The Best Google-Workspace-Administrator Exam Study Material Premium Files and Preparation Tool (Apr-2023) [Q26-Q47

The Best Google-Workspace-Administrator Exam Study Material Premium Files and Preparation Tool (Apr-2023) Get Instant Access to Google-Workspace-Administrator Practice Exam Questions

The Google-Workspace-Administrator (Google Cloud Certified - Professional Google Workspace Administrator) Certification Exam is designed to test an individual's knowledge and skills in managing and administering Google Workspace. This certification exam is ideal for IT professionals, administrators, and managers who are responsible for deploying, configuring, and managing Google Workspace in their organizations. The exam covers a wide range of topics, including user and group management, security and compliance, data migration and management, and collaboration and communication tools.

Q26. You act as the Google Workspace Administrator for a company that has just acquired another organization. The acquired company will be migrated into your Workspace environment in 6 months. Management has asked you to ensure that the Google Workspace users you currently manage can efficiently access rich contact information in Workspace for all users. This needs to occur before the migration, and optimally without additional expenditure. What step do you take to populate contact information for all users?
* Bulk-upload the contact information for these users via CSV into the Google Directory.
* Use the Domain Shared Contacts API to upload contact information for the acquired company&#8217;s users.
* Provision and license Google Workspace accounts for the acquired company&#8217;s users because they will need accounts in the future.
* Prepare an uploadable file to be distributed to your end users that allows them to add the acquired company&#8217;s user contact information to their personal contacts.
The Domain Shared Contacts API lets your applications get and update external contacts that are shared with all users in a Google Workspace domain. Shared contacts are visible to all users of a Google Workspace domain and all Google services have access to the contact list https://developers.google.com/admin-sdk/domain-shared-contacts/overview

Q27. A retail company has high employee turnover due to the cyclical nature in the consumer space. The increase in leaked confidential content has created the need for a specific administrative role to monitor ongoing employee security investigations. What step should you take to increase the visibility of such investigations?
* Assign the &#8216;Services Admin&#8217; role to an administrator with &#8216;Super Admin&#8217; privileges.
* Create a &#8216;Custom Role&#8217; and add all the Google Vault privileges for a new administrator.
* Validate that the new administrator has access to Google Vault.
* Create a &#8216;Custom Role&#8217; and add the ability to manage Google Vault matters, holds, searches, and exports.

Q28. Several customers have reported receiving fake collection notices from your company. The emails were received from accounts.receivable@yourcompany.com, which is the valid address used by your accounting department for such matters, but the email audit log does not show the emails in question. You need to stop these emails from being sent.

What two actions should you take? (Choose two.)
* Change the password for suspected compromised account accounts.receivable@yourcompany.com.
* Configure a Sender Policy Framework (SPF) record for your domain.
* Configure Domain Keys Identified Mail (DKIM) to authenticate email.
* Disable mail delegation for the accounts.receivable@yourcompany.com account.

* Disable &#8220;Allow users to automatically forward incoming email to another address.&#8221;
https://support.google.com/a/answer/33786?hl=en

https://support.google.com/a/answer/174124?hl=en

Q29. Your organization is on Google Workspace Enterprise and allows for external sharing of Google Drive files to facilitate collaboration with other Google Workspace customers. Recently you have had several incidents of files and folders being broadly shared with external users and groups. Your chief security officer needs data on the scope of external sharing and ongoing alerting so that external access does not have to be disabled.

What two actions should you take to support the chief security officer&#8217;s request? (Choose two.)
* Create a custom Dashboard for external sharing in the Security Investigation Tool.
* Review total external sharing in the Aggregate Reports section.
* Create an alert from Drive Audit reports to notify of external file sharing.
* Automatically block external sharing using DLP rules.
* Review who has viewed files using the Google Drive Activity Dashboard.

Q30. Your organization&#8217;s Sales Department uses a generic user account (sales@company.com) to manage requests. With only one employee responsible for managing the departmental account, you are tasked with providing the department with the most efficient means to allow multiple employees various levels of access and manage requests from a common email address.

What should you do?
* Configure a Google Group as an email list.
* Delegate email access to department employees.
* Configure a Google Group as a collaborative inbox.
* Configure a Google Group, and set the Access Level to Announcement Only.
https://support.google.com/a/answer/167430?hl=en

Q31. Your organization is part of a highly regulated industry with a very high turnover. In order to recycle licenses for new employees and comply with data retention regulations, it has been determined that certain Google Workspace data should be stored in a separate backup environment.

