GOOGLE CLOUD PROFESSIONAL CLOUD SECURITY ENGINEER PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://
googlecloudprofessionalcloudsecurityengineer.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. **Which API should be used for tokenization and pseudonymization in BigQuery?**

   A. Cloud Data Loss Prevention API

   B. Cloud Identity API

   C. BigQuery Data Transfer Service

   D. Cloud Key Management Service

2. **To automate patch management in virtual machines, which two actions should you take?**

   A. Use VM Manager and enable automatic patch updates

   B. View patch management data in a Security Command Center

   C. Deploy patches manually on each VM

   D. Update VMs using Google Cloud Console only

3. **To ensure GDPR compliance for resource creation, what should be applied to the Google Cloud organization?**

   A. Set up a budget for resources.

   B. Use the org policy constraint 'Google Cloud Platform - Resource Location Restriction'.

   C. Install a region-specific API.

   D. Regularly monitor compliance reports.

4. **What Google Cloud feature is essential for protecting sensitive workloads from boot-level malware?**

   A. Google Kubernetes Engine.

   B. Google Shielded VMs.

   C. Cloud Pub/Sub.

   D. Cloud Functions.

5. **To automatically grant read-only access to all department members for new projects, what is the recommended configuration?**

   A. Create a new project for each department

   B. Create a Folder per department and assign Project Viewer role to Google Group

   C. Use IAM roles for individual users

   D. Implement Google Groups for all employees

SAMPLE

6. To optimize responsiveness, which virtual machine configuration should be considered?

A. Use preemptible VMs for cost savings

B. Deploy a single large VM instead of multiple smaller VMs

C. Utilize autoscaling with instance groups

D. Avoid changing VM types once created

7. Why might you encounter access issues when creating a Cloud Storage bucket using a customer managed encryption key (CMEK) from a different project?

A. The CMEK is stored in an on-premises environment

B. The CMEK is in a different region than the Cloud Storage bucket

C. The CMEK was not properly backed in HSM

D. The Cloud Storage project has incorrect IAM roles assigned

8. Which product should be used for DDoS protection while meeting compliance requirements for known good CIDR traffic?

A. Cloud Functions

B. Cloud Armor

C. Cloud CDN

D. Cloud Load Balancing

9. Which IAM design is appropriate for a business user who must access curated reports in BigQuery?

A. Assign roles/bigquery.dataEditor role

B. Assign roles/bigquery.admin role

C. Create curated tables and assign roles/bigquery.dataViewer role

D. Assign roles/bigquery.dataOwner role

10. 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.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which API should be used for tokenization and pseudonymization in BigQuery?

A. Cloud Data Loss Prevention API

B. Cloud Identity API

C. BigQuery Data Transfer Service

D. Cloud Key Management Service

The correct choice is the Cloud Data Loss Prevention (DLP) API, which is specifically designed to help with sensitive data protection, including tokenization and pseudonymization. Tokenization is a process that replaces sensitive data with non-sensitive substitutes, known as tokens, to reduce the risk of exposing personally identifiable information (PII) during analytics operations, while pseudonymization allows data to be processed without directly identifying individuals. Using the Cloud DLP API, you can scan datasets for sensitive information and then apply tokenization or pseudonymization methods directly within BigQuery. This is essential for maintaining data privacy and compliance with regulations such as GDPR or HIPAA, where handling sensitive data must be done carefully to avoid exposure. The other options do not serve this specific purpose. The Cloud Identity API primarily deals with identity management and authentication, the BigQuery Data Transfer Service is focused on scheduling and automating data imports from various sources into BigQuery, and the Cloud Key Management Service is concerned with managing cryptographic keys rather than handling data tokenization or pseudonymization. Therefore, utilizing the Cloud DLP API is the best approach for securely handling sensitive data within BigQuery.

2. To automate patch management in virtual machines, which two actions should you take?

A. Use VM Manager and enable automatic patch updates

B. View patch management data in a Security Command Center

C. Deploy patches manually on each VM

D. Update VMs using Google Cloud Console only

Enabling automatic patch updates using VM Manager is a robust way to automate patch management for virtual machines. VM Manager offers capabilities to manage the lifecycle of your VMs, which includes the ability to schedule and automatically apply patches across a fleet of instances. By activating this feature, you mitigate the risk of vulnerabilities due to unpatched systems while also reducing the manual workload associated with managing updates individually. This approach not only ensures that the VMs are regularly and systematically updated but also adheres to best practices in maintaining security across your infrastructure. In contrast, manually deploying patches on each VM would require significant administrative effort and could lead to inconsistent patch levels across your environments, which is less efficient and raises security concerns. Relying solely on the Google Cloud Console for updates lacks the automation and management capabilities offered by VM Manager, and viewing patch management data in a Security Command Center does not actively engage with patch management processes, missing the proactive measures required for thorough management of VM security.

