Google Google-Workspace-Administrator Zertifizierungsprüfung, Google-Workspace-Administrator Antworten

Übrigens, Sie können die vollständige Version der ExamFragen Google-Workspace-Administrator Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1rwtuLCMAmHvYe1qV2_i2hfwekRzh2x0l

Solange Sie die Prüfung benötigen, können wir jederzeit die Schulungsunterlagen zur Google Google-Workspace-Administrator Zertifizierungsprüfung aktualisieren, um Ihre Prüfungsbedürfnisse abzudecken. Die Schulungsunterlagen von ExamFragen enthalten viele Übungsfragen und Antworten zur Google Google-Workspace-Administrator Zertifizierungsprüfung und geben Ihnen eine 100%-Pass-Garantie. Mit unseren Schulungsunterlagen können Sie sich besser auf Ihre Google-Workspace-Administrator Prüfung vorbereiten. Außerdem bieten wir Ihnen einen einjährigen kostenlosen Update-Service.

Die Google-Workspace-Administrator-Prüfung ist für Fachleute konzipiert, die ihre Expertise im Management und in der Verwaltung von Google Workspace-Lösungen demonstrieren möchten. Diese Zertifizierung eignet sich ideal für IT-Administratoren, Systemadministratoren und technische Fachleute, die ihre Fähigkeit demonstrieren möchten, Google Workspace zur Steigerung des Geschäftserfolgs zu nutzen.

Die Google Workspace Administrator-Zertifizierungsprüfung ist darauf ausgelegt, die Fähigkeiten von Fachleuten zu testen, die Google Workspace, früher bekannt als G Suite, verwalten und administrieren. Diese Prüfung richtet sich an Personen, die für die Verwaltung und Optimierung von Google Workspace-Diensten in ihrer Organisation verantwortlich sind. Die Prüfung ist darauf ausgelegt, das Wissen des Kandidaten über die Kernprinzipien von Google Workspace, einschließlich Gmail, Kalender, Drive und Docs, zu testen. Die Prüfung umfasst auch fortgeschrittene Themen wie Sicherheit, Compliance und Mobile Device Management.

>> Google Google-Workspace-Administrator Zertifizierungsprüfung <<

Google-Workspace-Administrator Neuesten und qualitativ hochwertige Prüfungsmaterialien bietet - quizfragen und antworten

Wollen Sie die Fragenkataloge zur Google Google-Workspace-Administrator Zertifizierungsprüfung haben, die Ihre Zeit und Energie sparen können? Dann wählen Sie ExamFragen. Unsere Fragenkataloge für Google Google-Workspace-Administrator Zertifizierungsprüfung werden Ihnen einjähriger Aktualisierung kostenlos bieten, damit Sie die neulich aktualisierten Informationen über Google Google-Workspace-Administrator Zertifizierungsprüfung erhalten können. Wir versprechen Ihnen, dass wir Ihnen alle Ihre bezahlten Summe zurückgeben werden, wenn Sie die Zertifizierungsprüfung nicht bestehen, nachdem Sie unsere Produkte gekauft haben.

Die Google Workspace Administrator-Zertifizierungsprüfung ist eine weltweit anerkannte professionelle Zertifizierung auf professioneller Ebene, die für Fachleute geeignet ist, die ihre Karriereaussichten verbessern möchten. Durch Erreichen dieser Zertifizierung können Einzelpersonen ihre Fähigkeit demonstrieren, Google Workspace -Anwendungen effektiv zu verwalten und bereitzustellen. Diese Zertifizierung ist ideal für IT -Fachkräfte, Systemadministratoren und IT -Berater, die für die Verwaltung und Bereitstellung von Google Workspace -Anwendungen verantwortlich sind.

Google Cloud Certified - Professional Google Workspace Administrator Google-Workspace-Administrator Prüfungsfragen mit Lösungen (Q102-Q107):

102. Frage
Your organization has been using Google Workspace for almost a year, and your annual security and risk assessment initiative is approaching in preparation for the risk assessment you want to quickly review all the security-related settings for Gmail, Drive and Calendar and identify the ones that may be posing risk What should you do?

- A. Review the Security health page in the Admin console
- B. Review all the alerts in the Alert center
- C. Review the Gmail Drive, and Calendar reports in the Reporting section in the Admin console.
- D. Review all settings for each organizational unit (OU) separately because it is the only way to see the security settings tor Workspace apps

Antwort: A

Begründung:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Navigate to Security Health Page: In the Admin console, go to the Security section and select Security health. This page provides a comprehensive overview of your organization's security settings.
Review Security Settings: The Security health page lists various security settings for Gmail, Drive, and Calendar. It highlights settings that might pose a risk and provides recommendations for improvement.
Identify and Mitigate Risks: Carefully review the highlighted settings. Follow the recommendations to enhance your organization's security posture. This ensures that any potential risks are identified and mitigated promptly.
Reference:
Google Workspace Admin Help: Security health
Google Workspace Security Best Practices

103. Frage
Your CISO is concerned about third party applications becoming compromised and exposing Google Workspace data you have made available to them. How could you provide granular insight into what data third party applications are accessing?
What should you do?

- A. Create a report using the Calendar Audit Activity logs.
- B. Create a report using the OAuth Token Audit Activity logs.
- C. Create a report using the Drive Audit Activity logs.
- D. Create a reporting using the API Permissions logs for Installed Apps.