How should you store data for this situation?
* Use routing rules to dual-deliver mail to an on-premises SMTP server and Google Workspace.
* Write a script and use Google Workspace APIs to access and download user data.
* Use a third-party tool to configure secure backup of Google Workspace data.
* Train users to use Google Takeout and store their archives locally.
https://cloud.google.com/solutions/partners/backing-up-g-suite-data-with-spinbackup

Q32. Your company has been engaged in a lawsuit, and the legal department has been asked to discover and hold all email for two specific users. Additionally, they have been asked to discover and hold any email referencing &#8220;Secret Project 123.&#8221;
What steps should you take to satisfy this request?
* Create a Matter and a Hold. Set the Hold to Gmail, set it to the top level Organization, and set the search terms to &#8220;secret project 123.&#8221; Create a second Hold. Set the second Hold to Gmail, set it to Accounts, and enter: user1 @your-company.com, user2@your-company.com. Save.
* Create a Matter and a Hold. Set the Hold to Gmail, set it to Accounts, and set the usernames to: user1@your-company.com, user2@your-company. Set the search terms to: (secret project 123). Save.
* Create a Matter and a Hold. Set the Hold to Gmail, set it to Accounts, and enter: user1@your- company.com AND user2@your-company.com. Set the search terms to: secret AND project AND 123. Save.
* Create a Matter and a Hold. Set the Hold to Gmail, set it to Accounts, and set the usernames to: user1@your-company.com,

user2@your-company. Set the search terms to secret OR project OR 123. Save.
The correct way to search for the esact term is in quotes (&#8220;project 123&#8221; and not (project 123)). Ref: https://support.google.com/vault/answer/2474474?hl=en. Also, afeter doing this ytou must create the retention rule using comas to separate user from user.

Q33. As a Workspace Administrator, you want to keep an inventory of the computers and mobile devices your company owns in order to track details such as device type and who the device is assigned to. How should you add the devices to the company-owned inventory?
* Download the company owned inventory template CSV file from the admin panel, enter the serial number of the devices, and upload it back to the company owned inventory in the admin panel.
* Download the company owned inventory template CSV file from the admin panel, enter the Device OS, serial number and upload it back to the company owned inventory in the admin panel.
* Download the company owned inventory template CSV file from the admin panel, enter the asset tag of the devices, and upload it back to the company owned inventory in the admin panel.
* Download the company owned inventory template CSV file from the admin panel, enter the Device OS, asset tag and upload it back to the company owned inventory in the admin panel.
https://support.google.com/a/answer/7129612?hl=en#zippy=%2Cassigning-devices%2Cadd-android-devices-for-the-most-management-features:~:text=Add%20devices%20to,and%20upload%20status.

Q34. As the Workspace Administrator, you have been asked to configure Google Cloud Directory Sync (GCDS) in order to manage Google Group memberships from an internal LDAP server. However, multiple Google Groups must have their memberships managed manually. When you run the GCDS sync, you notice that these manually managed groups are being deleted. What should you do to prevent these groups from being deleted?
* In the GCDS configuration manager, update the group deletion policy setting to &#8220;don&#8217;t delete Google groups not found in LDAP.&#8221;
* Use the Directory API to check and update the group&#8217;s membership after the GCDS sync is completed.
* Confirm that the base DN for the group email address attribute matches the base DN for the user email address attribute.
* In the user attribute settings of the GCDS configuration manager options, set the Google domain users deletion/suspension policy to &#8220;delete only active Google domain users not found in LDAP.&#8221;
https://support.google.com/a/answer/6258071?hl=en#zippy=%2Cgoogle-group-deletion-policy Don&#8217;t delete Google Groups not found in LDAP If checked, Google Group deletions in your Google domain are disabled, even when the Groups aren&#8217;t in your LDAP server.

Q35. In your organization, users have been provisioned with either Google Workspace Enterprise, Google Workspace Business, or no license, depending on their job duties, and the cost of user licenses is paid out of each division&#8217;s budget. In order to effectively manage the license disposition, team leaders require the ability to look up the type of license that is currently assigned, along with the last logon date, for their direct reports.

You have been tasked with recommending a solution to the Director of IT, and have gathered the following requirements:

Team leaders must be able to retrieve this data on their own (i.e., self-service).

Team leaders are not permitted to have any level of administrative access to the Google Workspace Admin panel.

Team leaders must only be able to look up data for their direct reports.

The data must always be current to within 1 week.

Costs must be mitigated.

What approach should you recommend?
* Export log data to BigQuery with custom scopes.
* Use a third-party tool.
* Use App Script and filter views within a Google Sheet.
* Create an app using AppMaker and App Script.
https://support.google.com/a/answer/9682494?hl=en

Q36. Your company has decided to change SSO providers. Instead of authenticating into Google Workspace and other cloud services with an external SSO system, you will now be using Google as the Identity Provider (IDP) and SSO provider to your other third-party cloud services.

What two features are essential to reconfigure in Google Workspace? (Choose two.)
* Apps > add SAML apps to your domain.
* Reconfigure user provisioning via Google Cloud Directory Sync.
* Replace the third-party IDP verification certificate.
* Disable SSO with third party IDP.
* Enable API Permissions for Google Cloud Platform.

Q37. A company has thousands of Chrome devices and bandwidth restrictions. They want to distribute the Chrome device updates over a period of days to avoid traffic spikes that would impact the low bandwidth network.

Where should you enable this in the Chrome management settings?
* Randomly scatter auto-updates.
* Update over cellular.
* Disable Auto update.
* Throttle the bandwidth.
Randomly scatter auto-updates over Only available if you choose to scatter updates Specifies the approximate number of days that managed Chrome devices download an update after its release. You can use this setting to avoid causing traffic spikes in old or low-bandwidth networks. Devices that are offline during this period download the update when they&#8217;re online again.
https://support.google.com/chrome/a/answer/1375678?hl=en#zippy=%2Cauto-update-settings

Q38. Your organization recently deployed Google Workspace. Your admin team has been very focused on configuring the core services for your environment, which has left you little time to pay attention to other areas. Your security team has just informed you that many users are leveraging unauthorized add-ons, and they are concerned about data exfiltration. The admin team wants you to cut off all add-ons access to Workspace data immediately and block all future add-ons until further notice. However, they approve of users leveraging their Workspace accounts to sign into third-party sites. What should you do?
* Modify your Marketplace Settings to block users from installing any app from the Marketplace.
* Set all API services to &#8220;restricted access&#8221; and ensure that all connected apps have limited access.
* Remove all client IDs and scopes from the list of domain-wide delegation API clients.
* Block each connected app&#8217;s access.
https://support.google.com/a/answer/162106?hl=en#zippy=%2Cview-edit-or-delete-clients-and-scopes:~:text=View%2C%20edit%2C%20or,immediately%20stop%20working.

Q39. Your organization syncs directory data from Active Directory to Google Workspace via Google Cloud Directory Sync. Users and Groups are updated from Active Directory on an hourly basis. A user&#8217;s last name and primary email address have to be changed. You need to update the user&#8217;s data.

What two actions should you take? (Choose two.)
* Add the user&#8217;s old email address to their account in the Google Workspace Admin panel.
* Change the user&#8217;s primary email address in the Google Workspace Admin panel.

* Change the user&#8217;s last name in the Google Workspace Admin panel.
* Change the user&#8217;s primary email in Active Directory.
* Change the user&#8217;s last name in Active Directory.
https://support.google.com/a/answer/106368?hl=en

Q40. Your company has an OU that contains your sales team and an OU that contains your market research team. The sales team is often a target of mass email from legitimate senders, which is distracting to their job duties. The market research team also receives that email content, but they want it because it often contains interesting market analysis or competitive intelligence. Constant Contact is often used as the source of these messages. Your company also uses Constant Contact for your own mass email marketing. You need to set email controls at the Sales OU without affecting your own outgoing email or the market research OU.

What should you do?
* Create a blocked senders list as the Sales OU that contains the mass email sender addresses, but bypass this setting for Constant Contact emails.
* Create a blocked senders list at the root level, and then an approved senders list at the Market Research OU, both containing the mass email sender addresses.
* Create a blocked senders list at the Sales OU that contains the mass email sender addresses.
* Create an approved senders list at the Market Research OU that contains the mass email sender addresses.
&#8220;The sales team is often a target of mass email from legitimate senders, which is distracting to their job duties&#8221; and &#8220;Constant Contact is often used as the source of these messages&#8221;. Nowhere in the question did it specify that emails received via Constant Contact should be allowed for the sales OU. It only mentioned that the company uses Constant Contact for its own outgoing emails- which in this case does not affect the answer at all.

Q41. The CEO of your company heard about new security and collaboration features and wants to know how to stay up to date. You are responsible for testing and staying up to date with new features, and have been asked to prepare a presentation for management.

What should you do?
* Download the Google Workspace roadmap, and work together with a deployment specialist for new features.
* Create a support ticket for the Google Workspace roadmap, and ask to enable the latest release of Google Workspace.
* Subscribe to the Google Workspace release calendar, and Join the Google Cloud Connect Community.
* Change Google Workspace release track to: Rapid Release for faster access to new features.

Q42. User A is a Basic License holder. User B is a Business License holder. These two users, along with many additional users, are in the same organizational unit at the same company. When User A attempts to access Drive, they receive the following error: &#8220;We are sorry, but you do not have access to Google Docs Editors. Please contact your Organization Administrator for access.&#8221; User B is not presented with the same error and accesses the service without issues.

How do you provide access to Drive for User A?
* Select User A in the Directory, and under the Apps section, check whether Drive and Docs is disabled. If so, enable it in the User record.
* In Apps > Google Workspace > Drive and Docs, select the organizational unit the users are in and enable Drive for the organizational unit.
* In Apps > Google Workspace, determine the Group that has Drive and Docs enabled as a service. Add User A to this group.
* Select User A in the Directory, and under the Licenses section, change their license from Basic to Business to add the Drive and Docs service.
https://support.google.com/a/answer/9050643

Q43. The Director of your Finance department has asked to be alerted if two financial auditors share any files outside the domain. You need to set an Admin Alert on Drive Sharing.

What should you do?
* Create a Google Group that has the two auditors as members, and then create a Drive DLP Rule that is assigned to that Group.
* Create a Content Compliance rule that looks for outbound share notifications from those two users, and Bcc the Director on those emails.
* Create two Drive Audit Alerts, one for each user, where the Visibility is &#8220;Shared Externally,&#8221; and email them to the Director.
* Check the Admin Console Dashboard Insights page periodically for external shares, and notify the Director of any changes.
https://support.google.com/a/answer/4579696?hl=en

https://support.google.com/a/answer/9725685

Q44. Your organization has just appointed a new CISO. They have signed up to receive admin alerts and just received an alert for a suspicious login attempt. They are trying to determine how frequently suspicious login attempts occur within the organization. The CISO has asked you to provide details for each user account that has had a suspicious login attempt in the past year and the number of times it occurred for each account.

What action should you take to meet these requirements?
* Use the login audit report to export all suspicious login details for analysis.
* Create a custom dashboard with the security investigation tool showing suspicious logins.
* Use the account activity report to export all suspicious login details for analysis.
* Create a custom query in BigQuery showing all suspicious login details.
Login audit log Track user sign-in activity You can use the Login audit log to track user sign-ins to your domain. You can review all sign-ins from web browsers. If a user signs in from an email client or a non-browser application, you can only review reports of suspicious attempts. Forward log event data to the Google Cloud Platform You can opt in to share the log event data with Google Cloud Platform. If you turn on sharing, data is forwarded to Cloud Logging, where you can query and view your logs, and control how you route and store your logs https://support.google.com/a/answer/4580120?hl=en

Q45. As a team manager, you need to create a vacation calendar that your team members can use to share their time off. You want to use the calendar to visualize online status for team members, especially if multiple individuals are on vacation What should you do to create this calendar?
* Request the creation of a calendar resource, configure the calendar to &#8220;Auto-accept invitations that do not conflict,&#8221; and give your team &#8220;See all event details&#8221; access.
* Create a secondary calendar under your account, and give your team &#8220;Make changes to events&#8221; access.
* Request the creation of a calendar resource, configure the calendar to &#8220;Automatically add all invitations to this calendar,&#8221; and give your team &#8220;See only free/busy&#8221; access.
* Create a secondary calendar under your account, and give your team &#8220;See only free/busy&#8221; access
https://support.google.com/a/answer/1034381?hl=en#:~:text=Automatically%20add%20all%20invitations%20to%20this%20calendar%E2%80%94All%20invitations%20show%20up%20on%20the%20resource%27s%20calendar%20even%20if%20some%20of%20them%20are%20for%20events%20that%20take%20place%20at%20the%20same%20time.

Q46. Your company is deploying Chrome devices. You want to make sure the machine assigned to the employee can only be signed in to by that employee and no one else.

What two things should you do? (Choose two.)
* Disable Guest Mode and Public Sessions.
* Enable a Device Policy of Sign In Screen and add the employee email address.
* Enroll a 2-Factor hardware key on the device using the employee email address.
* Enable a User Policy of Multiple Sign In Access and add just the employee email address.
* Enable a Device Policy of Restrict Sign In to List of Users, and add the employee email address.
https://support.google.com/chrome/a/answer/1375678?hl=en

Q47. Your Chief Information Security Officer is concerned about phishing. You implemented 2 Factor Authentication and forced hardware keys as a best practice to prevent such attacks. The CISO is curious as to how many such email phishing attempts you&#8217;ve avoided since putting the 2FA+Hardware Keys in place last month.

Where do you find the information your CISO is interested in seeing?
* Security > Advanced Security Settings > Phishing Attempts
* Apps > Google Workspace > Gmail > Phishing Attempts
* Security > Dashboard > Spam Filter: Phishing
* Reporting > Reports > Phishing
https://support.google.com/a/answer/7491892?hl=en