AWS Certified Advanced Networking Specialty Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

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. Don't worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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. **How can you reduce latencies when connecting VPCs in different regions while maintaining a transit VPC architecture?**

   A. Set up a local transit hub in the Singapore region

   B. Establish VPNs between the VPCs

   C. Increase instance sizes to improve performance

   D. Create additional subnets in each VPC

2. **What configuration is used to connect regarding the local preference for a transit VIF in a multi-region Direct Connect setup?**

   A. Route Map

   B. Policy-Based Routing

   C. BGP community tag 7224:7300

   D. Predefined Routing Protocol

3. **Which type of instances are the application servers deployed in?**

   A. On-Demand Instances

   B. Reserved Instances

   C. Spot Instances

   D. Auto Scaling group

4. **Which service can be used to evaluate the network performance of an AWS environment?**

   A. AWS CloudWatch

   B. AWS X-Ray

   C. AWS Trusted Advisor

   D. AWS Config

5. **What is the benefit of using Route 53 Resolver DNS Firewall?**

   A. Provides CloudFront caching

   B. Prevents unwanted outbound DNS queries

   C. Enables global reach for DNS queries

   D. Improves VPC peering connectivity

6. Where should a NAT gateway be placed in order to provide Internet access for instances in a private subnet?

A. In the Private Subnet

B. In the Public Subnet

C. In both Public and Private Subnets

D. In an isolated subnet

7. How many Internet Protocol Security (IPsec) tunnels are available for one Virtual Private Network (VPN) connection?

A. 1

B. 2

C. 3

D. 4

8. Which component is essential for the NAT instance in this architecture?

A. To balance traffic to the ELB

B. To enable secure access via SSH

C. To manage Auto Scaling operations

D. To provide redundancy for application servers

9. Which type of VPC endpoint is used for a private connection to AWS services?

A. Gateway Endpoint

B. Interface Endpoint

C. Private Endpoint

D. Cross-Region Endpoint

10. What is the correct CIDR format for a VPC subnet that needs to accommodate over 250 addresses?

A. 192.168.1.0/24

B. 192.168.1.0/25

C. 192.168.1.0/23

D. 192.168.1.0/22

Answers

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

Explanations

1. How can you reduce latencies when connecting VPCs in different regions while maintaining a transit VPC architecture?

A. Set up a local transit hub in the Singapore region

B. Establish VPNs between the VPCs

C. Increase instance sizes to improve performance

D. Create additional subnets in each VPC

Setting up a local transit hub in the Singapore region is an effective way to reduce latencies when connecting VPCs in different regions while maintaining a transit VPC architecture. A transit hub acts as a central point for all interconnections, facilitating efficient routing and management of inter-VPC traffic. By establishing a local transit hub close to the regions where your VPCs are deployed, you minimize the distance that data must travel, which directly contributes to lower latencies. This hub can efficiently handle traffic between multiple VPCs across different regions, allowing for optimized routes and reduced travel time for data packets. Other options, such as establishing VPNs between the VPCs, can introduce additional overhead and potential delays due to encryption and the nature of point-to-point connections. Increasing instance sizes may lead to improved processing capabilities, but it doesn't inherently address the latency between the VPCs. Similarly, creating additional subnets in each VPC does not impact the network latency between geographically separated VPCs. Therefore, the creation of a local transit hub strategically reduces latency and maintains efficient inter-VPC communication.

2. What configuration is used to connect regarding the local preference for a transit VIF in a multi-region Direct Connect setup?

A. Route Map

B. Policy-Based Routing

C. BGP community tag 7224:7300

D. Predefined Routing Protocol

In a multi-region Direct Connect setup, the configuration used to manage local preference for a transit Virtual Interface (VIF) makes use of BGP community tags. Specifically, the BGP community tag 7224:7300 is a well-defined tag in AWS that influences the routing decisions for traffic across multiple regions. When you use community tags like 7224:7300, you are explicitly instructing the routers to give a particular preference to routes associated with that community. This capability allows for effective traffic engineering by controlling the inbound and outbound traffic flow based on defined preferences. It effectively manipulates the BGP route selection process, where local preference is a key attribute that can dictate the best path for outbound traffic, thus enhancing the reliability and efficiency of routing in a multi-region Direct Connect architecture. Utilizing BGP community tags is integral in managing route preferences without needing extensive route map configurations or relying solely on policy-based routing, thereby streamlining the routing process. The levels of control provided through BGP community tags make them the correct choice for configuring the local preference in this context.

