# AWS CERTIFIED ADVANCED NETWORKING SPECIALTY PRACTICE EXAM (SAMPLE)

## STUDY GUIDE



## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE**

https://
awscertifiedadvancednetworkingspecialty.examzify.com

**Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.**

**ALL RIGHTS RESERVED.**

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

# Table of Contents


Copyright ..... 1

Table of Contents ..... 2

Introduction ..... 3

How to Use This Guide ..... 4

Questions ..... 5

Answers ..... 8

Explanations ..... 10

Next Steps ..... 16


SAMPLE

# Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

# How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

### 1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

### 2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

### 3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

### 4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

### 5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

### 6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

# Questions

SAMPLE

1. **What can help in achieving lower latency between AWS resources across different regions?**

   A. Utilizing a public subnet for all instances

   B. Using cross-region VPC peering

   C. Implementing AWS Lambda functions

   D. Establishing a local transit hub

2. **What is the primary benefit of using multiple availability zones in a VPC architecture?**

   A. Reduced cost for using AWS resources

   B. Data compliance with regulations

   C. Enhanced disaster recovery and availability

   D. Improved performance for single-instance applications

3. **What feature allows Amazon Route 53 to route traffic to healthy endpoints only?**

   A. Health checks

   B. DNS failover

   C. Geolocation routing

   D. Weighted routing

4. **Which AWS feature allows the application servers to scale based on demand?**

   A. Elastic Load Balancing

   B. Auto Scaling

   C. EC2 Instance Scheduler

   D. Amazon CloudWatch

5. **What is the best design for an IPSec VPN that prioritizes sensitive application traffic?**

   A. Terminate a VPN connection on an Amazon EC2 instance with a standard configuration

   B. Use a dedicated hardware appliance for the VPN connection

   C. Terminate on an EC2 instance with software supporting QoS and use DSCP markings

   D. Separate the sensitive application traffic into a different subnet

SAMPLE

**6. What is the function of a Network ACL in Amazon VPC?**

A. To provide routing for internet traffic

B. To provide an additional layer of security by controlling inbound and outbound traffic at the subnet level

C. To manage DNS records

D. To allocate IP addresses within subnets

**7. What is a recommended approach to scale up network performance for high throughput transfers?**

A. Increase the network bandwidth

B. Distribute the flows across many instances

C. Switch to a different AWS region

D. Optimize application code for network efficiency

**8. What does AWS CloudTrail do in terms of networking?**

A. Increases network bandwidth

B. Records API calls made on your account for auditing and compliance purposes

C. Monitors real-time traffic

D. Optimizes load balancers

**9. Which option minimizes network jitter and latency when connecting an on-premises network to AWS APIs?**

A. Public VIF

B. AWS Virtual Private Network

C. AWS Direct Connect public VIF

D. AWS Site-to-Site VPN

**10. Which feature allows you to filter traffic to and from an AWS resource based on rules?**

A. Network ACLs

B. Security Groups

C. Route 53

D. VPC Peering

SAMPLE

# Answers

SAMPLE

1. D
2. C
3. A
4. B
5. C
6. B
7. B
8. B
9. C
10. B

SAMPLE

# Explanations

SAMPLE

## 1. What can help in achieving lower latency between AWS resources across different regions?

A. Utilizing a public subnet for all instances

B. Using cross-region VPC peering

C. Implementing AWS Lambda functions

D. Establishing a local transit hub

*Establishing a local transit hub can significantly contribute to achieving lower latency between AWS resources across different regions. A local transit hub enables efficient routing of traffic between different VPCs and AWS services, facilitating optimized pathways for inter-region communication. By centralizing the traffic management in a transit hub, data can be transferred more quickly and reliably across regions, reducing latency compared to more direct but less optimized connection methods. In contrast, while cross-region VPC peering allows direct communication between resources in different VPCs across regions, it does not inherently optimize latency as effectively as a centralized transit solution. Utilizing a public subnet for all instances focuses more on accessibility rather than on minimizing latency, and implementing AWS Lambda functions may not directly contribute to reducing latency between regions as they are designed for event-based processing rather than facilitating networking connections.*

## 2. What is the primary benefit of using multiple availability zones in a VPC architecture?

A. Reduced cost for using AWS resources

B. Data compliance with regulations

C. Enhanced disaster recovery and availability

D. Improved performance for single-instance applications

*The primary benefit of using multiple availability zones in a Virtual Private Cloud (VPC) architecture is enhanced disaster recovery and availability. By deploying resources across multiple availability zones, you ensure that your applications are more resilient to failures. Each availability zone operates independently, with its own power, cooling, and physical security, which means that if one zone experiences an issue, the resources in the other zones can continue to function, minimizing downtime and maintaining service availability. Additionally, this architecture supports a better disaster recovery strategy. In the event of a localized disaster affecting one zone, having applications and data distributed across multiple zones allows for quicker recovery and continuity of operations. This strategy is especially critical for mission-critical applications where uptime is essential. Reducing costs, ensuring data compliance, and improving performance for single-instance applications, while valuable aspects, do not capture the primary benefit provided by multiple availability zones. These considerations can come into play depending on specific use cases, but they do not address the core advantage of using multiple availability zones for resilience and uptime.*

