Google Cloud Professional Cloud Security Engineer 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. 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 step is necessary after enabling Google Cloud Directory Sync (GCDS) for managing users from an on-premises LDAP server?**

   A. Run a manual sync process

   B. Configure LDAP search attributes

   C. Set up a recurring GCDS task

   D. Disable GCDS integration

2. **Which Google Cloud solution allows for managing encryption keys that must be stored in multiple regions for redundancy?**

   A. Cloud KMS

   B. Customer-managed encryption keys

   C. External Key Manager

   D. Cloud Storage encryption

3. **Which logs should a database administrator review to monitor malicious activities in a Cloud SQL instance?**

   A. System Logs

   B. Data Access Logs

   C. Audit Logs

   D. Activity Logs

4. **Which Google Cloud service allows for secure routing of external traffic to backend services?**

   A. Network Load Balancer

   B. Cloud Pub/Sub

   C. Cloud Functions

   D. Cloud Dataflow

5. **What is the best way for a customer to reliably deliver Stackdriver logs from GCP to their on-premises SIEM system?**

   A. Export logs manually from Stackdriver

   B. Configure Organizational Log Sinks to export to Cloud Pub/Sub

   C. Use Cloud Storage to hold logs for download

   D. Send logs via email alerts

6. What action must be performed to modify access to the VM running in a managed group?

A. Change its network settings

B. Modify VPC firewall rules

C. Update the VM instance itself

D. Install a dedicated API

7. What should be done immediately after identifying vulnerable Google Cloud CLI sessions?

A. Set the reauthentication frequency to a more secure duration.

B. Terminate all active sessions right away.

C. Upgrade all security software.

D. Alert users about session vulnerabilities.

8. What tool is recommended to provide access reviews evidence for IAM?

A. Policy Analyzer

B. Cloud IAM Role Viewer

C. Audit Log Viewer

D. Google Cloud Console

9. What should be configured to ensure secure communication between GCP and on-premises environments?

A. Use of NAT gateways

B. Private VPN connections

C. Public IP addresses for all instances

D. Cloud Pub/Sub messaging

10. To prevent any VM from reaching the public internet while performing batch processing, what should be enabled?

A. Public IP assignment

B. Firewall rules allowing outbound traffic

C. Private Google Access

D. Cloud IAM role management

Answers

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

Explanations

1. Which step is necessary after enabling Google Cloud Directory Sync (GCDS) for managing users from an on-premises LDAP server?

A. Run a manual sync process

B. Configure LDAP search attributes

C. Set up a recurring GCDS task

D. Disable GCDS integration

After enabling Google Cloud Directory Sync (GCDS) for managing users from an on-premises LDAP server, setting up a recurring GCDS task is a necessary step. This configuration allows GCDS to systematically synchronize user data from the LDAP server to Google Cloud. By scheduling this task to run at regular intervals, user accounts and their attributes in Google Cloud are kept in sync with the on-premises directory automatically. A manual sync process may be performed initially to ensure everything is up to date right after setup, but it does not maintain ongoing synchronization, meaning it is not sufficient for long-term management. While configuring LDAP search attributes is important for how GCDS retrieves user data, it is not a step directly tied to maintaining synchronization after GCDS is enabled. Disabling GCDS integration goes against the goal of managing users via the tool, as it would halt the synchronization processes that are intended to keep the user data consistent across environments. Thus, setting up a recurring task is critical to ensuring continuous and automated user management from the LDAP server to Google Cloud.

2. Which Google Cloud solution allows for managing encryption keys that must be stored in multiple regions for redundancy?

A. Cloud KMS

B. Customer-managed encryption keys

C. External Key Manager

D. Cloud Storage encryption

The correct choice highlights the importance of managing encryption keys in a manner that supports redundancy across multiple regions. By utilizing customer-managed encryption keys, organizations can maintain control over their own encryption processes and keys while ensuring that these keys are replicated and managed in multiple Google Cloud regions. This enables effective data protection strategies and compliance with regulatory requirements that may dictate the need for redundancy in key management. Customer-managed encryption keys provide the flexibility to define key rotation policies, access controls, and auditing capabilities, which are essential for maintaining a secure cloud environment. Furthermore, they enable organizations to align their encryption practices with their internal security policies while leveraging the distributed nature of Google Cloud. Other options, while relevant to encryption, do not specifically address the requirement for managing multiple regional storage of encryption keys as effectively. Cloud KMS, mentioned in the choices, is a powerful service for key management, but it is the customer-managed approach that emphasizes the redundancy aspect needed in this context. External Key Manager and Cloud Storage encryption also serve specific purposes within the Google Cloud security framework, but they do not specifically cater to the need for multi-region key management as directly as customer-managed encryption keys.

