Google Cloud Professional Cloud Network Engineer Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

This is a sample study guide. To access the full version with hundreds of questions,

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

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. **What is the primary routing metric used by Routing Information Protocol (RIP)?**

   A. Distance vector

   B. Hop count

   C. Cost

   D. Load balancing

2. **What does the Data Link layer use to identify devices on the Physical layer?**

   A. IP Addresses

   B. MAC Addresses

   C. TCP Ports

   D. URLs

3. **What role do routes play in Google Cloud networking?**

   A. They prioritize user access to resources

   B. They determine the flow of traffic within and outside the VPC

   C. They establish user permissions in the network

   D. They manage billing for network usage

4. **Why is it important to monitor network traffic in Google Cloud?**

   A. To increase storage limits

   B. To ensure high performance and security

   C. To reduce server costs

   D. To enhance data visualization

5. **What key configuration is needed for a backend service in an external load balancer?**

   A. Adding custom domains

   B. Defining health checks

   C. Setting up user authentication

   D. Creating documentation

6. How do you specify IP ranges when creating a firewall rule?

A. By generating random IPs

B. By defining source IP ranges in the rule configuration

C. By using default IP ranges specified by Google

D. By excluding specific IPs from the rule

7. Which limit is considered a hard limit for the number of primary IP ranges per subnet?

A. 1

B. 2

C. 3

D. 4

8. What is the maximum number of static routes allowed in a peering group?

A. 100

B. 200

C. 300

D. 400

9. What is a Cloud Router used for in Google Cloud?

A. To manage user access permissions

B. To monitor application logs

C. To dynamically manage route advertisements between the VPC and on-premises networks

D. To control backup policies for virtual machines

10. What is the common first step in migrating to Google Cloud Platform (GCP)?

A. Establish Direct Interconnect

B. Create an IPSec VPN

C. Set up a Cloud Router

D. Utilize Partner Interconnect

Answers

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

Explanations

1. What is the primary routing metric used by Routing Information Protocol (RIP)?

A. Distance vector

B. Hop count

C. Cost

D. Load balancing

The primary routing metric used by Routing Information Protocol (RIP) is hop count. RIP is a distance-vector routing protocol that measures the distance to a destination in terms of the number of hops required to reach that destination. Each hop represents a router that must be traversed to get from the source to the destination. The protocol considers a maximum of 15 hops, with 16 hops designated as unreachable, which limits the size of the network that RIP can effectively manage. This metric is simple to implement and provides a straightforward way to determine the best path to a destination. While RIP also falls into the category of distance vector protocols, the unique metric that primarily defines its routing decisions is indeed hop count, which helps in determining the most efficient route based on the number of routers crossed. Other options like cost, load balancing, and the general classification as a distance vector do not accurately capture the primary metric used by RIP to route packets, focusing instead on different networking principles or other routing protocols.

2. What does the Data Link layer use to identify devices on the Physical layer?

A. IP Addresses

B. MAC Addresses

C. TCP Ports

D. URLs

The Data Link layer uses MAC (Media Access Control) addresses to identify devices on the Physical layer. This is essential for enabling communication between devices on the same local network segment. MAC addresses are unique identifiers assigned to network interfaces for communications at the Data Link layer, allowing devices to recognize each other and facilitate the transmission of frames containing data. While IP addresses are used at the Network layer to route packets between different networks, they do not directly identify devices on a local physical network. TCP ports operate at the Transport layer to facilitate communication between applications on devices, and URLs serve as human-readable addresses that map to specific resources on the internet, not as identifiers for the hardware itself. Thus, the use of MAC addresses is crucial for addressing and controlling access to the network at the Data Link layer.