Antwort: B

Begründung:
* Access Admin Console: Log into your Google Workspace Admin Console.
* Navigate to Reports: Go to the Reports section within the Admin Console.
* OAuth Token Audit Log: Access the OAuth Token Audit Activity logs. This log provides detailed information about third-party applications that have been granted access to your Google Workspace data.
* Review Data Access: Review the logs to see which applications have accessed what type of data. This includes details on the scopes of access requested by the applications.
* Generate Report: Create a report from these logs to provide granular insight into the data accessed by third-party applications. This report can be used to assess and mitigate any potential risks.
References
* Google Support: Token audit log

104. Frage
How can you monitor increases in user reported Spam as identified by Google?

- A. Review user-reported spam in the Investigation Tool.
- B. Review post-delivery activity in the Email logs.

- C. Review post-delivery activity in the BigQuery Export.
- D. Review spike in user-reported spam in the Alert center.

Antwort: D

Begründung:
https://support.google.com/a/answer/9104586?hl=en

105. Frage
You are the administrator of a domain that requires iOS mobile device management. What initial steps should be taken to ensure that you can properly manage end-user iOS devices?

- A. In the Admin console, navigate to iOS management, and enable the Apple Push Certificate connector.
- B. Configure an Apple Push Certificate, and be sure to use a work address that can be accessed in the future.
- C. Configure an Apple Push Certificate, and select "certificate never expires."
- D. Follow the prompts under "company owned devices," and select "iOS Management." Select the option to "enforce management on iOS devices."

Antwort: B

Begründung:
To ensure proper management of iOS devices, follow these steps:
* Sign in to the Google Admin console: Use an account with super administrator privileges.
* Navigate to Device Management: Go to Devices > Mobile and endpoints > Settings > iOS settings.
* Configure Apple Push Certificate:
* Click on "Apple Push Certificate."
* Follow the instructions to create and upload an Apple Push Certificate. Ensure that you use a work email address that will be accessible in the future for renewal purposes.
* Enable iOS Management:
* Once the Apple Push Certificate is configured, enable iOS device management.
* Optionally, enforce management on iOS devices to ensure all devices are compliant.
References:
* Google Workspace Admin Help - Set up Apple Push Certificate
* Google Workspace Admin Help - Manage iOS devices

106. Frage
The human resources department notified you of a legal investigation that was started for an employee in the finance department. You need to ensure that this employee's Google Drive data is preserved for at least one year and does not get deleted by the user or by other means. The Google Vault default retention rules for Drive are set for five years. What should you do?

- A. Change the Vault default retention rule to one year instead of five.
- B. Place the employee into a separate organizational unit (OU). Create a custom one-year retention rule for this OU.
- C. Create a hold in Vault for the employee's Drive.
- D. Confirm that the Vault default retention rule is set for five years.

Antwort: C

Begründung:
When there's a legal investigation, the priority is to ensure that relevant data is preserved and not deleted, regardless of retention policies or user actions. A "hold" (also known as a litigation hold or legal hold) in Google Vault is specifically designed for this purpose. It overrides all retention rules (both default and custom) and prevents any data covered by the hold from being purged, even if a user attempts to delete it.
Here's why the other options are not the correct or best solution:
* A. Change the Vault default retention rule to one year instead of five. Changing the default retention rule would affect all Drive data in your organization, not just this specific employee's. It's a broad change and not suitable for a targeted legal hold. Moreover, it wouldn't guarantee preservation against user deletions.
* B. Place the employee into a separate organizational unit (OU). Create a custom one-year retention rule for this OU. While creating custom retention rules for OUs is possible, it's not the primary mechanism for a legal hold. Retention rules define when data can be deleted, but a hold prevents deletion irrespective of the retention period. If the employee deletes the data, a retention rule

won't stop it from moving to trash (and eventually being purged) unless a hold is in place. Furthermore, a one-year retention rule isn't the goal; the goal is to preserve for "at least one year" (meaning indefinitely until the hold is released). The default five-year rule is already longer than one year, but doesn't override user deletion.
* D. Confirm that the Vault default retention rule is set for five years. The question states that the default retention rule for Drive is already set for five years. While this is good for general data retention, it does not prevent a user from deleting their own files from Drive, nor does it specifically address the need for a legal hold where data must be absolutely preserved. A default retention rule does not override user deletion or ensure data preservation for legal purposes.
References from Google Workspace Administrator:
* Holds in Google Vault: This is the core concept. Holds prevent data from being purged from Google systems, regardless of retention rules or user actions, until the hold is released. They are specifically used for legal discovery or investigation purposes.
Reference: Google Workspace Admin Help: Place holds on user accounts
Reference: Google Workspace Admin Help: Holds prevent data from being purged (This page explicitly states that "Holds override retention rules-even if the retention period expires, data on hold is preserved.") Retention rules in Google Vault: While relevant to data management, retention rules define when data can be deleted if no hold applies. They do not prevent users from deleting data or ensure preservation for legal holds.
Reference: Google Workspace Admin Help: How retention works with Google services

107. Frage
.....

Google-Workspace-Administrator Antworten: https://www.examfragen.de/Google-Workspace-Administrator-pruefung-fragen.html

myportal.utt.edu.tt, www.stes.tyc.edu.tw, formationenlignemaroc.com, Disposable vapes

P.S. Kostenlose und neue Google-Workspace-Administrator Prüfungsfragen sind auf Google Drive freigegeben von ExamFragen verfügbar: https://drive.google.com/open?id=1rwtuLCMAmHvYe1qV2_i2hfwekRzh2x0l