3. Which type of instances are the application servers deployed in?

A. On-Demand Instances

B. Reserved Instances

C. Spot Instances

D. Auto Scaling group

The correct choice indicates that application servers are deployed in an Auto Scaling group. This is appropriate because Auto Scaling groups enable dynamic management of instances based on demand, maintaining performance and optimizing costs. They automatically adjust the number of running instances up or down based on traffic patterns or specific metrics, ensuring that applications have the right amount of resources available at any given time. Using an Auto Scaling group provides flexibility and resilience to application architectures, as it can seamlessly handle fluctuations in load. For example, during peak traffic, the group can spin up additional instances while scaling down during non-peak times, allowing for efficient use of resources while providing high availability. In contrast, On-Demand Instances are typically used for short-term needs without commitment, meaning they may not automatically scale; Reserved Instances offer cost savings for long-term capacity but do not have the inherent auto-scaling capabilities; and Spot Instances are generally used for cost-effective, interruptible workloads and require careful management, making them less suited for consistent application server deployments.

4. Which service can be used to evaluate the network performance of an AWS environment?

A. AWS CloudWatch

B. AWS X-Ray

C. AWS Trusted Advisor

D. AWS Config

The correct answer is AWS X-Ray, as it is a service designed to help developers analyze and debug distributed applications, including those deployed within AWS environments. While its primary focus is on tracing requests as they travel through various services and components, it also provides insights into application performance, including latency and bottlenecks that may affect network communication. By using AWS X-Ray, users can gain detailed insights into how their applications are performing over the network. This includes tracking and visualizing how requests move through microservices architectures and understanding where any performance issues may arise within the network paths. This level of analysis enables developers and network administrators to identify problematic areas and optimize the overall performance of their AWS environment. In contrast, AWS CloudWatch is more focused on monitoring resource utilization and system performance metrics, AWS Trusted Advisor provides best practice guidance, and AWS Config is primarily about resource compliance and configuration tracking. None of these services offer the same level of insight into network performance specifically as AWS X-Ray does.

5. What is the benefit of using Route 53 Resolver DNS Firewall?

A. Provides CloudFront caching

B. Prevents unwanted outbound DNS queries

C. Enables global reach for DNS queries

D. Improves VPC peering connectivity

The benefit of using Route 53 Resolver DNS Firewall is that it prevents unwanted outbound DNS queries. This feature is crucial for maintaining a secure networking environment, as it allows organizations to filter and control DNS traffic both to and from their virtual private clouds (VPCs). By using a DNS firewall, you can block DNS queries that originate from your VPC to domains that are known to be malicious or unauthorized. This helps to mitigate the risk of data exfiltration, malware communications, and other potential threats that could arise from unfiltered DNS traffic. Ultimately, it enhances overall network security by ensuring that only legitimate DNS resolutions are permitted, thus protecting your resources from external threats. In contrast, options related to caching, global reach, or improving VPC connectivity do not pertain to the specific security-focused functionality of the DNS Firewall, which is designed to control and secure DNS query behavior.

6. Where should a NAT gateway be placed in order to provide Internet access for instances in a private subnet?

A. In the Private Subnet

B. In the Public Subnet

C. In both Public and Private Subnets

D. In an isolated subnet

The NAT gateway should be placed in a public subnet to provide Internet access for instances in a private subnet. This is because a NAT gateway is specifically designed to allow instances that do not have their own public IP addresses (i.e., instances in a private subnet) to access the Internet for purposes such as downloading updates or accessing external services. When the NAT gateway is in a public subnet, it can have a public IP address and can communicate directly with the Internet. The private subnet instances, which do not have public IP addresses, route their outbound traffic through the NAT gateway. This setup ensures that while the instances in the private subnet maintain their privacy and security (since they are not directly accessible from the Internet), they can still initiate outbound connections. This architecture leverages the NAT gateway's ability to manage the translation of private IP addresses to a public IP address, allowing for smooth communication with the outside world while maintaining proper security and isolation within the private subnet.

