vmexam.com
#1 Cloud and VM Certification Guide

AWS ANS-C01

AWS ADVANCED NETWORKING SPECIALTY CERTIFICATION QUESTIONS & ANSWERS

Exam Summary – Syllabus – Questions

ANS-C01

AWS Certified Advanced Networking - Specialty

65 Questions Exam – 750 / 1000 Cut Score – Duration of 170 minutes

www.VMExam.com

Table of Contents

Know Your ANS-C01 Certification Well:

The ANS-C01 is best suitable for candidates who want to gain knowledge in the AWS Specialty. Before you start your ANS-C01 preparation you may struggle to get all the crucial Advanced Networking Specialty materials like ANS-C01 syllabus, sample questions, study guide.

But don't worry the ANS-C01 PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the ANS-C01 syllabus?
- How many questions are there in the ANS-C01 exam?
- Which Practice test would help me to pass the ANS-C01 exam at the first attempt?

Passing the ANS-C01 exam makes you AWS Certified Advanced Networking - Specialty. Having the Advanced Networking Specialty certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

AWS ANS-C01 Advanced Networking Specialty Certification Details:

Exam Name	AWS Certified Advanced Networking - Specialty (Advanced Networking Specialty)
Exam Code	ANS-C01
Exam Price	$300 USD
Duration	170 minutes
Number of Questions	65
Passing Score	750 / 1000
Recommended Training / Books	**AWS training for advanced networking**
Schedule Exam	**AWS Certification**
Sample Questions	**AWS ANS-C01 Sample Questions**
Recommended Practice	**AWS Certified Advanced Networking - Specialty Practice Test**

ANS-C01 Syllabus:

Section	Objectives
Network Design - 30%	
Design a solution that incorporates edge network services to optimize user performance and traffic management for global architectures.	**Knowledge of:** • Design patterns for the usage of content distribution networks (for example, Amazon CloudFront) • Design patterns for global traffic management (for example, AWS Global Accelerator) • Integration patterns for content distribution networks and global traffic management with other services (for example, Elastic Load Balancing [ELB], Amazon API Gateway) **Skills in:** • Evaluating requirements of global inbound and outbound traffic from the internet to design an appropriate content distribution solution
Design DNS solutions that meet public, private, and hybrid requirements.	**Knowledge of:** • DNS protocol (for example, DNS records, TTL, DNSSEC, DNS delegation, zones) • DNS logging and monitoring • Amazon Route 53 features (for example, alias records, traffic policies, resolvers, health checks) • Integration of Route 53 with other AWS networking services (for example, Amazon VPC) • Integration of Route 53 with hybrid, multi-account, and multi-Region options • Domain registration **Skills in:** • Using Route 53 public hosted zones • Using Route 53 private hosted zones • Using Route 53 Resolver endpoints in hybrid and AWS architectures • Using Route 53 for global traffic management • Creating and managing domain registrations
Design solutions that integrate load	**Knowledge of:**

Section	Objectives
balancing to meet high availability, scalability, and security requirements.	• How load balancing works at layer 3, layer 4, and layer 7 of the OSI model • Different types of load balancers and how they meet requirements for network design, high availability, and security • Connectivity patterns that apply to load balancing based on the use case (for example, internal load balancers, external load balancers) • Scaling factors for load balancers • Integrations of load balancers and other AWS services (for example, Global Accelerator, CloudFront, AWS WAF, Route 53, Amazon Elastic Kubernetes Service [Amazon EKS], AWS Certificate Manager [ACM]) • Configuration options for load balancers (for example, proxy protocol, cross-zone load balancing, session affinity [sticky sessions], routing algorithms) • Configuration options for load balancer target groups (for example, TCP, GENEVE, IP compared with instance) • AWS Load Balancer Controller for Kubernetes clusters • Considerations for encryption and authentication with load balancers (for example, TLS termination, TLS passthrough) **Skills in:** • Selecting an appropriate load balancer based on the use case • Integrating auto scaling with load balancing solutions • Integrating load balancers with existing application deployments
Define logging and monitoring requirements across AWS and hybrid networks.	**Knowledge of:** • Amazon CloudWatch metrics, agents, logs, alarms, dashboards, and insights in AWS architectures to provide visibility • AWS Transit Gateway Network Manager in architectures to provide visibility • VPC Reachability Analyzer in architectures to provide visibility • Flow logs and traffic mirroring in architectures to provide visibility