3. Which logs should a database administrator review to monitor malicious activities in a Cloud SQL instance?

A. System Logs

B. Data Access Logs

C. Audit Logs

D. Activity Logs

A database administrator should focus on Data Access Logs to effectively monitor malicious activities in a Cloud SQL instance. These logs are designed to capture information on database access events, including successful and failed attempts to query the database. By analyzing the Data Access Logs, an administrator can identify unusual access patterns, such as repeated failed login attempts or unexpected queries, which may indicate unauthorized access or other malicious activities. While other logs serve important purposes, they do not specifically target the monitoring of access to database data. System Logs typically contain information about the operational status and performance of the database system, rather than detailed access events. Audit Logs, on the other hand, provide insights into administrative actions or changes to the configuration and security settings within Cloud SQL but may not directly record every data access event. Activity Logs generally capture a high-level overview of the actions taken within the Google Cloud environment but do not provide the granularity needed to monitor specific database access attempts. By leveraging Data Access Logs, a database administrator can better secure the Cloud SQL instance and respond to potential threats by identifying and addressing any suspicious activities promptly.

4. Which Google Cloud service allows for secure routing of external traffic to backend services?

A. Network Load Balancer

B. Cloud Pub/Sub

C. Cloud Functions

D. Cloud Dataflow

The Network Load Balancer is specifically designed for flexible and efficient routing of external traffic to backend services while ensuring high availability and failover capabilities. It can handle millions of requests per second and can direct traffic based on the geographical location of the incoming requests. This service is ideal for distributing incoming traffic across various backend instances, which can be virtual machine instances, containerized applications, or other services, ensuring optimal performance and resource utilization. Moreover, the Network Load Balancer operates at the transport layer (Layer 4), allowing it to manage TCP and UDP traffic, making it suitable for non-HTTP traffic as well. It also supports static IP addresses, which can be beneficial for maintaining consistent access points for clients. The other options offered do not inherently provide the functionality required for secure routing of external traffic to backend services. For instance, Cloud Pub/Sub is a messaging service that facilitates event-driven architectures and does not route traffic to backend services. Cloud Functions serves as a serverless compute service executing code in response to events but isn't focused on routing external traffic. Cloud Dataflow, designed for data processing and stream analytics, also does not serve as a routing mechanism for external traffic. Therefore, the Network Load Balancer stands out as the appropriate service for the routing task

5. What is the best way for a customer to reliably deliver Stackdriver logs from GCP to their on-premises SIEM system?

A. Export logs manually from Stackdriver

B. Configure Organizational Log Sinks to export to Cloud Pub/Sub

C. Use Cloud Storage to hold logs for download

D. Send logs via email alerts

The best way for a customer to reliably deliver Stackdriver logs from Google Cloud Platform (GCP) to their on-premises Security Information and Event Management (SIEM) system is to configure Organizational Log Sinks to export to Cloud Pub/Sub. When logs are exported using Cloud Pub/Sub, it allows for real-time, asynchronous transmission of logs. This approach ensures that logs are reliably sent to a specified destination, which can include custom endpoints. The Pub/Sub service facilitates flexible handling of logs, as it can accommodate various consumers that need to process the logs further. By integrating this with on-premises systems, the customer can set up subscribers that pull data from the Cloud Pub/Sub topic and forward it to their SIEM system, facilitating a robust pipeline for log data that can scale and handle potential bursts in log generation. The other approaches lack reliability or scalability. For instance, exporting logs manually from Stackdriver is labor-intensive and prone to human error, making it an unreliable method for consistent logging. Using Cloud Storage for downloading logs is more suitable for ad hoc access rather than continuous delivery, thus not optimal for real-time or nearly real-time logging needs. Sending logs via email alerts is also not feasible for large volumes or structured logging data, leading to potential

6. What action must be performed to modify access to the VM running in a managed group?

A. Change its network settings

B. Modify VPC firewall rules

C. Update the VM instance itself

D. Install a dedicated API

To modify access to a VM running in a managed instance group, adjusting VPC firewall rules is crucial. VPC firewall rules govern the traffic to and from instances in a Virtual Private Cloud (VPC) network. By modifying these rules, you can specifically control which IP addresses or ranges are allowed to access the VM, along with the protocols and ports that are open. For instance, if you need to allow SSH access to the VM, you would configure a firewall rule to allow inbound traffic on port 22 from specific IP addresses. Conversely, if you want to restrict access, you would modify the rules to block certain traffic patterns. Other options might seem related but do not directly result in modified access configurations for the VM. For instance, changing network settings may not sufficiently address access control on its own, and updating the VM instance itself typically pertains to changing configurations or applying patches rather than access control. Similarly, installing a dedicated API does not inherently affect access settings for the VM as that is more about extending functionality or integration capabilities rather than outright access control. Thus, modifying VPC firewall rules is the most effective and direct way to manage access to VMs in such a setup.