SAMPLE

## 3. What feature allows Amazon Route 53 to route traffic to healthy endpoints only?

A. Health checks

B. DNS failover

C. Geolocation routing

D. Weighted routing

*Amazon Route 53 uses health checks to assess the state of specified endpoints, such as web servers or applications, to determine whether they are healthy and can handle traffic. This feature is essential for maintaining high availability and reliability in applications by ensuring that only endpoints that are functioning correctly receive incoming requests. When Route 53 performs a health check, it sends periodic requests to the endpoint and monitors the responses. If an endpoint does not respond as expected or fails the health check, Route 53 can automatically stop routing traffic to that endpoint, thereby preventing user requests from being directed to unavailable resources. This mechanism enhances the overall resilience of applications hosted on AWS. Other options do not inherently ensure that traffic is directed solely to healthy endpoints. For instance, DNS failover is a feature that works in conjunction with health checks but is not a standalone feature. Geolocation routing and weighted routing are methods of directing traffic based on location or specific weightings, which do not assess the health of the endpoints involved. Thus, the fundamental mechanism that enables Route 53 to route traffic appropriately based on endpoint health is the health checks feature.*

## 4. Which AWS feature allows the application servers to scale based on demand?

A. Elastic Load Balancing

B. Auto Scaling

C. EC2 Instance Scheduler

D. Amazon CloudWatch

*Auto Scaling is the feature that allows application servers to automatically adjust the number of instances in response to demand. This means that as the application's load increases, Auto Scaling can launch additional EC2 instances to handle the increased traffic or workload. Conversely, it can also terminate instances when demand decreases, ensuring that resources are not wasted and costs are optimized. Auto Scaling works in conjunction with CloudWatch, which monitors application performance and triggers scaling actions based on predefined metrics or thresholds. This integration ensures that the scaling process is responsive to real-time data about the application's needs, providing a robust and flexible way to maintain performance during varying levels of demand. While Elastic Load Balancing distributes incoming application traffic across multiple targets (like EC2 instances), it does not inherently provide scaling capabilities; it works in conjunction with Auto Scaling to ensure that the load is balanced across the available instances. The EC2 Instance Scheduler is designed for scheduling specific start and stop times for EC2 instances and is not focused on dynamic scaling based on demand. Amazon CloudWatch is primarily a monitoring and observability service, offering data and insights that can inform Auto Scaling decisions but does not perform the scaling action itself.*

SAMPLE

## 5. What is the best design for an IPSec VPN that prioritizes sensitive application traffic?

A. Terminate a VPN connection on an Amazon EC2 instance with a standard configuration

B. Use a dedicated hardware appliance for the VPN connection

C. Terminate on an EC2 instance with software supporting QoS and use DSCP markings

D. Separate the sensitive application traffic into a different subnet

*Terminating the VPN connection on an EC2 instance with software that supports Quality of Service (QoS) and using Differentiated Services Code Point (DSCP) markings is the best design for prioritizing sensitive application traffic. This approach enables the implementation of traffic management policies that can prioritize sensitive application data over other types of traffic. By leveraging QoS, you can define and enforce which types of traffic should receive higher priority, ensuring that sensitive application data gets the necessary bandwidth and low latency. DSCP markings help in classifying and managing packets as they traverse the network, allowing routers and switches to recognize the importance of the traffic and handle it accordingly. This design provides the flexibility to adjust traffic prioritization based on the application's needs and allows for better performance and reliability for critical data transmissions. Additionally, it retains the ability to scale and adapt within the AWS cloud environment, making it a more versatile solution. Using a dedicated hardware appliance for the VPN connection, for instance, might offer robust performance and security features but may not provide the same level of control over traffic prioritization as QoS configurations allow. While terminating on an EC2 instance with a standard configuration can work for general purposes, it lacks the advanced traffic management capabilities necessary for prioritizing sensitive application traffic*

## 6. What is the function of a Network ACL in Amazon VPC?

A. To provide routing for internet traffic

B. To provide an additional layer of security by controlling inbound and outbound traffic at the subnet level

C. To manage DNS records

D. To allocate IP addresses within subnets

*The function of a Network ACL (Access Control List) in Amazon VPC is to provide an additional layer of security by controlling inbound and outbound traffic at the subnet level. Network ACLs act as a firewall that helps regulate traffic flow based on defined rules. This means that for every packet of data trying to enter or exit a subnet, the Network ACL checks the rules configured to determine whether to allow or deny the traffic. Network ACLs operate independently of security groups, allowing for a more granular control mechanism. While security groups are associated with instances and function as stateful firewalls, Network ACLs apply to the entire subnet and are stateless, meaning they must explicitly allow both incoming and outgoing traffic. This dual-layered security approach enhances the protection of resources within a VPC. In contrast, the other options do not accurately describe the primary function of a Network ACL. For example, routing for internet traffic is managed by route tables, not Network ACLs. Managing DNS records is the role of Route 53 or similar services, and the allocation of IP addresses within subnets is performed through the VPC's built-in IP addressing mechanism, specifically using CIDR blocks. Therefore, the choice regarding the control of inbound and outbound traffic at the subnet level*