Section	Objectives
	• Access logging (for example, load balancers, CloudFront) **Skills in:** • Identifying the logging and monitoring requirements • Recommending appropriate metrics to provide visibility of the network status • Capturing baseline network performance
Design a routing strategy and connectivity architecture between on-premises networks and the AWS Cloud.	**Knowledge of:** • Routing fundamentals (for example, dynamic compared with static, BGP) • Layer 1 and layer 2 concepts for physical interconnects (for example, VLAN, link aggregation group [LAG], optics, jumbo frames) • Encapsulation and encryption technologies (for example, Generic Routing Encapsulation [GRE], IPsec) • Resource sharing across AWS accounts • Overlay networks **Skills in:** • Identifying the requirements for hybrid connectivity • Designing a redundant hybrid connectivity model with AWS services (for example, AWS Direct Connect, AWS Site-to-Site VPN) • Designing BGP routing with BGP attributes to influence the traffic flows based on the desired traffic patterns (load sharing, active/passive) • Designing for integration of a software-defined wide area network (SD-WAN) with AWS (for example, Transit Gateway Connect, overlay networks)
Design a routing strategy and connectivity architecture that include multiple AWS accounts, AWS Regions, and VPCs to support different connectivity patterns.	**Knowledge of:** • Different connectivity patterns and use cases (for example, VPC peering, Transit Gateway, AWS PrivateLink) • Capabilities and advantages of VPC sharing • IP subnets and solutions accounting for IP address overlaps **Skills in:**

Section	Objectives
	• Connecting multiple VPCs by using the most appropriate services based on requirements (for example, using VPC peering, Transit Gateway, PrivateLink) • Using VPC sharing in a multi-account setup • Managing IP overlaps by using different available services and options (for example, NAT, PrivateLink, Transit Gateway routing)
Network Implementation - 26%	
Implement routing and connectivity between on-premises networks and the AWS Cloud.	**Knowledge of:** • Routing protocols (for example, static, dynamic) • VPNs (for example, security, accelerated VPN) • Layer 1 and types of hardware to use (for example, Letter of Authorization [LOA] documents, colocation facilities, Direct Connect) • Layer 2 and layer 3 (for example, VLANs, IP addressing, gateways, routing, switching) • Traffic management and SD-WAN (for example, Transit Gateway Connect) • DNS (for example, conditional forwarding, hosted zones, resolvers) • Security appliances (for example, firewalls) • Load balancing (for example, layer 4 compared with layer 7, reverse proxies, layer 3) • Infrastructure automation • AWS Organizations and AWS Resource Access Manager (AWS RAM) (for example, multi-account Transit Gateway, Direct Connect, Amazon VPC, Route 53) • Test connectivity (for example, Route Analyzer, Reachability Analyzer) • Networking services of VPCs **Skills in:** • Configuring the physical network requirements for hybrid connectivity solutions • Configuring static or dynamic routing protocols to work with hybrid connectivity solutions • Configuring existing on-premises networks to connect