7. How many Internet Protocol Security (IPsec) tunnels are available for one Virtual Private Network (VPN) connection?

A. 1

B. 2

C. 3

D. 4

A Virtual Private Network (VPN) connection in AWS can utilize two Internet Protocol Security (IPsec) tunnels. This design is implemented to ensure high availability and redundancy. Each tunnel provides a separate encrypted connection between your on-premises network and the AWS cloud, allowing for continuous communication even if one tunnel were to fail. The concept of having two IPsec tunnels is crucial for providing a failover mechanism. If one tunnel experiences an issue, traffic can continue to flow through the other tunnel without interruption, thus safeguarding against potential downtime. This setup is particularly beneficial for enterprises that rely on consistent connectivity for critical applications. With the two IPsec tunnels, AWS supports dynamic routing protocols, such as Border Gateway Protocol (BGP), to facilitate automatic failover operations. The dual-tunnel approach also enables load balancing of traffic, enhancing overall network efficiency. This redundancy and load balancing feature is a key aspect of cloud environments designed for robustness and reliability.

8. Which component is essential for the NAT instance in this architecture?

A. To balance traffic to the ELB

B. To enable secure access via SSH

C. To manage Auto Scaling operations

D. To provide redundancy for application servers

In a NAT instance architecture, the primary role of the NAT (Network Address Translation) instance is to allow instances in a private subnet to initiate outbound traffic to the internet while preventing the internet from initiating inbound connections to those instances. For this setup to function effectively, securing access to the NAT instance is crucial. Enabling secure access via SSH allows network administrators or engineers to connect to the NAT instance for configuration, monitoring, and troubleshooting purposes. This secure access is fundamental to manage the instance effectively, ensuring that it operates correctly and remains up to date. While the other components listed may be important in different contexts (such as load balancing, auto-scaling management, or redundancy), they do not directly pertain to the specific requirement of a NAT instance to facilitate secure management access. Therefore, emphasizing secure SSH access is key to maintaining the integrity and operational capability of a NAT instance within a cloud architecture.

9. Which type of VPC endpoint is used for a private connection to AWS services?

A. Gateway Endpoint

B. Interface Endpoint

C. Private Endpoint

D. Cross-Region Endpoint

The type of VPC endpoint that provides a private connection to AWS services is the Interface Endpoint. This endpoint allows you to connect to service APIs hosted by AWS services using a private IP address from your VPC. With Interface Endpoints, you can access supported AWS services and your own VPC endpoints without needing an internet gateway, NAT device, or any public IP address. This is especially beneficial for services that are not directly accessible via a gateway approach, as it enables more granular control over network traffic, enhances security by keeping traffic within the AWS backbone, and contributes to lower data transfer costs compared to accessing services over the public internet. In contrast, a Gateway Endpoint is designed for accessing Amazon S3 and DynamoDB exclusively, and it does not facilitate private connections to a broad range of AWS services. Private Endpoint is not a standard terminology used in AWS documentation, and Cross-Region Endpoint refers to connections that span multiple regions, which is not suitable for establishing a private connection within the same region. Thus, the Interface Endpoint is the primary choice for connecting privately to a variety of AWS services.

10. What is the correct CIDR format for a VPC subnet that needs to accommodate over 250 addresses?

A. 192.168.1.0/24

B. 192.168.1.0/25

C. 192.168.1.0/23

D. 192.168.1.0/22

To accommodate over 250 addresses in a VPC subnet, it's essential to choose a CIDR block that allows for sufficient IP addresses. When determining the number of usable addresses in a subnet, the formula to calculate usable IP addresses is 2^(32 - subnet mask bits) - 2. The "-2" accounts for the network and broadcast addresses, which cannot be assigned to hosts. For the CIDR block 192.168.1.0/23: - The subnet mask is 23 bits, meaning there are 32 - 23 = 9 bits left for host addresses. - Using the formula, this gives us 2^9 - 2 = 512 - 2 = 510 usable addresses. This means that a /23 subnet can accommodate significantly more than 250 IP addresses, making it suitable for the requirement outlined in the question. Other CIDR blocks provided do not meet the requirement: - A /24 provides 256 total addresses, which after accounting for the network and broadcast addresses leaves only 254 usable addresses—less than needed. - A /25 provides just 126 usable addresses, insufficient for the requirement. - A /22 yields 1022 usable addresses, which exceeds the need but also

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!