SAMPLE

## 7. What is a recommended approach to scale up network performance for high throughput transfers?

A. Increase the network bandwidth

B. Distribute the flows across many instances

C. Switch to a different AWS region

D. Optimize application code for network efficiency

*Distributing the flows across many instances is a recommended approach to scale up network performance for high throughput transfers because it allows for parallel processing of data. When multiple instances handle different parts of the workload, the overall throughput can significantly improve. This technique takes advantage of horizontal scaling, which effectively balances the load and can help achieve higher bandwidth utilization. By leveraging multiple instances, you not only spread out the demands on your network but also take advantage of the capacity of each instance, allowing for simultaneous transfers. This is particularly applicable in scenarios where data can be processed in parallel, thereby reducing bottlenecks that might occur if a single instance were to manage all the traffic. Increasing network bandwidth is a valid consideration but may not always be feasible or cost-effective, and simply enhancing bandwidth doesn't necessarily mean that the actual data transfer will improve if it's bottlenecked by limited processing capabilities or inefficient coding practices. Switching to a different AWS region does not inherently improve network performance, as it may introduce additional latencies and complexities due to geographical distance and routing. Furthermore, optimizing application code for network efficiency is crucial but usually addresses inefficiencies rather than scaling throughput in a direct manner. Thus, distributing flows across many instances effectively enhances scalability and performance for high throughput transfers, making it*

## 8. What does AWS CloudTrail do in terms of networking?

A. Increases network bandwidth

B. Records API calls made on your account for auditing and compliance purposes

C. Monitors real-time traffic

D. Optimizes load balancers

*AWS CloudTrail plays a critical role in network security and compliance by recording API calls made on your AWS account. It automatically captures information about the requests that are made to AWS services, such as which service was called, by whom, and from which IP address. This data provides comprehensive logs that help in auditing and investigating any incidents or changes that may have occurred within your AWS environment. By maintaining a detailed record of API activity, CloudTrail assists organizations in ensuring compliance with internal policies and regulatory requirements, as well as in analyzing potential security incidents. This information can also be essential for troubleshooting issues within the networking and overall AWS infrastructure, making it invaluable for maintaining a secure and efficient cloud environment. The other options do not reflect the capabilities of AWS CloudTrail; its purpose is centered on logging API calls rather than enhancing bandwidth, monitoring real-time traffic, or performing load balancer optimizations. Therefore, recognizing CloudTrail's function in the context of networking emphasizes its importance in governance, risk management, and compliance within AWS.*

SAMPLE

## 9. Which option minimizes network jitter and latency when connecting an on-premises network to AWS APIs?

A. Public VIF

B. AWS Virtual Private Network

C. AWS Direct Connect public VIF

D. AWS Site-to-Site VPN

*Choosing AWS Direct Connect public VIF as the method for connecting an on-premises network to AWS APIs is optimal for minimizing network jitter and latency. AWS Direct Connect establishes a dedicated network connection from your premises directly to AWS. This provides a more stable and consistent connection compared to internet-based options, which can experience fluctuations in performance due to variable internet traffic. With Direct Connect, traffic does not traverse the public internet, which significantly reduces the chances of jitter - the variability in packet arrival time that can affect the quality of real-time applications. The dedicated line also contributes to consistently lower latency compared to other methods like VPNs, where traffic may be subject to additional processing and routing delays caused by the complexities of internet transit. In contrast, options like public VIF and AWS Site-to-Site VPN typically rely on the public internet for connectivity, which means they inherit the web's inherent latency and jitter characteristics from shared bandwidth and variable routing paths. While these solutions provide secure connections, they do not offer the same level of performance consistency that Direct Connect provides. Thus, for critical applications requiring minimal jitter and latency, AWS Direct Connect public VIF is the superior choice.*

## 10. Which feature allows you to filter traffic to and from an AWS resource based on rules?

A. Network ACLs

B. Security Groups

C. Route 53

D. VPC Peering

*The correct answer, Security Groups, are virtual firewalls for your Amazon EC2 instances and other resources that control inbound and outbound traffic based on defined rules. Each security group acts at the instance level and provides a more granular approach to traffic filtering. You can specify rules that permits or denies certain types of traffic based on protocol, port number, and source or destination IP address. In AWS, security groups are stateful, meaning that if an incoming request is allowed, the response is automatically allowed regardless of outbound rules. This characteristic is essential for simplifying the management of allowed traffic for EC2 instances. By using security groups, you can easily establish a tightly controlled environment, allowing only the necessary traffic to interact with your AWS resources while maintaining overall security. This is essential for following best practices in cloud security. While Network ACLs also filter traffic based on rules, they operate at the subnet level rather than the instance level, and they are stateless. Route 53, on the other hand, is a domain name system (DNS) service and does not provide traffic filtering features. VPC Peering is a networking connection between two VPCs allowing them to communicate, but it does not involve filtering traffic through rules.*

SAMPLE

# Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://awscertifiedadvancednetworkingspecialty.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE