aws training and certification

AWS Certified Advanced Networking – Specialty (ANS-C00) Exam Guide

Introduction

The AWS Certified Advanced Networking – Specialty (ANS-C00) exam is intended for individuals who perform an AWS Networking Specialist's role. The exam validates advanced technical skills and experience for design and implementation of AWS and hybrid IT network architectures at scale. The exam is for individuals who perform complex networking tasks. It validates an individual's ability to do the following:

- Design, develop, and deploy cloud-based solutions by using AWS
- Implement core AWS services according to basic architectural best practices
- Design and maintain network architecture for all AWS services
- Use tools to automate AWS networking tasks

Target candidate description

The target candidate has a level of expertise in advanced networking that significantly exceeds expectations of an AWS Certified Solutions Architect – Professional. The target candidate is likely an experienced solutions architect (5–7 years or more) who has a networking focus and who has design, implementation, and troubleshooting expertise. The target candidate likely has a background in infrastructure engineering at scale (for example, complex SMB, enterprise, ISP, LAN/WAN environments).

Recommended general IT knowledge

The target candidate should have knowledge in the following areas:

- Advanced networking architectures and interconnectivity options (for example, IP VPN, multiprotocol label switching [MPLS], virtual private LAN service [VPLS])
- Networking technologies within the Open Systems Interconnection (OSI) model, and how they affect implementation decisions
- Development of automation scripts and tools. Design, implementation, and optimization of the following:
    - Routing architectures (including static and dynamic)
    - Multi-Region solutions for a global enterprise
    - Highly available connectivity solutions (for example, AWS Direct Connect, VPN)
- CIDR and subnetting (IPv4 and IPv6)
- IPv6 transition challenges
- Generic solutions for network security features, including AWS WAF, intrusion detection systems (IDS), intrusion prevention systems (IPS), DDoS protection, and economic denial of service/sustainability (EDoS)

Recommended AWS knowledge

The target candidate should have the following knowledge:

- Professional experience using AWS technology
- AWS security best practices

- AWS storage options and their underlying consistency models
- AWS networking nuances and how they relate to the integration of AWS services

What is considered out of scope for the target candidate?

The following is a non-exhaustive list of related job tasks that the target candidate is not expected to be able to perform. These items are considered out of scope for the exam:

- Possess application development skills
- Possess SysOps skills beyond that of the Solutions Architect – Professional level

Exam content

Response types

There are two types of questions on the exam:

- **Multiple choice:** Has one correct response and three incorrect responses (distractors)
- **Multiple response:** Has two or more correct responses out of five or more response options

Select one or more responses that best complete the statement or answer the question. Distractors, or incorrect answers, are response options that a candidate with incomplete knowledge or skill might choose. Distractors are generally plausible responses that match the content area.

Unanswered questions are scored as incorrect; there is no penalty for guessing. The exam includes 50 questions that will affect your score.

Unscored content

The exam includes 15 unscored questions that do not affect your score. AWS collects information about candidate performance on these unscored questions to evaluate these questions for future use as scored questions. These unscored questions are not identified on the exam.

Exam results

The AWS Certified Advanced Networking – Specialty exam is a pass or fail exam. The exam is scored against a minimum standard established by AWS professionals who follow certification industry best practices and guidelines.

Your results for the exam are reported as a scaled score of 100–1,000. The minimum passing score is 750. Your score shows how you performed on the exam as a whole and whether or not you passed. Scaled scoring models help equate scores across multiple exam forms that might have slightly different difficulty levels.

Your score report may contain a table of classifications of your performance at each section level. This information is intended to provide general feedback about your exam performance. The exam uses a compensatory scoring model, which means that you do not need to achieve a passing score in each section. You need to pass only the overall exam.

Each section of the exam has a specific weighting, so some sections have more questions than others. The table contains general information that highlights your strengths and weaknesses. Use caution when interpreting section-level feedback.

Content outline

This exam guide includes weightings, test domains, and objectives for the exam. It is not a comprehensive listing of the content on the exam. However, additional context for each of the objectives is available to help guide your preparation for the exam. The following table lists the main content domains and their weightings. The table precedes the complete exam content outline, which includes the additional context. The percentage in each domain represents only scored content.

Domain	% of Exam
Domain 1: Design and implement hybrid IT network architectures at scale	24%
Domain 2: Design and implement AWS networks	28%
Domain 3: Automate AWS tasks	8%
Domain 4: Configure network integration with application services	14%
Domain 5: Design and implement for security and compliance	12%
Domain 6: Manage, optimize, and troubleshoot the network	14%
TOTAL	**100%**

Domain 1: Design and implement hybrid IT network architectures at scale

1.1 Apply procedural concepts for the implementation of connectivity for hybrid IT architecture

1.2 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

1.3 Explain the process to extend connectivity using Direct Connect

1.4 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
- Route Direct Connect traffic to multiple AWS regions with a Direct Connect gateway

1.5 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

Domain 2: Design and implement AWS networks

2.1 Apply AWS networking concepts

2.2 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)
- 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

2.3 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

2.4 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.)

2.5 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

2.6 Evaluate and optimize cost allocations given a network design and application data flow
- Estimate charges based on network design
- Estimate charges based on the application data flow (for example, VPC-E, AWS Key Management Service (AMS KMS) snapshot copy, Amazon S3 cross-region-replication, inter-Availability Zone, etc.)

Domain 3: Automate AWS tasks

3.1 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

3.2 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

Domain 4: Configure network integration with application services

4.1 Leverage the capabilities of Amazon Route 53

4.2 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 sets
- Given business requirements, design an effective health check strategy

4.3 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

4.4 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

4.5 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

4.6 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

Domain 5: Design and implement for security and compliance

5.1 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

5.2 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)

5.3 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

5.4 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

- 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

Domain 6: Manage, optimize, and troubleshoot the network

6.1 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