mirroring. Analyze the traffic to identify the traffic that the NAT gateway processes.

B. Examine the VPC flow logs to identity the traffic that traverses the NAT gateway.

C. Set up an AWS Cost and Usage Report in the AWS Billing and Cost Management console. Examine the report to find more details about the NAT gateway charges.

D. Verify that the security groups attached to the EC2 instances allow outgoing traffic only to the IP addresses that the hostname resolves to, the VPC CIDR block, and the AWS IP address ranges for Amazon S3 and DynamoDB.

E. Verify that the gateway VPC endpoints for Amazon S3 and DynamoDB are both set up and associated with the route tables of the private subnets.

Correct Answer: BD

QUESTION 15

A company is hosting an application on Amazon EC2 instances behind an Application Load Balancer. The instances are in an Amazon EC2Auto Scaling group. Because of a recent change to a security group, external users cannot access the application.A network engineer needs to prevent this downtime from happening again. The network engineer must implement a solution that remediatesnoncompliant changes to security groups.Which solution will meet these requirements?

A. Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security groupconfiguration. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.

B. Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security groupconfiguration. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.

C. Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security groupconfiguration. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.

D. Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security groupconfiguration. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.

Correct Answer: D

https://aws.amazon.com/blogs/mt/remediate-noncompliant-aws-config-rules-with-aws-systems-manager-automation-runbooks/