G Professional Collaboration Engineer Practice Exam (Sample)

Study Guide

BY EXAMZIFY

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. **What should you do to change the organizational unit of Chrome devices during enterprise enrollment?**

   A. Change Enrollment Permissions to only allow users in this organization.

   B. Change Enrollment Controls to Place Chrome device in user organization.

   C. Change Enrollment Controls to Keep Chrome device in current location.

   D. Change Enrolment Permissions to not allow users to enroll new devices.

2. **What measure should you take to inform the CTO about accounts re-enabled after Security Awareness Training?**

   A. Enable "Suspicious login" rule to notify the CTO.

   B. Enable "Suspended user made active" rule and notify the CTO.

   C. Enable "Email settings changed" rule and inform the CTO.

   D. Automatic notifications to all Super Administrators.

3. **What should you check first when a user experiences access issues with Drive?**

   A. Confirm special permissions were set at the file level.

   B. Ensure the correct licenses are assigned for the user's organizational unit.

   C. Verify that the user belongs to the appropriate groups with Drive access.

   D. Check for any recent organizational policy changes.

4. **Which of the following is a feature of Google Sheets that promotes collaboration?**

   A. Single-user editing mode

   B. Simultaneous editing and chat features

   C. Generating automatic reports only

   D. File export options

5. **What should be done to prepare the team for future interface changes in Gmail?**

    A. Enable "Scheduled Release" in new user features.

    B. Uncheck "Enable Gmail Labs for my users."

    C. Enable "Rapid Release" for the organization.

    D. Stop auto-updates in Device Management.

6. **What does Google Drive primarily facilitate?**

    A. Collaborative editing

    B. Document approval processes

    C. File storage and sharing

    D. Virtual meetings

7. **What allows Google Workspace Admins to receive alerts about potential security issues?**

    A. Backup notifications

    B. Alert Center

    C. User audit trails

    D. Cloud monitoring tools

8. **How can teams collaborate effectively on video projects using Google Workspace?**

    A. By using Google Calendar for scheduling

    B. By using Google Meet and Google Drive

    C. By creating shared online workspaces

    D. By submitting reports via Google Docs

9. **What action allows the Director of Finance to be alerted when two auditors share files externally?**

    A. Create a Google Group that includes the two auditors and set a Drive DLP Rule.

    B. Create a Content Compliance rule for outbound share notifications.

    C. Create two Drive Audit Alerts for each auditor's external shares.

    D. Check the Admin Console Dashboard periodically for notifications.

10. What should you do to ensure the correct users in finance receive a commonly used third-party app?

    A. For the Finance OU, enable the third-party app in SAML apps.

    B. For the Finance OU, enable the third-party app in Marketplace Apps.

    C. At the root level, disable the third-party app.

    D. At the root level, allow users to install only whitelisted apps from the G Suite Marketplace.

Answers

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

Explanations

1. What should you do to change the organizational unit of Chrome devices during enterprise enrollment?

A. Change Enrollment Permissions to only allow users in this organization.

B. Change Enrollment Controls to Place Chrome device in user organization.

C. Change Enrollment Controls to Keep Chrome device in current location.

D. Change Enrolment Permissions to not allow users to enroll new devices.

To change the organizational unit of Chrome devices during enterprise enrollment, the correct approach involves utilizing the enrollment controls effectively. By selecting the option that allows you to "Place Chrome device in user organization," you ensure that the devices are assigned to the correct organizational unit at the time of enrollment. This means that when a user enrolls a Chrome device, it will automatically be placed into the designated organizational unit corresponding to the user's credentials. This capability is crucial in managing devices in a large organizational environment effectively, as it helps to apply the correct policies and settings specific to the organizational unit. Properly aligning devices with their respective units also enhances security and compliance with organizational standards. In contrast, the other choices do not result in a reassignment of the organizational unit. For example, limiting enrollment permissions restricts the users who can enroll devices but does not change the organizational unit assignment. Similarly, keeping devices in the current location or prohibiting new enrollments will not facilitate the change of organizational units for already enrolled devices. Each of these options addresses different aspects of device management but does not directly answer the need to alter the organizational unit during the enrollment process.

