AWS ANS-C00

AWS ADVANCED NETWORKING SPECIALTY CERTIFICATION QUESTIONS & ANSWERS

Exam Summary – Syllabus – Questions

ANS-C00

AWS Certified Advanced Networking - Specialty

65 Questions Exam – 700 / 1000 Cut Score – Duration of 170 minutes

www.VMExam.com

Table of Contents

Know Your ANS-C00 Certification Well:

The ANS-C00 is best suitable for candidates who want to gain knowledge in the AWS Specialty. Before you start your ANS-C00 preparation you may struggle to get all the crucial Advanced Networking Specialty materials like ANS-C00 syllabus, sample questions, study guide.

But don't worry the ANS-C00 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-C00 syllabus?
- How many questions are there in the ANS-C00 exam?
- Which Practice test would help me to pass the ANS-C00 exam at the first attempt?

Passing the ANS-C00 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-C00 Advanced Networking Specialty Certification Details:

Exam Name	AWS Certified Advanced Networking - Specialty (Advanced Networking Specialty)
Exam Code	ANS-C00
Exam Price	$300 USD
Duration	170 minutes
Number of Questions	65
Passing Score	700 / 1000
Recommended Training / Books	**Exam Readiness - AWS Certified Advanced Networking - Specialty**
Schedule Exam	**PEARSON VUE**
Sample Questions	**AWS ANS-C00 Sample Questions**
Recommended Practice	**AWS Certified Advanced Networking - Specialty Practice Test**

ANS-C00 Syllabus:

Section	Objectives
Design and implement hybrid IT network architectures at scale - 24%	
Apply procedural concepts for the implementation of connectivity for hybrid IT architecture	
Given a scenario, derive an appropriate hybrid IT architecture connectivity solution	- Determine IP address allocations for a low-level design - Map the application flows to create a communication matrix - Implement device configurations based on templates - Determine implementation steps for the configuration of the AWS console (AWS, Direct Connect link, VPN, On-premises, L1→7 testing, etc.) - Integrate AWS and on-premises DNS services - Outline the components of a solution (for example, diagram, protocols within a solution, VLANs, 801.q, BFD, etc.) - Evaluate a network architecture diagram for alignment to business and technical requirements - Determine implementation steps for the configuration of devices (AWS, Direct Connect link, VPN, On-premises, L1→7 testing, etc.) - Customize device configurations based on business requirements - Given business and technical requirements, define a rollback procedure - Design multipath links into the VPC to meet business requirements - Determine the high availability/load balancing requirements specific to an architecture
Explain the process to extend connectivity using Direct Connect	
Evaluate design alternatives leveraging Direct Connect	- Determine the appropriate region(s) to use in support of private VIFs - Determine the appropriate resiliency strategy - Determine whether customer device colocation at the DX facility is required - Restrict public VIF access to specific regional services - Determine whether multiple sub-1G connections are required - Determine Direct Connect facilities required to provide connection redundancy

Section	Objectives
	- Route Direct Connect traffic to multiple AWS regions with a Direct Connect gateway
Define routing policies for hybrid IT architectures	- Determine a routing policy according to customer requirements concerning high availability, load balancing, traffic shaping, and security - Define link parameters for the routing peers (AWS router peering with an on-premises router) - Define BGP parameters that will be required to implement the routing policy (for example, BGP metrics, AS number) - Implement device-based configuration for route manipulation outside the routing protocol configurations (route filtering, route maps, policy based routing, ACL's, AS manipulations) in order to implement the routing policy - Determine a testing plan - Create router configurations (including BGP configuration, policy/security configurations) - Test the implementation
Design and implement AWS networks - 28%	
Apply AWS networking concepts	
Given customer requirements, define network architectures on AWS	- Explain the purpose and functionality of AWS software-defined networking - Describe how network isolation within AWS works (VPC) and its various components - Calculate the number of IP addresses required - Calculate the number of networks/subnets required and the number of hosts within each network - Classify the level of isolation between subnets - Explain the traffic flow requirements between subnets and in/out of VPC - Outline the requirements of global networks and communication between them - Create VPC, subnets, route tables, and Network ACLs using the AWS console or AWS tools according to customer requirements - Create and attach gateways - Leverage VPC endpoints to meet customer requirements - Design an IP addressing scheme based on the customer requirements and estimate the subnet size (subnet masks) for each subnet - Differentiate the subnets into various logical units based on customer requirements (security isolation, dev/test/prod environment, etc.) - Design a security model for each subnet (Network ACL, public/private subnet)

