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

Table of Contents

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.

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!

Questions

1. **Which tool allows you to visualize your VPC network and node relationships?**

   A. AWS Architecture Icons

   B. AWS Network Manager

   C. AWS Trusted Advisor

   D. AWS Cost Explorer

2. **What is the primary advantage of using the Data Plane Development Kit (DPDK) over enhanced networking on AWS?**

   A. DPDK integrates with AWS management tools

   B. DPDK reduces operating system overhead for networking

   C. DPDK is easier to implement than enhanced networking

   D. DPDK guarantees higher short-term bandwidth

3. **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

4. **What AWS feature allows the creation of a dual-homed instance in a VPC?**

   A. Subnets

   B. Elastic Load Balancer

   C. Elastic Network Interface

   D. NAT Gateway

5. **What feature of the Elastic Load Balancer (ELB) is utilized in the described application architecture?**

   A. Sticky sessions

   B. Round-robin configuration

   C. Session affinity

   D. URL-based routing

6. What feature of AWS Elastic Load Balancing helps to automatically distribute incoming application traffic across multiple targets?

A. Health checks

B. Load balancing algorithm

C. Routing table

D. Traffic shaping

7. Which security feature within a VPC controls stateful traffic?

A. Network Access Control Lists

B. Route Tables

C. Security Groups

D. VPN Connections

8. 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

9. How can you extend your on-premises network into AWS?

A. By using AWS VPN or AWS Direct Connect

B. By setting up a CloudFormation stack

C. By utilizing Amazon RDS for database replication

D. By configuring public IP addresses

10. What is the main function of AWS Shield Advanced?

A. To manage and allocate cloud resources effectively

B. To provide enhanced DDoS protection and a 24x7 Security Operations Center (SOC) team

C. To automate cloud infrastructure updates

D. To enhance data storage options

Answers

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

Explanations

1. Which tool allows you to visualize your VPC network and node relationships?

A. AWS Architecture Icons

B. AWS Network Manager

C. AWS Trusted Advisor

D. AWS Cost Explorer

The correct option for visualizing your VPC network and node relationships is AWS Network Manager. AWS Network Manager is specifically designed to help you manage and visualize global networks, including VPCs. It provides a comprehensive view of your network topology, making it easier to understand how your VPCs, VPN connections, and Transit Gateways interconnect. This tool enables network administrators to visualize network architecture, monitor performance, and gain insights into network-related metrics. Using AWS Network Manager, you can see how different components of your network interact, detect bottlenecks, and optimize your configuration, which is essential for advanced networking tasks. This visualization capability helps enhance troubleshooting and ensure that network resources are utilized effectively. The other options listed do serve different purposes. AWS Architecture Icons are graphical elements used for drawing architecture diagrams but do not provide a direct visualization of network and node relationships. AWS Trusted Advisor focuses on best practices for AWS accounts, offering recommendations in areas like cost optimization and security, rather than network visualization. AWS Cost Explorer helps analyze and visualize your AWS spending and usage over time, which is unrelated to network topology or VPC visualization.

2. What is the primary advantage of using the Data Plane Development Kit (DPDK) over enhanced networking on AWS?

A. DPDK integrates with AWS management tools

B. DPDK reduces operating system overhead for networking

C. DPDK is easier to implement than enhanced networking

D. DPDK guarantees higher short-term bandwidth

The primary advantage of using the Data Plane Development Kit (DPDK) over enhanced networking on AWS is that DPDK reduces operating system overhead for networking. This is significant because DPDK allows applications to bypass the kernel network stack, which typically incurs latency and processing overhead. By using DPDK, network functions can be implemented in user-space applications, resulting in lower processing delays and faster packet processing. This streamlined approach can dramatically improve throughput and efficiency for high-performance networking applications. In contrast, enhanced networking features provided by AWS utilize additional virtualized hardware capabilities to enhance performance but still operate within the constraints of the operating system's stack. While these features improve network performance to a degree, they do not achieve the same level of efficiency and performance as the user-space operation model offered by DPDK. Thus, in scenarios where maximizing network performance and minimizing latency are critical, DPDK represents a more advantageous choice than enhanced networking on AWS.

3. 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.

4. What AWS feature allows the creation of a dual-homed instance in a VPC?

A. Subnets

B. Elastic Load Balancer

C. Elastic Network Interface

D. NAT Gateway

The correct response is that an Elastic Network Interface (ENI) allows for the creation of a dual-homed instance in a Virtual Private Cloud (VPC). An ENI is a virtual network interface that can be attached to an instance in a VPC. When you attach more than one Elastic Network Interface to an instance, you effectively create a dual-homed or multi-homed setup. This allows the instance to connect to multiple subnets or network segments, which can be an essential requirement for scenarios such as high availability, inter-subnet communication, or separating network traffic for security or performance reasons. An instance can have multiple network interfaces, and each ENI can be assigned to different subnets, allowing for flexible networking and configuration options. This capability is vital for distributing workloads across different subnets or providing redundancy if one interface or subnet becomes unavailable. Other options, such as subnets, Elastic Load Balancers, and NAT Gateways, serve different purposes within an AWS environment. Subnets are used to segment a VPC's IP address range, Elastic Load Balancers distribute incoming traffic among multiple instances, and NAT Gateways are used for providing internet access to instances in a private subnet, but none of these features enable an instance to have