2. What measure should you take to inform the CTO about accounts re-enabled after Security Awareness Training?

A. Enable "Suspicious login" rule to notify the CTO.

B. Enable "Suspended user made active" rule and notify the CTO.

C. Enable "Email settings changed" rule and inform the CTO.

D. Automatic notifications to all Super Administrators.

Choosing to enable the "Suspended user made active" rule and inform the CTO is the most appropriate measure in this context. This option directly addresses the specific situation of accounts being re-enabled after Security Awareness Training. By activating this rule, you create a mechanism that triggers a notification specifically when users who had previously been suspended are reactivated. This allows the CTO to stay informed about potential security implications and user behavior changes, ensuring that the organization's security posture is maintained and that the training has been effective. In contrast, other choices do not directly relate to the event of re-enabling accounts post-training. For instance, enabling the "Suspicious login" rule would be more relevant for monitoring unusual access patterns rather than account reactivations. The "Email settings changed" rule pertains to alterations in email configurations, which is not related to the re-enabling of accounts. Lastly, automatic notifications to all Super Administrators, while informative, would not specifically convey targeted information regarding suspended accounts that have been reactivated, diluting the focus of the communication needed for this particular situation.

3. What should you check first when a user experiences access issues with Drive?

A. Confirm special permissions were set at the file level.

B. Ensure the correct licenses are assigned for the user's organizational unit.

C. Verify that the user belongs to the appropriate groups with Drive access.

D. Check for any recent organizational policy changes.

When troubleshooting access issues with Google Drive, the first step should involve ensuring that the user has the correct licenses assigned for their organizational unit. This is critical as licenses dictate the level of access and features that a user can utilize within Google Workspace. If a user lacks the appropriate license, they may find themselves unable to access Drive or its functionalities, regardless of settings or permissions configured elsewhere. Licenses determine whether users have access to applications like Google Drive, and different organizational units may have varying licensing configurations. Therefore, confirming that the user has been provisioned with the necessary licenses specific to their organizational unit is essential before delving into file-level permissions or group memberships. Once license verification is completed, other factors such as permissions, group memberships, and policy changes can be evaluated. However, ensuring the proper licensing is fundamental as it lays the groundwork for all users' access within the organization.

4. Which of the following is a feature of Google Sheets that promotes collaboration?

A. Single-user editing mode

B. Simultaneous editing and chat features

C. Generating automatic reports only

D. File export options

Simultaneous editing and chat features are fundamental to promoting collaboration in Google Sheets. This functionality allows multiple users to work on the same document at the same time, facilitating real-time updates and contributions. As users make changes, those modifications are immediately visible to all collaborators, thus enhancing productivity and reducing the potential for version control issues. Moreover, the integrated chat feature allows users to communicate directly within the document environment without needing to switch to another application. This seamless interaction fosters teamwork by enabling users to discuss changes, provide feedback, or ask questions right where the work is happening. Combining simultaneous editing with chat makes the collaboration process more efficient and effective, encouraging users to engage constructively on shared projects. In contrast, other options do not specifically enhance collaborative efforts as directly. Single-user editing mode restricts input to one person at a time, which does not promote teamwork. Generating automatic reports, while useful, does not involve real-time collaboration amongst users. File export options, although beneficial for sharing documents outside of Google Sheets, do not facilitate ongoing collaborative efforts within the platform.

5. What should be done to prepare the team for future interface changes in Gmail?

A. Enable "Scheduled Release" in new user features.

B. Uncheck "Enable Gmail Labs for my users."

C. Enable "Rapid Release" for the organization.

D. Stop auto-updates in Device Management.

Enabling "Scheduled Release" in new user features is a strategy that allows organizations to manage and prepare for changes that may occur in Gmail's interface. This option provides a controlled rollout of new features, ensuring that the team can approach updates thoughtfully. By activating the Scheduled Release, organizations will receive new features and changes after they have been tested in the Rapid Release channel. This means the team can prepare for adjustments ahead of time, familiarizing themselves with any new functionalities or interface changes prior to widespread deployment. This approach minimizes potential disruptions and allows for targeted training and communication strategies to help users adapt seamlessly to the changes. In contrast, while options like unchecking "Enable Gmail Labs" or stopping auto-updates might seem like viable approaches to manage change, they do not provide a proactive framework for adjusting to future updates. These options could hinder access to new and potentially beneficial features instead of preparing for their implementation. Enabling "Rapid Release," while it allows access to the latest features, does not provide the same level of preparedness as Scheduled Release, as it involves immediate and unverified changes that might not allow adequate time for user adaptation.

6. What does Google Drive primarily facilitate?

A. Collaborative editing

B. Document approval processes

C. File storage and sharing

D. Virtual meetings

Google Drive primarily facilitates file storage and sharing. It serves as a cloud-based storage solution, allowing users to store files securely online and access them from various devices. This centralizes document management, making it easier for individuals and teams to organize, share, and collaborate on files in a seamless manner. Users can upload a variety of file types, including documents, images, and videos, providing flexibility for different needs. While collaborative editing is indeed a feature of Google Docs—an application within the Google Drive ecosystem—the core function of Google Drive itself is focused on storage and sharing capabilities. This foundation allows for enhanced collaboration by enabling users to share documents with others and set specific permissions for viewing, commenting, or editing. Thus, the primary role of Google Drive emphasizes its capacity to act as a reliable platform for storing and sharing files.