Section	Objectives
	with the AWS Cloud • Configuring existing on-premises name resolution with the AWS Cloud • Configuring and implementing load balancing solutions • Configuring network monitoring and logging for AWS services • Testing and validating connectivity between environments
Implement routing and connectivity across multiple AWS accounts, Regions, and VPCs to support different connectivity patterns.	**Knowledge of:** • Inter-VPC and multi-account connectivity (for example, VPC peering, Transit Gateway, VPN, third-party vendors, SD-WAN, multiprotocol label switching [MPLS]) • Private application connectivity (for example, PrivateLink) • Methods of expanding AWS networking connectivity (for example, Organizations, AWS RAM) • Host and service name resolution for applications and clients (for example, DNS) • Infrastructure automation • Authentication and authorization (for example, SAML, Active Directory) • Security (for example, security groups, network ACLs, AWS Network Firewall) • Test connectivity (for example, Route Analyzer, Reachability Analyzer, tooling) **Skills in:** • Configuring network connectivity architectures by using AWS services in a single-VPC or multi-VPC design (for example, DHCP, routing, security groups) • Configuring hybrid connectivity with existing third-party vendor solutions • Configuring a hub-and-spoke network architecture (for example, Transit Gateway, transit VPC) • Configuring a DNS solution to make hybrid connectivity possible • Implementing security between network boundaries • Configuring network monitoring and logging by using AWS solutions

Section	Objectives
Implement complex hybrid and multi-account DNS architectures.	**Knowledge of:** • When to use private hosted zones and public hosted zones • Methods to alter traffic management (for example, based on latency, geography, weighting) • DNS delegation and forwarding (for example, conditional forwarding) • Different DNS record types (for example, A, AAAA, TXT, pointer records, alias records) • DNSSEC • How to share DNS services between accounts (for example, AWS RAM) • Requirements and implementation options for outbound and inbound endpoints **Skills in:** • Configuring DNS zones and conditional forwarding • Configuring traffic management by using DNS solutions • Configuring DNS for hybrid networks • Configuring appropriate DNS records • Configuring DNSSEC on Route 53 • Configuring DNS within a centralized or distributed network architecture • Configuring DNS monitoring and logging on Route 53
Automate and configure network infrastructure.	**Knowledge of:** • Infrastructure as code (IaC) (for example, AWS Cloud Development Kit [AWS CDK], AWS CloudFormation, AWS CLI, AWS SDK, APIs) • Event-driven network automation • Common problems of using hardcoded instructions in IaC templates when provisioning cloud networking resources **Skills in:** • Creating and managing repeatable network configurations • Integrating event-driven networking functions • Integrating hybrid network automation options with

Section	Objectives
	AWS native IaC • Eliminating risk and achieving efficiency in a cloud networking environment while maintaining the lowest possible cost • Automating the process of optimizing cloud network resources with IaC
Network Management and Operation - 20%	
Maintain routing and connectivity on AWS and hybrid networks.	**Knowledge of:** • Industry-standard routing protocols that are used in AWS hybrid networks (for example, BGP over Direct Connect) • Connectivity methods for AWS and hybrid networks (for example, Direct Connect gateway, Transit Gateway, VIFs) • How limits and quotas affect AWS networking services (for example, bandwidth limits, route limits) • Available private and public access methods for custom services (for example, PrivateLink, VPC peering) • Available inter-Regional and intra-Regional communication patterns **Skills in:** • Managing routing protocols for AWS and hybrid connectivity options (for example, over a Direct Connect connection, VPN) • Maintaining private access to custom services (for example, PrivateLink, VPC peering) • Using route tables to direct traffic appropriately (for example, automatic propagation, BGP) • Setting up private access or public access to AWS services (for example, Direct Connect, VPN) • Optimizing routing over dynamic and static routing protocols (for example, summarizing routes, CIDR overlap)
Monitor and analyze network traffic to troubleshoot and optimize connectivity patterns.	**Knowledge of:** • Network performance metrics and reachability constraints (for example, routing, packet size) • Appropriate logs and metrics to assess network