5. What feature of the Elastic Load Balancer (ELB) is utilized in the described application architecture?

A. Sticky sessions

B. Round-robin configuration

C. Session affinity

D. URL-based routing

In the context of Elastic Load Balancers (ELB), the feature that is recognized in application architectures often centers on how traffic is managed and distributed among various instances. The round-robin configuration allows the load balancer to distribute incoming requests evenly across multiple targets, ensuring an effective load distribution. This method is significant in keeping workloads balanced, particularly in situations where each request is independent of others. By using round-robin, all instances behind the load balancer receive an equal share of traffic over time, thus optimizing resource utilization and enhancing overall application performance. In contrast, sticky sessions or session affinity refer to keeping a user's requests directed to the same instance, which is useful for maintaining state but does not focus on equal load distribution. URL-based routing, while beneficial for directing specific requests to certain backend services based on URL paths, does not inherently provide a mechanism for ensuring balanced traffic across multiple instances. Thus, the round-robin configuration is a foundational feature for achieving load balancing in applications, aligning perfectly with the need for an efficient response to varying levels of incoming traffic.

6. What feature of AWS Elastic Load Balancing helps to automatically distribute incoming application traffic across multiple targets?

A. Health checks

B. Load balancing algorithm

C. Routing table

D. Traffic shaping

The feature of AWS Elastic Load Balancing that helps to automatically distribute incoming application traffic across multiple targets is the load balancing algorithm. This algorithm plays a crucial role in determining how requests are allocated to various targets (such as EC2 instances) within the load balancer. It ensures that traffic is evenly balanced, which contributes to optimized resource utilization and improved application performance. When incoming traffic hits the load balancer, the load balancing algorithm selects a target based on predefined rules, such as round-robin, least connections, or IP hash, among others. This selection process helps manage workloads efficiently and provides high availability by ensuring that no single instance is overwhelmed by too much traffic. In contrast, health checks are employed to monitor the status of the targets and determine if they are available to handle requests, while routing tables define how data packets are directed within the network but do not contribute to the distribution of application traffic. Traffic shaping refers to managing the flow of packets to ensure network quality, which is not directly related to how requests are distributed among targets by the load balancer. Thus, the load balancing algorithm is the key feature that facilitates automatic traffic distribution, making it essential for scalable and resilient applications on AWS.

7. Which security feature within a VPC controls stateful traffic?

A. Network Access Control Lists

B. Route Tables

C. Security Groups

D. VPN Connections

The security feature within a VPC that controls stateful traffic is Security Groups. Security Groups operate at the instance level and are designed to act as virtual firewalls, managing inbound and outbound traffic for associated instances based on defined rules. The key aspect of Security Groups being stateful means that if an inbound request is allowed, the response traffic for that request is automatically allowed regardless of outbound rules. This allows for more intuitive management of security settings, as the connections initiated from the instance can return traffic without needing separate rules defined. In contrast, Network Access Control Lists (ACLs) are stateless; they require you to define both inbound and outbound rules explicitly. Route Tables primarily determine the paths for traffic flow within a VPC but do not provide any direct security controls. VPN Connections facilitate private connections between your VPC and on-premises networks but do not function as a traffic control mechanism that enforces security rules. Therefore, it is the stateful nature and the control over specific instance traffic that clearly make Security Groups the correct answer in this context.

8. 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.

9. How can you extend your on-premises network into AWS?

A. By using AWS VPN or AWS Direct Connect

B. By setting up a CloudFormation stack

C. By utilizing Amazon RDS for database replication

D. By configuring public IP addresses

Extending an on-premises network into AWS is primarily achieved through services that enable secure and efficient connectivity. Utilizing AWS VPN or AWS Direct Connect allows for the establishment of a private connection between the on-premises network and AWS. AWS VPN provides a secure, encrypted connection over the internet, enabling remote access to AWS resources. This is beneficial for organizations looking to maintain a secure link without requiring dedicated physical infrastructure. On the other hand, AWS Direct Connect offers a dedicated, private fiber-optic network connection from the on-premises environment to AWS, providing potentially lower latency and increased reliability compared to internet-based connections. Direct Connect can significantly enhance performance for applications that require consistent bandwidth or that are sensitive to latency. Both services effectively integrate on-premises environments with AWS, facilitating hybrid cloud architectures, seamless data access, and extended network functionalities. The other options, such as setting up a CloudFormation stack, are focused on resource deployment and management rather than network connectivity. Utilizing Amazon RDS pertains specifically to database services and replication, which do not address the network extension aspect. Configuring public IP addresses would not provide the secure, private connectivity needed for extending a network into AWS, as public IP addresses allow exposure to the internet rather than a secure link.

10. What is the main function of AWS Shield Advanced?

A. To manage and allocate cloud resources effectively

B. To provide enhanced DDoS protection and a 24x7 Security Operations Center (SOC) team

C. To automate cloud infrastructure updates

D. To enhance data storage options

The main function of AWS Shield Advanced is to provide enhanced DDoS protection and access to a 24x7 Security Operations Center (SOC) team. This service is specifically designed to safeguard applications running on AWS against Distributed Denial of Service (DDoS) attacks. AWS Shield Advanced not only offers additional detection and mitigation capabilities beyond the standard Shield service, but it also provides real-time attack visibility and the support of security experts who can assist in incident response. The protection offered by Shield Advanced is critical for businesses that require high availability and reliability, particularly those with applications that need to withstand sophisticated DDoS attacks. This service allows organizations to maintain the performance and availability of their services even under attack, while also offering cost protection from scaling charges that may incur due to a DDoS attack. In essence, AWS Shield Advanced is not concerned with resource management, automation of infrastructure updates, or enhancing data storage options; it is focused solely on defending against and mitigating DDoS threats, making it a vital component of an organization's security posture in the cloud.

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!