7. What allows Google Workspace Admins to receive alerts about potential security issues?

A. Backup notifications

B. Alert Center

C. User audit trails

D. Cloud monitoring tools

The Alert Center is a centralized location within Google Workspace that provides administrators with real-time alerts and notifications regarding potential security issues, policy violations, and important account activities. This tool is crucial for proactive security management, as it enables admins to quickly identify and respond to incidents that could affect their organization's data and user accounts. The alerts generated by the Alert Center can include information about unusual login attempts, phishing threats, unauthorized access attempts, and other suspicious activities. By leveraging these alerts, administrators can take appropriate actions to mitigate risks and safeguard their organization's resources. In contrast, backup notifications relate to the status of backups rather than security alerts, user audit trails focus on user activity without generating security alerts, and cloud monitoring tools generally provide operational metrics rather than specific security incident alerts.

8. How can teams collaborate effectively on video projects using Google Workspace?

A. By using Google Calendar for scheduling

B. By using Google Meet and Google Drive

C. By creating shared online workspaces

D. By submitting reports via Google Docs

Using Google Meet and Google Drive together fosters effective collaboration among teams working on video projects. Google Meet provides a robust platform for real-time video communication, allowing team members to brainstorm, discuss ideas, and provide instant feedback during live meetings. This interaction can significantly enhance the creative process and streamline decision-making. On the other hand, Google Drive serves as a central repository for all the project's relevant files, including raw video footage, scripts, storyboards, and edits. Team members can upload, store, and share files seamlessly, ensuring everyone has access to the most current versions and assets of the project. The integration of these tools allows teams to communicate and coordinate their efforts efficiently, leading to improved collaboration and productivity. Other options, while helpful in different contexts, do not directly enhance real-time interaction and resource sharing in the same manner as the combination of Google Meet and Google Drive.

9. What action allows the Director of Finance to be alerted when two auditors share files externally?

A. Create a Google Group that includes the two auditors and set a Drive DLP Rule.

B. Create a Content Compliance rule for outbound share notifications.

C. Create two Drive Audit Alerts for each auditor's external shares.

D. Check the Admin Console Dashboard periodically for notifications.

The most effective action to alert the Director of Finance when two auditors share files externally is to create two Drive Audit Alerts for each auditor's external shares. This approach ensures that the Director is promptly notified each time either auditor engages in external file sharing, thus providing direct oversight and the accountability necessary when sensitive information is involved. Drive Audit Alerts are intentionally designed to monitor and track specific activities related to files, including sharing events. By setting these alerts for each auditor, the Director of Finance can receive instant notifications, enabling them to respond swiftly if any external sharing activities occur that they need to be aware of. This method provides a clear and direct line of information regarding file sharing practices. The alternative options do not provide the same level of specificity or immediacy. For instance, a Google Group with a Drive DLP Rule may not provide adequate targeted alerts, and while a Content Compliance rule could notify about outbound sharing, it generally covers broader compliance issues and may not be tailored for specific audit scenarios. Checking the Admin Console Dashboard regularly might miss real-time sharing events, which is less proactive compared to setting up direct alerts for individual auditors.

10. What should you do to ensure the correct users in finance receive a commonly used third-party app?

A. For the Finance OU, enable the third-party app in SAML apps.

B. For the Finance OU, enable the third-party app in Marketplace Apps.

C. At the root level, disable the third-party app.

D. At the root level, allow users to install only whitelisted apps from the G Suite Marketplace.

Enabling the third-party app in Marketplace Apps specifically for the Finance Organizational Unit (OU) is the right approach to ensure that the correct users in finance have access to the application. Marketplace Apps in G Suite allow administrators to manage and control which applications are accessible to specific users or groups within the organization. By enabling the app at the OU level, you ensure that only those users within the Finance OU can utilize it, streamlining access based on their roles and needs. This method provides a tailored approach to app management, allowing for better oversight of which applications are available to different segments of the organization while ensuring compliance and security. Other options don't provide a focused solution tailored to the specific needs of the Finance department. For example, enabling the app in SAML apps focuses on Single Sign-On integrations and may not directly manage access as effectively as Marketplace Apps. Disabling the app at the root level or restricting app installations would unnecessarily limit access for those who actually need the app in that specific department.

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://g-professionalcollaborationengineer.examzify.com

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