Section	Objectives
	- Determine the routing characteristics for each subnet - Design a model for connecting a VPC to the public internet (if required) and the security around that based on customer requirements - Design a model for inter-VPC communication (within a region/global) and the security around that based on customer requirements, including AWS Transit Gateway - Select ecosystem solutions that augment AWS services and address customer requirements - Determine if a subnet should be shared with multiple AWS accounts
Propose optimized designs based on the evaluation of an existing implementation	- Map best practice for particular product sets used and identified in HLD or account usage with best practice identified from whitepapers and other AWS reference documentation (for example, using GAP analysis between current deployment and AWS best practices) - Make recommendations around differences between current deployment identified in HLD and AWS best practices - Determine and carry out a change management plan based upon target architecture - Determine an appropriate network optimization strategy (for example, placement groups, enhanced networking, additional ENI, ENA, EFA, ecosystem, EBS Optimized, MTU, throughput to the internet) - Use tools including, GAP Analyses, AWS Reference architectures, AWS whitepapers, AWS Documentation for specific products
Determine network requirements for a specialized workload	- Determine specialized workload(s) and its network requirements (for example, bandwidth requirement, latency requirement, reliability/resiliency requirement, encryption requirements) - Outline components of the solution (for example, diagram, protocols within a solution, VLANs, 801.q, BFD, etc.)
Derive an appropriate architecture based on customer and application requirements	- Map business and application requirements to technical solution - Determine application requirements and translate to technical requirements - Evaluate customer business requirements and compare them to application requirements, mapping differences - Map application flow requirements to network capabilities - Outline a requirements definition document detailing mapped customer requirements to application requirements within the network limitations of the system - Translate customer requirements into AWS components
Evaluate and optimize cost	- Estimate charges based on network design - Estimate charges based on the application data flow (for

Section	Objectives
allocations given a network design and application data flow	example, VPC-E, AWS Key Management Service (AMS KMS) snapshot copy, Amazon S3 cross-region-replication, interAvailability Zone, etc.)
Automate AWS tasks - 8%	
Evaluate automation alternatives within AWS for network deployments	- Manage VPC infrastructure using AWS CloudFormation - Extend network provisioning self-service using AWS Service Catalog - Store Infrastructure-as-Code artifacts in AWS CodeCommit - Audit changes using AWS Config, Amazon Single Notification Service (Amazon SNS), AWS Lambda, and CloudFormation drift detection - Implement overlay network configurations dynamically using Amazon EC2 tags (e.g., multicast), Transit Gateway to route multicast traffic between subnets of attached VPCs - Leverage Lambda as a CloudFormation custom resource for integration with external systems, including IPAM software - Build CloudFormation templates using CloudFormation
Evaluate tool-based alternatives within AWS for network operations and management	- Use scripting (any language) to implement highly available solutions for NAT, firewalls, etc., on EC2 - Use APIs to interrogate current network component status/configuration - Implement EC2 monitoring scripts for Amazon CloudWatch and Amazon CloudWatch Logs - Use the Network Manager console to visualize and monitor the global network - Use VPC traffic mirroring to monitor traffic - Given a customer scenario, utilize CloudWatch to monitor for aggregated metrics and issue notifications and automated fixes
Configure network integration with application services - 14%	
Leverage the capabilities of Amazon Route 53	
Evaluate DNS solutions in a hybrid IT architecture	- Leverage Route 53 aliases with other AWS services. - Select appropriate DNS record types, values, and TTLs - Based on customer requirements, determine the appropriate DNS zone type (public/private) - Describe the differences between public and private hosted zones - Given business requirements, design an appropriate DNS routing strategy - Design and configure a hierarchy of hosted zones and record

