GOOGLE-WORKSPACE-ADMINISTRATOR Q&As

Google Cloud Certified - Professional Google Workspace Administrator

Pass Google GOOGLE-WORKSPACE-ADMINISTRATOR Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/google-workspace-administrator.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

Your company wants to provide secure access for its employees. The Chief Information Security Officer disabled peripheral access to devices, but wants to enable 2-Step verification. You need to provide secure access to the applications using Google Workspace.

What should you do?

A. Enable additional security verification via email.

B. Enable authentication via the Google Authenticator.

C. Deploy browser or device certificates via Google Workspace.

D. Configure USB Yubikeys for all users.

Correct Answer: B

Explanation: Enable authentication via the Google Authenticator is the only secure option since USB device aren\\'t usable. Google Authenticator is the most secure option after physical key.

QUESTION 2

Your organization is using Password Sync to sync passwords from Active Directory to Google Workspace. A user changed their network password and cannot log in to Google Workspace with the new password. What steps should you take to troubleshoot this issue?

A. Reinstall Password Sync on all domain controllers.

B. Reauthorize the Password Sync tool in the Google Workspace Admin Console.

C. Confirm that the Password Sync service is running on all domain controllers.

D. Reset the user\\'s password in Active Directory.

Correct Answer: C

Explanation: https://support.google.com/a/answer/11237847?hl=enandref_topic=4498019 The network password is determined to be with AD. In this case, you must verify that password sync is installed on all domain controllers. This is the initial troubleshooting. After this troubleshooting, the logs of these connectors are taken https://www.youtube.com/watch?v=P-r8bvivZuM

QUESTION 3

Your organization\\'s information security team has asked you to determine and remediate if a user (user1@example.com) has shared any sensitive documents outside of your organization. How would you audit access to documents that the user shared inappropriately?

A. Open Security Investigation Tool-> Drive Log Events. Add two conditions: Visibility Is External, and Actor Is user1@example.com.

B. Have the super administrator use the Security API to audit Drive access.

C. As a super administrator, change the access on externally shared Drive files manually under user1@example.com.

D. Open Security Dashboard-> File Exposure Report-> Export to Sheet, and filter for user1@example.com.

Correct Answer: A

https://support.google.com/a/answer/11480192?hl=enandref_topic=11479095#:~:text=View%20files%20shared,Click%20Search.

QUESTION 4

Your company works regularly with a partner. Your employees regularly send emails to your partner\\'s employees. You want to ensure that the Partner contact information available to your employees will allow them to easily select Partner names and reduce sending errors.

What should you do?

A. Educate users on creating personal contacts for the Partner Employees.

B. Add a secondary domain for the Partner Company and create user entries for each Partner user.

C. Create shared contacts in the Directory using the Directory API.

D. Create shared contacts in the Directory using the Domain Shared Contacts API.

Correct Answer: D

https://developers.google.com/admin-sdk/domain-shared-contacts

QUESTION 5

Your company recently acquired an organization that was not leveraging Google Workspace. Your company is currently using Google Cloud Directory Sync (GCDS) to sync from an LDAP directory into Google Workspace. You want to deploy a second instance of GCDS and apply the same strategy with the newly acquired organization, which also has its users in an LDAP directory. How should you change your GCDS instance to ensure that the setup is successful? (Choose two.)

A. Provide your current GCDS instance with admin credentials to the recently acquired organization\\'s LDAP directory.

B. Add an LDAP sync rule to your current GCDS instance in order to synchronize new users.

C. Set up exclusion rules to ensure that users synced from the acquired organization\\'s LDAP are not, suspended.

D. Set up an additional instance of GCDS running on another server, and handle the acquired organization\\'s synchronization.

E. Upgrade to the multiple LDAP version of GCDS.

Correct Answer: CD

Explanation: https://support.google.com/a/answer/7177266?hl=en#zippy=%2Ccan-i-sync- gcds-from-multiple-ldap-

directories GCDS can only sync from a single LDAP directory. If you have multiple LDAP directories, it is recommended that you consolidate your LDAP server data into a single directory. You need to run 2 separate GCDS instances while creating exclusion rules to prevent suspensions/deletions.