SAMPLE

3. To ensure GDPR compliance for resource creation, what should be applied to the Google Cloud organization?

A. Set up a budget for resources.

B. Use the org policy constraint 'Google Cloud Platform - Resource Location Restriction'.

C. Install a region-specific API.

D. Regularly monitor compliance reports.

Utilizing the org policy constraint 'Google Cloud Platform - Resource Location Restriction' is essential for ensuring GDPR compliance in the context of resource creation in Google Cloud. The General Data Protection Regulation (GDPR) requires that personal data be processed and stored within specific geographical boundaries, particularly within the European Union. By applying the resource location restriction policy, organizations can enforce rules that prevent the creation or storage of resources outside designated regions. This is crucial for compliance because it allows organizations to control where their data is processed and ensures that they adhere to the legal requirements set forth by GDPR. This constraint effectively limits the geographical locations in which resources can be created, helping to safeguard personal data and reduce the risk of non-compliance. The other options, while they may provide various levels of utility and support security best practices, do not specifically address the fundamental requirement of geographic data handling as mandated by GDPR. Setting up a budget is focused on financial management rather than legal compliance. Installing a region-specific API may help in functionality, but it does not inherently safeguard data locations. Regularly monitoring compliance reports is a valuable practice, yet without the foundational policy in place to restrict data handling geographically, it may not ensure compliance by itself.

4. What Google Cloud feature is essential for protecting sensitive workloads from boot-level malware?

A. Google Kubernetes Engine.

B. Google Shielded VMs.

C. Cloud Pub/Sub.

D. Cloud Functions.

Google Shielded VMs are essential for protecting sensitive workloads from boot-level malware because they provide a hardened environment specifically designed to ensure the integrity of the virtual machine (VM) and its boot process. Shielded VMs incorporate several security features, including secure boot, which verifies the digital signatures of boot components to prevent unauthorized code from running during the boot process, and the virtual trusted platform module (vTPM), which helps in establishing a root of trust and secure storage for sensitive data and cryptographic keys. In addition to secure boot, Shielded VMs also include features like integrity monitoring, ensuring that any changes to the system are detected and reported. This level of protection is vital for sensitive workloads that, if compromised at the boot level, could have dire consequences for data integrity and security. The other options do not provide this specific level of boot integrity and protection against lower-level threats. Google Kubernetes Engine focuses on managing containerized applications, Cloud Pub/Sub serves as a messaging service for event-driven systems, and Cloud Functions allows for serverless computing but does not incorporate the specific boot protection features provided by Shielded VMs. Therefore, for safeguarding workloads against boot-level malware, Google Shielded VMs is the appropriate choice.

SAMPLE

5. To automatically grant read-only access to all department members for new projects, what is the recommended configuration?

A. Create a new project for each department

B. Create a Folder per department and assign Project Viewer role to Google Group

C. Use IAM roles for individual users

D. Implement Google Groups for all employees

The recommended configuration of creating a Folder per department and assigning the Project Viewer role to a Google Group is effective because it allows for centralized management of permissions while promoting automation and scalability. By organizing projects under departmental folders, any new project created within that folder will inherit the permissions set at the folder level, which simplifies the process of granting read-only access. This means that when a new project is added to the folder, all members of the designated Google Group automatically receive the Project Viewer role without the need for individual configurations. This approach minimizes administrative overhead, ensuring that access is consistent and easily manageable as team members come and go. Additionally, it allows for clear organizational structure and visibility into what is accessible to each department, facilitating better security and compliance practices. Other configurations may not effectively meet the requirement for automation and management. For instance, creating a new project for each department would lead to redundancy and require separate permissions management for each project. Using IAM roles for individual users can be cumbersome to manage as it increases the number of configurations needed and does not easily accommodate new project additions. Implementing Google Groups for all employees, while beneficial for grouping, does not inherently control access levels to projects without an explicit role assignment, leaving significant access management to manual handling.