Section	Objectives
	sets - Given business requirements, design an effective health check strategy
Determine the appropriate configuration of DHCP within AWS	- Explain key concepts and functionality of DHCP - Describe how DHCP works in AWS (for example, layer 2 broadcast) - Determine appropriate use of DHCP for assignment of IP addresses (for example, secondary IPs) - Configure DHCP option-sets to meet application requirements - Implement solutions where linked applications require different DHCP option-sets
Given a scenario, determine an appropriate load balancing strategy within the AWS ecosystem	- Implement sticky sessions - Identify strategies for retrieving client IP addresses - Configure load balancing of TCP, HTTP, and HTTPS services - Given business and application requirements, design an application health check strategy - Leverage ecosystem (for example, Elastic Load Balancers and third-party solutions) offerings to meet application requirements - Given a scenario, identify an appropriate load balancing solution
Determine a content distribution strategy to optimize for performance	- Identify and map the end-to-end content flows to create a communication matrix - Identify and map the end-to-end DNS flows to create a communication matrix - Given a scenario, determine the appropriate Amazon CloudFront solution (URLs, protocols [HTTP and/or HTTPS], methods) - Determine implementation steps for CloudFront, origin server, and related services – Route 53 (or AWS Global Accelerator where more appropriate), EC2, S3, AWS Direct Connect, etc. - using the AWS console. - Determine measurement methodologies to ensure alignment to business requirements
Reconcile AWS service requirements with network requirements	- Determine how an AWS service communicates over the network (protocols, ports, etc.) - Design the data flow model from an AWS service to the rest of the in-scope components (within AWS service, public internet) - Determine how the application interacts with an AWS service and design the network communication flow between them - Determine the CIDR requirements for an AWS service (if any) - Build the network security model for an AWS service

Section	Objectives
Design and implement for security and compliance - 12%	
Evaluate design requirements for alignment with security and compliance objectives	- Given security requirements, select appropriate AWS tools and eco-system - Implement an isolated subnet architecture - Design and implement an AWS network architecture to meet security and compliance requirements (for example, a demilitarized zone (DMZ), three tier) - Develop a threat model and identify an appropriate mitigation strategy for a given implementation - Identify security vulnerabilities and/or compliance violations in a given scenario
Evaluate monitoring strategies in support of security and compliance objectives	- Create and interact with a VPC flow log - Use AWS CloudTrail for monitoring attempted/completed networking resource changes - Implement automated alarms using CloudWatch - Implement customized metrics using CloudWatch - Determine an overall security/monitoring solution based on customer business requirements - Analyze administration and security tools (for example, CloudTrail, CloudWatch, instance logs, cmdb) for authorized changes (potentially on InfoSec side)
Evaluate AWS security features for managing network traffic	- Contrast and compare functional capabilities of security groups, Network ACLs, and IAM policies - Determine the network security requirements for the application - Determine and map the application flows to create policy enforcement objects (security groups, Network ACLs, or IAM policies) - Determine the appropriate application of security groups versus Network ACLs, versus IAM policies - Implement security groups, Network ACLs, and IAM policies according to the security requirements (for example. restrict who can make changes to networking resources including VPCs, subnets, routing tables, security groups, Network ACLs, VGW, IGW, etc.) - Test compliance with the stated requirements - Outline the network security solution (for example, diagram, protocols allowed/denied through security groups, Network ACLs, permissions matrix for allowed/denied actions on networking resources) - Customize implementation based on business requirements
Utilize encryption technologies to secure network communications	- Determine the applicable compliance requirements for encryption - Determine what application data needs to be encrypted - Determine the data flow and systems that will store that data

Section	Objectives
	- Implement pertinent encryption solution(s) to encrypt data in transit and data at rest (S3, Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Solution (Amazon RDS), and custom solutions on EC2) - Implement the encryption key management solution (using AWS Key Management Service (AWS KMS) or a customer owned third-party solution) - Implement auditing of access to encrypted data - Test to verify compliance - Outline the components of the solution (encryption, key management, audit controls etc.) - Identify any application performance impact due to encryption and recommend a mitigating solution
Manage, optimize, and troubleshoot the network - 14%	
Given a scenario, troubleshoot and resolve a network issue	- Review route tables to locate black holes or lack of route propagation - Interrogate on-premises devices (VPN or Direct Connect) to identify network reachability - Validate L1-L4 reachability and investigate potential cause of failure at each layer - Given standard diagnostic information, identify implementation errors or faults in the AWS network configuration - Assess appropriate use of security groups and Network ACLs (permit compared to deny) - Use VPC flow logs to locate configuration errors or potential security holes in security groups or Network ACLs

AWS ANS-C00 Sample Questions:

Question: 1

A company is extending its on-premises data center to AWS. Peak traffic is expected to range between 1 Gbps and 2 Gbps.

A network engineer must ensure that there is sufficient bandwidth between AWS and the data center to handle peak traffic. The solution should be highly available and cost effective.

What should be implemented to address these needs?

a) Deploy a 10 Gbps AWS Direct Connect connection with an IPsec VPN backup.
b) Deploy two 1 Gbps AWS Direct Connect connections in a link aggregation group.
c) Deploy two 1 Gbps AWS Direct Connect connections in a link aggregation group to two different Direct Connect locations.
d) Deploy a 10 Gbps AWS Direct Connect connection to two different Direct Connect locations.

Answer: c

Question: 2

A company is creating new features for its ecommerce website. These features will be deployed as microservices using different domain names for each service. The company requires the use of HTTPS for all its public-facing websites. The application requires the client's source IP.

Which combination of actions should be taken to accomplish this?

(Select TWO.)

a) Use a Network Load Balancer to distribute traffic to each service.
b) Use an Application Load Balancer to distribute traffic to each service.
c) Configure the application to retrieve client IPs using the X-Forwarded-For header.
d) Configure the application to retrieve client IPs using the X-Forwarded-Host header.
e) Configure the application to retrieve client IPs using the PROXY protocol header.

Answer: b, c

Question: 3

A network engineer needs to limit access to the company's Amazon S3 bucket to specific source networks. What should the network engineer do to accomplish this?

a) Create an ACL on the S3 bucket, limiting access to the CIDR blocks of the specified networks.
b) Create a bucket policy on the S3 bucket, limiting access to the CIDR blocks of the specified networks using a condition statement.
c) Create a security group allowing inbound access to the CIDR blocks of the specified networks and apply the security group to the S3 bucket.
d) Create a security group allowing inbound access to the CIDR blocks of the specified networks, create a S3 VPC endpoint, and apply the security group to the VPC endpoint.

Answer: b

Question: 4

A network engineer is architecting a high performance computing solution on AWS. The system consists of a cluster of Amazon EC2 instances that require low-latency communications between them.

Which method will meet these requirements?

a) Launch instances into a single subnet with a size equal to the number of instances required for the cluster.
b) Create a cluster placement group. Launch Elastic Fabric Adapter (EFA)-enabled instances into the placement group.
c) Launch Amazon EC2 instances with the largest available number of cores and RAM. Attach Amazon EBS Provisioned IOPS (PIOPS) volumes. Implement a shared memory system across all instances in the cluster.
d) Choose an Amazon EC2 instance type that offers enhanced networking. Attach a 10 Gbps non-blocking elastic network interface to the instances.

Answer: b

Question: 5

A company's on-premises network has an IP address range of 11.11.0.0/16. Only IPs within this network range can be used for inter-server communication. The IP address range 11.11.253.0/24 has been allocated for the cloud.

A network engineer needs to design a VPC on AWS. The servers within the VPC should be able to communicate with hosts both on the internet and on-premises through a VPN connection.

Which combination of configuration steps meet these requirements?

(Select TWO.)

a) Set up the VPC with an IP address range of 11.11.253.0/24.
b) Set up the VPC with an RFC 1918 private IP address range (for example, 10.10.10.0/24). Set up a NAT gateway to do translation between 10.10.10.0/24 and 11.11.253.0/24 for all outbound traffic.
c) Set up a VPN connection between a virtual private gateway and an on-premises router. Set the virtual private gateway as the default gateway for all traffic. Configure the on-premises router to forward traffic to the internet.
d) Set up a VPN connection between a virtual private gateway and an on-premises router. Set the virtual private gateway as the default gateway for traffic destined to 11.11.0.0/24. Add a VPC subnet route to point the default gateway to an internet gateway for internet traffic.
e) Set up the VPC with an RFC 1918 private IP address range (for example, 10.10.10.0/24). Set the virtual private gateway to do a source IP translation of all outbound packets to 11.11.0.0/16.

Answer: a, c

Question: 6

A company has an application that processes confidential data. The data is currently stored in an onpremises data center.

A network engineer is moving workloads to AWS, and needs to ensure confidentiality and integrity of the data in transit to AWS. The company has an existing AWS Direct Connect connection.

Which combination of steps should the network engineer perform to set up the most cost-effective connection between the on-premises data center and AWS?

(Select TWO.)

a) Attach an internet gateway to the VPC.
b) Configure a public virtual interface on the AWS Direct Connect connection.
c) Configure a private virtual interface to the virtual private gateway.
d) Set up an IPsec tunnel between the customer gateway and a software VPN on Amazon EC2.
e) Set up a Site-to-Site VPN between the customer gateway and the virtual private gateway.

Answer: b, e

Question: 7

A network engineer needs to design a solution for an application running on an Amazon EC2 instance to connect to a publicly accessible Amazon RDS Multi-AZ DB instance in a different VPC and Region. Security requirements mandate that the traffic not traverse the internet.

Which configuration will ensure that the instances communicate privately without routing traffic over the internet?

a) Create a peering connection between the VPCs and update the routing tables to route traffic between the VPCs. Enable DNS resolution support for the VPC peering connection. Configure the application to connect to the DNS endpoint of the DB instance.
b) Create a gateway endpoint to the DB instance. Update the routing tables in the application VPC to route traffic to the gateway endpoint.
c) Configure a transit VPC to route traffic between the VPCs privately. Configure the application to connect to the DNS endpoint of the DB instance.
d) Create a NAT gateway in the same subnet as the EC2 instances. Update the routing tables in the application VPC to route traffic through the NAT gateway to the DNS endpoint of the DB instance.

Answer: a

Question: 8

A company has implemented a critical environment on AWS. For compliance purposes, a network engineer needs to verify that the Amazon EC2 instances are using a specific approved security group and belong to a specific VPC.

The configuration history of the instances should be recorded and, in the event of any compliance issues, the instances should be automatically stopped.

What should be done to meet these requirements?

a) Enable AWS CloudTrail and create a custom Amazon CloudWatch alarm to perform the required checks. When the CloudWatch alarm is in a failed state, trigger the stop this instance action to stop the noncompliant EC2 instance.
b) Configure a scheduled event with AWS CloudWatch Events to invoke an AWS Lambda function to perform the required checks. In the event of a noncompliant resource, invoke another Lambda function to stop the EC2 instance.
c) Configure an event with AWS CloudWatch Events for an EC2 instance state-change notification that triggers an AWS Lambda function to perform the required checks. In the event of a noncompliant resource, invoke another Lambda function to stop the EC2 instance.
d) Enable AWS Config and create custom AWS Config rules to perform the required checks. In the event of a noncompliant resource, use a remediation action to execute an AWS Systems Manager document to stop the EC2 instance.

Answer: d

Question: 9

A company's internal security team receives a request to allow Amazon S3 access from inside the corporate network. All external traffic must be explicitly allowed through the corporate firewalls.

How can the security team grant this access?

a) Schedule a script to download the Amazon S3 IP prefixes from AWS developer forum announcements. Update the firewall rules accordingly.
b) Schedule a script to download and parse the Amazon S3 IP prefixes from the ip-ranges.json file. Update the firewall rules accordingly.
c) Schedule a script to perform a DNS lookup on Amazon S3 endpoints. Update the firewall rules accordingly.
d) Connect the data center to a VPC using AWS Direct Connect. Create routes that forward traffic from the data center to an Amazon S3 VPC endpoint.

Answer: b

Question: 10

A company's compliance requirements specify that web application logs must be collected and analyzed to identify any malicious activity.

A network engineer also needs to monitor for remote attempts to change the network interface of web instances.

Which services and configurations will meet these requirements?

a) Install the Amazon CloudWatch Logs agent on the web instances to collect application logs. Use VPC Flow Logs to send data to CloudWatch Logs. Use CloudWatch Logs metric filters to define the patterns to look for in the log data.
b) Configure AWS CloudTrail to log all management and data events to a custom Amazon S3 bucket and Amazon CloudWatch Logs. Use VPC Flow Logs to send data to CloudWatch Logs. Use CloudWatch Logs metric filters to define the patterns to look for in the log data.
c) Configure AWS CloudTrail to log all management events to a custom Amazon S3 bucket and Amazon CloudWatch Logs. Install the Amazon CloudWatch Logs agent on the web instances to collect application logs. Use CloudWatch Logs Insights to define the patterns to look for in the log data.
d) Enable AWS Config to record all configuration changes to the web instances. Configure AWS CloudTrail to log all management and data events to a custom Amazon S3 bucket. Use Amazon Athena to define the patterns to look for in the log data stored in Amazon S3.

Answer: c

Study Guide to Crack AWS Advanced Networking Specialty ANS-C00 Exam:

- Getting details of the ANS-C00 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-C00 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-C00 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-C00 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-C00 practice tests is must. Continuous practice will make you an expert in all syllabus areas.