7. What should be done immediately after identifying vulnerable Google Cloud CLI sessions?

A. Set the reauthentication frequency to a more secure duration.

B. Terminate all active sessions right away.

C. Upgrade all security software.

D. Alert users about session vulnerabilities.

The best course of action after identifying vulnerable Google Cloud CLI sessions is to set the reauthentication frequency to a more secure duration. This approach directly addresses the security posture of your sessions by ensuring that sessions do not remain active longer than necessary, reducing the window of opportunity for an attacker to exploit any vulnerabilities. By implementing a more secure reauthentication frequency, you enhance your security controls and minimize the risks associated with long-lived sessions. It encourages users to revalidate their identities more often, reducing the chances of unauthorized access via sessions that may have been left open unintentionally or hijacked. While terminating all active sessions might seem like a quick fix, it does not address the underlying issue of session management and can disrupt legitimate users who are logged in, potentially causing operational issues. Upgrading all security software is a proactive step but may not be the immediate response required to address the specific vulnerability found in the CLI sessions. This action tends to be part of a broader security maintenance strategy rather than a direct response to the vulnerability. Alerting users about session vulnerabilities is important for awareness and may help prevent future issues, but it does not provide an immediate solution to the identified vulnerabilities. The focus should be on implementing measures that improve security on the sessions themselves rather than just informing users

8. What tool is recommended to provide access reviews evidence for IAM?

A. Policy Analyzer

B. Cloud IAM Role Viewer

C. Audit Log Viewer

D. Google Cloud Console

The Policy Analyzer is designed to evaluate and review Identity and Access Management (IAM) policies in Google Cloud. It helps identify who has access to what resources within your cloud environment, enabling administrators to gain insights into permissions and roles assigned to users, groups, and service accounts. Using the Policy Analyzer, organizations can conduct access reviews effectively, ensuring that permissions align with the principle of least privilege and identifying any outdated or unnecessary access. It generates data that can be utilized as evidence during audits, reinforcing compliance and security posture. This tool enhances governance by helping to maintain a clear understanding of IAM policies in place and supports better decision-making for access management. Other options may provide some information on IAM or permissions in the cloud, but they do not specifically focus on the comprehensive analysis or review needed for access audit purposes like the Policy Analyzer does. For example, the Cloud IAM Role Viewer can display roles but does not analyze them for access reviews. Audit Log Viewer provides logs of activities but does not directly assist in evaluating IAM policies. The Google Cloud Console is a general interface for managing resources and permissions rather than a specialized tool for access reviews.

9. What should be configured to ensure secure communication between GCP and on-premises environments?

A. Use of NAT gateways

B. Private VPN connections

C. Public IP addresses for all instances

D. Cloud Pub/Sub messaging

The choice of configuring private VPN connections is essential for ensuring secure communication between Google Cloud Platform (GCP) and on-premises environments. A private VPN (Virtual Private Network) establishes an encrypted tunnel for data transmission between the two environments, protecting sensitive information as it travels across the public internet. This secure connection allows for secure data exchange while maintaining the confidentiality and integrity of the data being transmitted. Utilizing a private VPN also helps organizations comply with security standards and regulations that may require secure communications for sensitive data transfer. It provides a robust solution for extending on-premises networks to GCP, facilitating seamless hybrid cloud architectures. In contrast, options like using NAT gateways and public IP addresses do not inherently provide secure communication. NAT gateways are primarily focused on managing outbound traffic and may not protect the data itself, while public IP addresses can expose instances to potential vulnerabilities as they are accessible over the internet. Cloud Pub/Sub messaging serves a different purpose, primarily for messaging and event-driven architectures, rather than securing network communication. Therefore, configuring private VPN connections effectively addresses the need for secure interconnectivity between GCP and on-premises environments.

10. To prevent any VM from reaching the public internet while performing batch processing, what should be enabled?

A. Public IP assignment

B. Firewall rules allowing outbound traffic

C. Private Google Access

D. Cloud IAM role management

Enabling Private Google Access is the appropriate choice for ensuring that virtual machines (VMs) can interact with Google services without being assigned public IP addresses. This feature allows VMs in a private network to reach Google APIs and services securely, while still restricting their access to the public internet. By utilizing Private Google Access, you can maintain a higher level of security by keeping the VMs isolated from the public internet, which is critical for sensitive operations like batch processing. This approach ensures that the VMs can still perform necessary tasks that involve Google services without exposing them to potential threats and vulnerabilities associated with public internet access. In contrast, public IP assignment would expose the VM to the internet, inherently increasing security risks. Firewall rules allowing outbound traffic would permit access to the public internet, which is contrary to the requirement for isolation. Cloud IAM role management focuses on identity and access management rather than network traffic control, hence it does not directly facilitate the goal of preventing VMs from reaching the public internet.

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://googlecloudprofessionalcloudsecurityengineer.examzify.com

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