Section	Objectives
	performance and reachability issues (for example, packet loss) • Tools to collect and analyze logs and metrics (for example, CloudWatch, VPC Flow Logs, VPC Traffic Mirroring) • Tools to analyze routing patterns and issues (for example, Reachability Analyzer, Transit Gateway Network Manager) **Skills in:** • Analyzing tool output to assess network performance and troubleshoot connectivity (for example, VPC Flow Logs, Amazon CloudWatch Logs) • Mapping or understanding network topology (for example, Transit Gateway Network Manager) • Analyzing packets to identify issues in packet shaping (for example, VPC Traffic Mirroring) • Troubleshooting connectivity issues that are caused by network misconfiguration (for example, Reachability Analyzer) • Verifying that a network configuration meets network design requirements (for example, Reachability Analyzer) • Automating the verification of connectivity intent as a network configuration changes (for example, Reachability Analyzer) • Troubleshooting packet size mismatches in a VPC to restore network connectivity
Optimize AWS networks for performance, reliability, and cost-effectiveness.	**Knowledge of:** • Situations in which a VPC peer or a transit gateway are appropriate • Different methods to reduce bandwidth utilization (for example, unicast compared with multicast, CloudFront) • Cost-effective connectivity options for data transfer between a VPC and on-premises environments • Different types of network interfaces on AWS • High-availability features in Route 53 (for example, DNS load balancing using health checks with latency and weighted record sets) • Availability of options from Route 53 that provide

Section	Objectives
	reliability • Load balancing and traffic distribution patterns • VPC subnet optimization • Frame size optimization for bandwidth across different connection types **Skills in:** • Optimizing for network throughput • Selecting the right network interface for the best performance (for example, elastic network interface, Elastic Network Adapter [ENA], Elastic Fabric Adapter [EFA]) • Choosing between VPC peering, proxy patterns, or a transit gateway connection based on analysis of the network requirements provided • Implementing a solution on an appropriate network connectivity service (for example, VPC peering, Transit Gateway, VPN connection) to meet network requirements • Implementing a multicast capability within a VPC and on-premises environments • Creating Route 53 public hosted zones and private hosted zones and records to optimize application availability (for example, private zonal DNS entry to route traffic to multiple Availability Zones) • Updating and optimizing subnets for auto scaling configurations to support increased application load • Updating and optimizing subnets to prevent the depletion of available IP addresses within a VPC (for example, secondary CIDR) • Configuring jumbo frame support across connection types • Optimizing network connectivity by using Global Accelerator to improve network performance and application availability
Network Security, Compliance, and Governance - 24%	
Implement and maintain network features to meet security and compliance needs and	**Knowledge of:** • Different threat models based on application architecture

Section	Objectives
requirements.	• Common security threats • Mechanisms to secure different application flows • AWS network architecture that meets security and compliance requirements **Skills in:** • Securing inbound traffic flows into AWS (for example, AWS WAF, AWS Shield, Network Firewall) • Securing outbound traffic flows from AWS (for example, Network Firewall, proxies, Gateway Load Balancers) • Securing inter-VPC traffic within an account or across multiple accounts (for example, security groups, network ACLs, VPC endpoint policies) • Implementing an AWS network architecture to meet security and compliance requirements (for example, untrusted network, perimeter VPC, three-tier architecture) • Developing a threat model and identifying appropriate mitigation strategies for a given network architecture • Testing compliance with the initial requirements (for example, failover test, resiliency) • Automating security incident reporting and alerting using AWS
Validate and audit security by using network monitoring and logging services.	**Knowledge of:** • Network monitoring and logging services that are available in AWS (for example, CloudWatch, AWS CloudTrail, VPC Traffic Mirroring, VPC Flow Logs, Transit Gateway Network Manager) • Alert mechanisms (for example, CloudWatch alarms) • Log creation in different AWS services (for example, VPC flow logs, load balancer access logs, CloudFront access logs) • Log delivery mechanisms (for example, Amazon Kinesis, Route 53, CloudWatch) • Mechanisms to audit network security configurations (for example, security groups, AWS Firewall Manager, AWS Trusted Advisor) **Skills in:** • Creating and analyzing a VPC flow log (including base

Section	Objectives
	and extended fields of flow logs) • Creating and analyzing network traffic mirroring (for example, using VPC Traffic Mirroring) • Implementing automated alarms by using CloudWatch • Implementing customized metrics by using CloudWatch • Correlating and analyzing information across single or multiple AWS log sources • Implementing log delivery solutions • Implementing a network audit strategy across single or multiple AWS network services and accounts (for example, Firewall Manager, security groups, network ACLs)
Implement and maintain confidentiality of data and communications of the network.	**Knowledge of:** • Network encryption options that are available on AWS • VPN connectivity over Direct Connect • Encryption methods for data in transit (for example, IPsec) • Network encryption under the AWS shared responsibility model • Security methods for DNS communications (for example, DNSSEC) **Skills in:** • Implementing network encryption methods to meet application compliance requirements (for example, IPsec, TLS) • Implementing encryption solutions to secure data in transit (for example, CloudFront, Application Load Balancers and Network Load Balancers, VPN over Direct Connect, AWS managed databases, Amazon S3, custom solutions on Amazon EC2, Transit Gateway) • Implementing a certificate management solution by using a certificate authority (for example, ACM, AWS Private Certificate Authority [ACM PCA]) • Implementing secure DNS communications

AWS ANS-C01 Sample Questions:

Question: 1

An ecommerce company has a business-critical application that runs on Amazon EC2 instances in a VPC. The company's development team has been testing a new version of the application on test EC2 instances.

The development team wants to test the new application version against production traffic to address any problems that might occur before the company releases the new version across all servers.

Which solution will meet this requirement with no impact on the end user's experience?

a) Configure Amazon Route 53 weighted routing policies by configuring records that have the same name and type as each of the instances. Assign relative weights to the production instances and the test instances.
b) Create an Application Load Balancer with weighted target groups. Add more than one target group to the forward action of a listener rule. Specify a weight for each target group.
c) Implement Traffic Mirroring to replay the production requests to the test instances. Configure the source as the production instances. Configure the target as the test instances.
d) Configure an NGINX proxy in front of the production servers. Use the NGINX mirroring capability.

Answer: c

Question: 2

A company hosts its ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in a private subnet with the default DHCP options set. Internet connectivity is through a NAT gateway that is configured in the public subnet.

A third-party audit of the security infrastructure identifies a DNS exfiltration vulnerability. The company must implement a highly available solution that protects against this vulnerability.

Which solution will meet these requirements MOST cost-effectively?

a) Configure a BIND server with DNS filtering. Modify the DNS servers in the DHCP options set.
b) Use Amazon Route 53 Resolver DNS Firewall. Configure a domain list with a rule group.
c) Use AWS Network Firewall with domain name filtering.
d) Configure an Amazon Route 53 Resolver outbound endpoint with rules to filter and block suspicious traffic.

Answer: b

Question: 3

A company hosts a public hosted zone in Amazon Route 53. The company wants to configure DNS Security Extensions (DNSSEC) signing for the public hosted zone. All the company's business-critical applications are running in the us-west-2 Region.

The company has created a symmetric, customer managed, single-Region key in us-west-2 by using AWS Key Management Service (AWS KMS). A network engineer finds that the existing AWS KMS key cannot be used to create a key-signing key (KSK).

How can the network engineer resolve this issue?

a) Recreate a symmetric, customer managed, multi-Region key in the us-east-1 Region. Use this key to create a KSK.
b) Recreate a symmetric, customer managed, single-Region key in us-west-2. Use this key to create a KSK.
c) Recreate an asymmetric, customer managed key with an ECC_NIST_P256 key spec in the us-east-1 Region. Use this key to create a KSK.
d) Recreate an asymmetric, customer managed key with an ECC_NIST_P256 key spec in us-west-2. Use this key to create a KSK.

Answer: c

Question: 4

A company has developed a new web application that processes confidential data that is hosted on Amazon EC2 instances.

The application needs to scale and must use certificates to authenticate clients. The application is configured to request a client's certificate and will validate the certificate as part of the initial handshake.

Which Elastic Load Balancing (ELB) solution will meet these requirements?

a) Configure an Application Load Balancer (ALB) that includes an HTTPS listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the ALB. Configure HTTPS as the protocol for the target group.
b) Configure a Network Load Balancer (NLB) that includes a TLS listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the NLB. Configure the NLB to terminate TLS. Configure TLS as the protocol for the target group.
c) Configure a Network Load Balancer (NLB) that includes a TCP listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the NLB. Configure TCP as the protocol for the target group.
d) Configure an Application Load Balancer (ALB) that includes a TLS listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the ALB. Configure TLS as the protocol for the target group.

Answer: c

Question: 5

A company has multiple VPCs in the us-east-1 Region. The company has deployed a website in one of the VPCs.

The company wants to implement split-view DNS so that the website is accessible internally from the VPCs and externally over the internet with the same domain name, example.com.

Which solution will meet these requirements?

a) Change the DHCP options for each VPC to use the IP address of an on-premises DNS server. Create a private hosted zone and a public hosted zone for example.com. Map the private hosted zone to the website's internal IP address. Map the public hosted zone to the website's external IP address.
b) Create Amazon Route 53 private hosted zones and public hosted zones that have the same name, example.com. Associate the VPCs with the private hosted zone. Create records in each hosted zone that determine how traffic is routed.
c) Create an Amazon Route 53 Resolver inbound endpoint for resolving example.com internally. Create a Route 53 public hosted zone for routing external DNS queries.
d) Create an Amazon Route 53 Resolver outbound endpoint for resolving example.com externally. Create a Route 53 private hosted zone for routing internal DNS queries.

Answer: b

Question: 6

A company is designing infrastructure on AWS with three VPCs connected to a transit gateway. The three VPCs are an application VPC, a backend VPC, and an inspection VPC.

The application VPC and the backend VPC have compute instances deployed in Availability Zone A and Availability Zone B. Stateful firewalls are deployed in the same Availability Zones in the inspection VPC, which is a shared services VPC.

All traffic is routed through the inspection VPC through the stateful layer 7 virtual firewall appliances to comply with a security policy that mandates traffic inspection. There are no overlapping IP addresses across the three VPCs.

A network engineer must ensure that traffic between the application VPC and the backend VPC can route through the inspection VPC's stateful firewalls.

Which solution will meet these requirements?

a) Create IPsec VPN connections between the transit gateway and the virtual firewall appliances.
b) Configure Virtual Router Redundancy Protocol (VRRP) on the virtual firewall appliances.
c) Set up BGP between the transit gateway and the virtual firewall appliances.
d) Enable transit gateway appliance mode for the VPC attachment to the inspection VPC.

Answer: d

Question: 7

A company collects a high volume of shipping data and stores the data in an on-premises data center. A network engineer wants to use Amazon S3 to store the data during the first phase of a migration to AWS.

During this phase, an application that resides in the data center will need to access the data privately in an S3 bucket that the company created.

The company has set up an AWS Direct Connect connection with a private VIF to connect the on-premises data center to a VPC. The network engineer plans to use this Direct Connect connection for the hybrid cloud setup. The solution must be highly available.

What should the network engineer do next to implement this architecture?

a) Configure an S3 gateway endpoint in the VPC. Update VPC route tables to route traffic to the S3 gateway endpoint. Configure the S3 gateway endpoint DNS name in the on-premises application.
b) Configure an S3 interface endpoint in the VPC. Configure the S3 interface endpoint DNS name in the on-premises application.
c) Configure an S3 gateway endpoint in the VPC. Update VPC route tables to route traffic to the S3 gateway endpoint. Configure an HTTP proxy on an Amazon EC2 instance in the VPC to route traffic to the S3 gateway endpoint. Configure the HTTP proxy DNS name in the on-premises application.
d) Configure an S3 interface endpoint in the VPC. Update VPC route tables to route traffic to the S3 interface endpoint. Configure an HTTP proxy on an Amazon EC2 instance in the VPC to route traffic to the S3 interface endpoint. Configure the HTTP proxy DNS name in the on-premises application.

Answer: b

Question: 8

A gaming company is planning to launch a globally available game that is hosted in one AWS Region. The game backend is hosted on Amazon EC2 instances that are part of an Auto Scaling group.

The game uses the gRPC protocol for bidirectional streaming between game clients and the backend. The company needs to filter incoming traffic based on the source IP address to protect the game.

Which solution will meet these requirements?

a) Configure an AWS Global Accelerator accelerator with an Application Load Balancer (ALB) endpoint. Attach the ALB to the Auto Scaling group. Configure an AWS WAF web ACL for the ALB to filter traffic based on the source IP address.
b) Configure an AWS Global Accelerator accelerator with a Network Load Balancer (NLB) endpoint. Attach the NLB to the Auto Scaling group. Configure security groups for the EC2 instances to filter traffic based on the source IP address.

c) Configure an Amazon CloudFront distribution with an Application Load Balancer (ALB) endpoint. Attach the ALB to the Auto Scaling group. Configure an AWS WAF web ACL for the ALB to filter traffic based on the source IP address.
d) Configure an Amazon CloudFront distribution with a Network Load Balancer (NLB) endpoint. Attach the NLB to the Auto Scaling group. Configure security groups for the EC2 instances to filter traffic based on the source IP address.

Answer: a

Question: 9

A company is migrating many applications from two on-premises data centers to AWS. The company's network team is setting up connectivity to the AWS environment. The migration will involve spreading the applications across two AWS Regions: us-east-1 and us-west-2. The company has set up AWS Direct Connect connections at two different locations. Direct Connect connection 1 is to the first data center and is at a location in us-east-1. Direct Connect connection 2 is to the second data center and is at a location in us-west-2.

The company has connected both Direct Connect connections to a single Direct Connect gateway by using transit VIFs. The Direct Connect gateway is associated with transit gateways that are deployed in each Region.

All traffic to and from AWS must travel through the first data center. In the event of failure, the second data center must take over the traffic.

How should the network team configure BGP to meet these requirements?

a) Configure the local preference BGP community tag 7224:7300 for the transit VIF connected to Direct Connect connection 1.
b) Configure the local preference BGP community tag 7224:9300 for the transit VIF connected to Direct Connect connection 2.
c) Use the AS_PATH attribute to prepend the additional hop for the transit VIF connected to Direct Connect connection 2.
d) Use the AS_PATH attribute to prepend the additional hop for the transit VIF connected to Direct Connect connection 1.

Answer: a

Question: 10

A company is using Amazon Route 53 Resolver for its hybrid DNS infrastructure. The company is using Route 53 Resolver forwarding rules for authoritative domains that are hosted on on-premises DNS servers.

The company achieves hybrid network connectivity by using an AWS Site-to-Site VPN connection. A new governance policy requires logging for DNS traffic that originates in the AWS Cloud.

The policy also requires the company to query DNS traffic to identify the source IP address of the resources that the query originated from, along with the DNS name that was requested.

Which solution will meet these requirements?

a) Create VPC flow logs for all VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the IP address and DNS name.
b) Modify the existing Route 53 Resolver rules to configure logging. Send the logs to an Amazon S3 bucket. Use Amazon Athena to query the IP address and DNS name.
c) Configure DNS logging for the Site-to-Site VPN connection. Send the logs to an Amazon S3 bucket. Use Amazon Athena to query the IP address and DNS name.
d) Configure Route 53 Resolver query logging for all VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the IP address and DNS name.

Answer: d

Study Guide to Crack AWS Advanced Networking Specialty ANS-C01 Exam:

- Getting details of the ANS-C01 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the ANS-C01 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the AWS provided training for ANS-C01 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the ANS-C01 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on ANS-C01 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for ANS-C01 Certification

Make VMExam.com your best friend during your AWS Certified Advanced Networking - Specialty exam preparation. We provide authentic practice tests for the ANS-C01 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual ANS-C01 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the ANS-C01 exam.

Start Online practice of ANS-C01 Exam by visiting URL

https://www.vmexam.com/aws/ans-c01-aws-certified-advanced-networking-specialty