3. What role do routes play in Google Cloud networking?

A. They prioritize user access to resources

B. They determine the flow of traffic within and outside the VPC

C. They establish user permissions in the network

D. They manage billing for network usage

In Google Cloud networking, routes are fundamental as they determine the flow of traffic within the Virtual Private Cloud (VPC) and beyond. Routes are essentially rules that dictate how network traffic is directed to its destination based on the destination IP address and a set of criteria, such as the most specific route matched or the next-hop address. When traffic originates from a source, the routes configured in the VPC are consulted to decide where to send this traffic, whether to another instance within the same VPC, to another network, or even to the internet. By carefully configuring routes, network engineers can control and optimize traffic flow, enhance security, and ensure that the resources communicate efficiently as desired. In contrast, while the other options touch on aspects of network management, they do not align with the primary function of routes. User access prioritization and permissions are managed through IAM (Identity and Access Management) policies rather than routes, and billing concerns are addressed through different monitoring and metering mechanisms within Google Cloud, not by routing configurations. Therefore, the ability of routes to dictate the traffic's journey within the network makes option B the accurate choice.

4. Why is it important to monitor network traffic in Google Cloud?

A. To increase storage limits

B. To ensure high performance and security

C. To reduce server costs

D. To enhance data visualization

Monitoring network traffic in Google Cloud is crucial for several reasons, primarily ensuring high performance and security. By keeping an eye on the flow of data across the network, you can identify potential bottlenecks that may affect application performance. Understanding where traffic is coming from and going to allows for better management of resources, ensuring that the network operates efficiently without unexpected slowdowns. From a security perspective, monitoring network traffic helps in detecting suspicious activity. Anomalies or unexpected patterns can indicate potential security breaches or malicious intent, allowing for prompt investigation and mitigation. Ensuring that your resources are secure is vital for protecting sensitive data and maintaining compliance with industry regulations. Overall, maintaining a close watch on network traffic is integral to achieving optimal performance and safeguarding the security of resources in Google Cloud environments, thus enhancing the overall user experience and data integrity.

5. What key configuration is needed for a backend service in an external load balancer?

A. Adding custom domains

B. Defining health checks

C. Setting up user authentication

D. Creating documentation

For an external load balancer to effectively distribute traffic to a backend service, defining health checks is a crucial configuration. Health checks are mechanisms that allow the load balancer to determine the availability and performance of the backend instances. When health checks are defined, the load balancer can regularly ping the backend services according to a specified interval, and based on the responses, it can decide whether to route traffic to those instances. If a backend service fails health checks, the load balancer will stop routing traffic to it, ensuring that users are not directed to services that are down or experiencing issues. This helps maintain high availability and reliability for applications using the load balancer. Therefore, defining health checks is essential for operational efficiency, as it enables proactive traffic management and minimizes downtime. Other configurations, such as adding custom domains or setting up user authentication, while important in different contexts, do not directly relate to the core functionality of the load balancer in managing backend service health and availability. Creating documentation is also valuable for operational clarity but is not a technical configuration necessary for the load balancer's functionality.

6. How do you specify IP ranges when creating a firewall rule?

A. By generating random IPs

B. By defining source IP ranges in the rule configuration

C. By using default IP ranges specified by Google

D. By excluding specific IPs from the rule

When creating a firewall rule in Google Cloud, you specify IP ranges by defining source IP ranges in the rule configuration. This approach allows you to granularly control which IP addresses are permitted or denied access based on your security requirements. The source IP ranges can be specified as single IP addresses, CIDR notation (for example, 192.168.1.0/24), or as a specific range. This flexibility is crucial for setting up rules that align with your network's security posture, enabling you to manage inbound and outbound traffic effectively. Utilizing this method ensures you have precise control over who can access your resources, facilitating security based on the needs of your organization. By selecting specific ranges, you can tailor your firewall rules to only allow traffic from known, trusted sources, enhancing the overall security of your network environment.

7. Which limit is considered a hard limit for the number of primary IP ranges per subnet?

A. 1

B. 2

C. 3

D. 4

In Google Cloud, the configuration of subnets is critical for organizing and managing network resources effectively. A hard limit refers to a restriction that cannot be exceeded, and in this case, the number of primary IP ranges that can be assigned to a single subnet in Google Cloud is set at one. This means that each subnet can have only one primary IP range, which dictates the IP addressing within that subnet. This limit is important because it simplifies the management of IP addresses within a virtual private cloud (VPC) and ensures clarity in routing and network traffic management. Having a single primary IP range helps streamline configurations and reduces the risk of overlapping IP addresses or conflicting routes within a subnet.   The focus on maintaining a singular primary IP range aligns with best practices for subnet design, promoting better organization and performance within the cloud network. For those managing Google Cloud networks, understanding this hard limit is essential for effective architecture planning and implementation.

8. What is the maximum number of static routes allowed in a peering group?

A. 100

B. 200

C. 300

D. 400

The maximum number of static routes allowed in a peering group is 300. This limit is defined to ensure that the routing information exchanged in a peering configuration remains manageable and efficient. Each static route can represent a specific path to a destination network, and having a defined cap helps maintain the performance of the networking setup.   When configuring peering in Google Cloud, it is important to consider this limit as it could impact how you design your network architecture. For instance, if you anticipate needing more than 300 routes, you may need to explore alternative routing strategies or split your routes across multiple peering groups to accommodate your networking needs. Understanding and respecting these limitations are crucial in optimizing the performance and scalability of your cloud networking solutions.

9. What is a Cloud Router used for in Google Cloud?

A. To manage user access permissions

B. To monitor application logs

C. To dynamically manage route advertisements between the VPC and on-premises networks

D. To control backup policies for virtual machines

A Cloud Router in Google Cloud is primarily used to dynamically manage route advertisements between a Virtual Private Cloud (VPC) network and on-premises networks or other VPCs. This is especially important in hybrid cloud environments where businesses need to maintain connectivity between their cloud resources and local data centers. Cloud Router facilitates the exchange of routes using Border Gateway Protocol (BGP), enabling seamless and automated updates of the routing table without the need for manual configuration. This dynamic routing capability allows for better scalability and flexibility, ensuring that any changes in the network topology, such as adding or removing on-premises or cloud resources, can be managed efficiently. By leveraging Cloud Router, network engineers can ensure that traffic is routed optimally, which helps maintain a stable and reliable network connection, especially in scenarios where multiple routes may be involved. This is crucial for performance and reliability in cloud architectures that require continuous and real-time data flow between different environments. The other options listed, such as managing access permissions, monitoring application logs, or controlling backup policies, involve different components and services within Google Cloud that do not pertain to the functionalities offered by Cloud Router.

10. What is the common first step in migrating to Google Cloud Platform (GCP)?

A. Establish Direct Interconnect

B. Create an IPSec VPN

C. Set up a Cloud Router

D. Utilize Partner Interconnect

The common first step in migrating to Google Cloud Platform (GCP) is to create an IPSec VPN. This is primarily because establishing a secure connection between the on-premises infrastructure and the Google Cloud environment is crucial for a successful migration. An IPSec VPN provides a secure and encrypted tunnel over the internet, allowing for a reliable transfer of data during the migration process. This secure connection facilitates the movement of workloads and data to GCP while ensuring that sensitive information remains protected. It is especially useful for organizations that may not have the immediate need or resources to set up dedicated interconnections. Utilizing an IPSec VPN allows for initial testing and transfer of workloads while providing a flexible and cost-effective solution to meet immediate migration needs. While options like establishing Direct Interconnect or utilizing Partner Interconnect may provide higher bandwidth and lower latency connections for larger or production-grade migrations, they typically come into play after initial steps have been taken, often requiring more planning and resources. Setting up a Cloud Router is also part of the networking configuration process but is generally done after a secure connection, such as an IPSec VPN, has been established.

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://googlecloudprofessionalcloudnetengr.examzify.com

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