DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: Google
Exam: Professional Google Workspace Administrator
Number of questions in the database: 149
Exam Version: NOV.2026

Topic 1 - Exam A

Question #1*Topic 1*

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?

- A. In the GCDS configuration manager, update the group deletion policy setting to “don't delete Google groups not found in LDAP.”
- B. Use the Directory API to check and update the group’s membership after the GCDS sync is completed.
- C. Confirm that the base DN for the group email address attribute matches the base DN for the user email address attribute.
- D. In the user attribute settings of the GCDS configuration manager options, set the Google domain users deletion/suspension policy to “delete only active Google domain users not found in LDAP.”

Correct Answer: *A*

Respuesta por mayor votación de la comunidad

A (100%)

Question #2*Topic 1*

Your marketing department needs an easy way for users to share items more appropriately. They want to easily link-share Drive files within the marketing department, without sharing them with your entire company. What should you do to fulfil this request? (Choose two.)

- A. Create a shared drive that's shared internally organization-wide.
- B. Update Drive sharing for the marketing department to restrict to internal.
- C. Create a shared drive for internal marketing use.
- D. Update the link sharing default to the marketing team when creating a document.
- E. In the admin panel Drive settings, create a target audience that has all of marketing as members.

https://dbcloud.academy/

Correct Answer: *CE*

Respuesta por mayor votación de la comunidad

CE (74%)

BE (17%)

9%

Question #3*Topic 1*

Your company has a broad, granular IT administration team, and you are in charge of ensuring proper administrative control. One of those teams, the security team, requires access to the Security Investigation Tool. What should you do?

- A. Assign the pre-built security admin role to the security team members.
- B. Create a Custom Admin Role with the Security Center privileges, and then assign the role to each of the security team members.
- C. Assign the Super Admin Role to the security team members.
- D. Create a Custom Admin Role with the security settings privilege, and then assign the role to each of the security team members.

Correct Answer: *B*

Respuesta por mayor votación de la comunidad

B (72%)

D (28%)

Question #4*Topic 1*

Your organization has a new security requirement around data exfiltration on iOS devices. You have a requirement to prevent users from copying content from a Google app (Gmail, Drive, Docs, Sheets, and Slides) in their work account to a Google app in their personal account or a third-party app. What steps should you take from the admin panel to prevent users from copying data from work to non-work apps on iOS devices?

- A. Navigate to “Data Protection” setting in Google Admin Console's Device management section and disable the “Allow users to copy data to personal apps” checkbox.
- B. Disable “Open Docs in Unmanaged Apps” setting in Google Admin Console’s Device management section.
- C. Navigate to Devices > Mobile and endpoints > Universal Settings > General and turn on Basic Mobile Management.

https://dbcloud.academy/

- D. Clear the “Allow items created with managed apps to open in unmanaged apps” checkbox.

Correct Answer: *A*

Respuesta por mayor votación de la comunidad

A (90%)

10%

Question #5*Topic 1*

Your organization recently implemented context-aware access policies for Google Drive to allow users to access Drive only from corporate managed desktops. Unfortunately, some users can still access Drive from non-corporate managed machines. What preliminary checks should you perform to find out why the Context-Aware Access policy is not working as intended? (Choose two.)

- A. Confirm that the user has a Google Workspace Enterprise Plus license.
- B. Delete and recreate a new Context-Aware Access device policy.
- C. Check whether device policy application is installed on users’ devices.
- D. Confirm that the user has at least a Google Workspace Business license.
- E. Check whether Endpoint Verification is installed on users’ desktops.

Correct Answer: *AE*

Respuesta por mayor votación de la comunidad

AE (74%)

CE (26%)

Question #6*Topic 1*

Your organization has enabled spoofing protection against unauthenticated domains. You are receiving complaints that email from multiple partners is not being received. While investigating this issue, you find that emails are all being sent to quarantine due to the configured safety setting. What should be the next step to allow uses to review these emails and reduce the internal complaints while keeping your environment secure?

- A. Add your partner domains IPs to the Inbound Gateway setting.
- B. Change the spoofing protection to deliver the emails to spam instead of quarantining them.
- C. Add your partner sending IP addresses to an allowlist.
- D. Change the spoofing protection to deliver the emails to inboxes with a custom warning instead of quarantining them.

https://dbcloud.academy/

Correct Answer: *B*

Respuesta por mayor votación de la comunidad

B (66%)

A (20%)

9%

Question #7*Topic 1*

As the Workspace Administrator, you have been asked to delete a temporary Google Workspace user account in the marketing department. This user has created Drive documents in My Documents that the marketing manager wants to keep after the user is gone and removed from Workspace. The data should be visible only to the marketing manager. As the Workspace Administrator, what should you do to preserve this user's Drive data?

- A. In the user deletion process, select “Transfer” in the data in other apps section and add the manager's email address.
- B. Use Google Vault to set a retention period on the OU where the users reside.
- C. Before deleting the user, add the user to the marketing shared drive as a contributor and move the documents into the new location.
- D. Ask the user to create a folder under MyDrive, move the documents to be shared, and then share that folder with the marketing team manager.

Correct Answer: *C*

Respuesta por mayor votación de la comunidad

A (100%)

Question #8*Topic 1*

As a Google Workspace administrator for your organization, you are tasked with controlling which third-party apps can access Google Workspace data. Before implementing controls, as a first step in this process, you want to review all the third-party apps that have been authorized to access Workspace data. What should you do?

- A. Open Admin Console > Security > API Controls > App Access Control > Manage Third Party App Access.
- B. Open Admin Console > Security > API Controls > App Access Control > Manage Google Services.
- C. Open Admin Console > Security > Less Secure Apps.
- D. Open Admin Console > Security > API Controls > App Access Control > Settings.

https://dbcloud.academy/

Correct Answer: *A*

Respuesta por mayor votación de la comunidad

A (100%)

Question #9*Topic 1*

Your organization wants more visibility into actions taken by Google staff related to your data for audit and security reasons. They are specifically interested in understanding the actions performed by Google support staff with regard to the support cases you have opened with Google. What should you do to gain more visibility?

- A. From Google Admin Panel, go to Audit, and select Access Transparency Logs.
- B. From Google Admin Panel, go to Audit, and select Login Audit Log.
- C. From Google Admin Panel, go to Audit, and select Rules Audit Log.
- D. From Google Admin Panel, go to Audit, and select Admin Audit Log.

Correct Answer: *D*

Respuesta por mayor votación de la comunidad

A (100%)

Question #10*Topic 1*

Your organization recently had a sophisticated malware attack that was propagated through embedded macros in email attachments. As a Workspace administrator, you want to provide an additional layer of anti-malware protection over the conventional malware protection that is built into Gmail. What should you do to protect your users from future unknown malware in email attachments?

- A. Run queries in Security Investigation Tool.
- B. Turn on advanced phishing and malware protection.
- C. Enable Security Sandbox.
- D. Enable Gmail confidential mode.

Correct Answer: *B*

Respuesta por mayor votación de la comunidad

C (76%)

B (24%)

https://dbcloud.academy/