6. To optimize responsiveness, which virtual machine configuration should be considered?

A. Use preemptible VMs for cost savings

B. Deploy a single large VM instead of multiple smaller VMs

C. Utilize autoscaling with instance groups

D. Avoid changing VM types once created

Utilizing autoscaling with instance groups is a key strategy for optimizing responsiveness in cloud environments. Autoscaling enables the automatic adjustment of the number of virtual machine instances in response to fluctuating demand. This means that during periods of high load, additional instances can be spun up to handle the increased traffic, ensuring that application performance remains high and users experience quick response times. Conversely, during low usage periods, unnecessary resources can be shut down, leading to cost savings. This dynamic scaling is crucial for applications that experience varying workloads, as it ensures that resources are allocated efficiently in real-time. The flexibility of instance groups in combination with autoscaling allows for the allocation of just the right amount of resources when they are needed most, thereby maintaining high responsiveness and optimizing resource utilization. In contrast, the other options do not directly address responsiveness in the same way. Preemptible VMs are designed for cost savings but can be terminated at any time, which may risk application performance during critical loads. Deploying a single large VM can lead to resource contention and may not scale efficiently with demand, while avoiding changes to VM types can lead to suboptimal performance if the initial configurations do not match current workload requirements. Autoscaling provides a more robust solution for maintaining responsiveness in a cloud environment

SAMPLE

7. Why might you encounter access issues when creating a Cloud Storage bucket using a customer managed encryption key (CMEK) from a different project?

A. The CMEK is stored in an on-premises environment

B. The CMEK is in a different region than the Cloud Storage bucket

C. The CMEK was not properly backed in HSM

D. The Cloud Storage project has incorrect IAM roles assigned

When creating a Cloud Storage bucket that uses a customer-managed encryption key (CMEK), it's important to ensure that the CMEK is in the same region as the Cloud Storage bucket itself. If the CMEK is located in a different region, it cannot be accessed during the bucket creation process. Google Cloud's infrastructure requires that the encryption key and the data it encrypts reside in the same region to maintain performance, compliance, and security considerations. Regions are geographical areas where data centers are located, and key management services are designed to operate within the region's boundaries. Attempting to create a Cloud Storage bucket with a CMEK from a different region would lead to access issues, as the key would not be available for use. The other options revolve around scenarios that, while they may lead to access issues in different contexts, do not directly relate to the fundamental requirement that a CMEK must reside in the same region as the resource it secures. For example, storing the CMEK in an on-premises environment would cause access problems, but that situation doesn't pertain to the specific requirement regarding regional alignment. Similarly, issues with improper backing or IAM role assignments relate to different aspects of key management and access control, rather than the geographical constraints required by Google

8. Which product should be used for DDoS protection while meeting compliance requirements for known good CIDR traffic?

A. Cloud Functions

B. Cloud Armor

C. Cloud CDN

D. Cloud Load Balancing

Cloud Armor is specifically designed to provide DDoS protection while ensuring compliance requirements, particularly for environments that need to manage and secure traffic based on known good CIDR ranges. It uses a set of security policies to protect applications from various types of attacks, including DDoS. In the context of managing traffic based on "known good" CIDR blocks, Cloud Armor allows for advanced configurations to permit or deny traffic based on specific IP ranges, which is critical for maintaining security compliance. This capability helps organizations to create a shield around their sensitive applications by allowing only trusted traffic to reach them while blocking potential threats. Other products mentioned do not specialize in this combination of DDoS protection and compliance with CIDR-based access control. For example, Cloud Functions is suited for handling serverless functions and does not provide network-level protection against DDoS attacks. Cloud CDN focuses on caching static content to improve performance rather than protecting against DDoS. Cloud Load Balancing provides scalability and distributes traffic efficiently but lacks the specific features for security policy enforcement against DDoS attacks. Thus, the choice of Cloud Armor is appropriate for environments that require robust DDoS defense along with compliance measures for known traffic sources.

SAMPLE

9. Which IAM design is appropriate for a business user who must access curated reports in BigQuery?

A. Assign roles/bigquery.dataEditor role

B. Assign roles/bigquery.admin role

C. Create curated tables and assign roles/bigquery.dataViewer role

D. Assign roles/bigquery.dataOwner role

The choice to create curated tables and assign the roles/bigquery.dataViewer role is particularly suitable for a business user who needs access to curated reports in BigQuery. This role grants the user the necessary permissions to read and query data within the specified tables without giving them the ability to modify or delete the underlying data. This is essential in a reporting context, where users typically only need to analyze existing data rather than change it. By focusing on curated tables, the data can be organized and tailored to meet specific reporting requirements, ensuring that the user has access to only the relevant datasets. This prevents potential misuse of sensitive data and maintains the integrity of the overall data structure. In environments where data governance and security are critical, limiting access to just the data needed for reporting tasks helps mitigate risks associated with unauthorized alterations or access to sensitive information. In contrast, the other roles mentioned carry permissions that exceed what is necessary for simply viewing reports. Roles such as dataEditor or dataOwner allow for modifying and managing data, which is inappropriate for a business user whose primary function is to view and analyze data rather than manage it.

10. 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

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://googlecloudprofessionalcloudsecurityengineer.examzify.com

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

SAMPLE