Google
GCP-GWA
Google Workspace Administrator

- **Up to Date products, reliable and verified.**
- **Questions and Answers in PDF Format.**

Full Version Features:

- **90 Days Free Updates**
- **30 Days Money Back Guarantee**
- **Instant Download Once Purchased**
- **24 Hours Live Chat Support**

For More Information:

https://www.testsexpert.com/

- **Product Version**

Latest Version: 6.0

Question: 1

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?

A. Assign the 'Services Admin' role to an administrator with 'Super Admin' privileges.
B. Create a 'Custom Role' and add all the Google Vault privileges for a new administrator.
C. Validate that the new administrator has access to Google Vault.
D. Create a 'Custom Role' and add the ability to manage Google Vault matters, holds, searches, and exports.

Answer: D

Question: 2

A subset of users from the finance and human resources (HR) teams need to share documents with an external vendor. However, external content sharing is prohibited for the entire finance team. What would be the most secure method to enable external sharing for this set of users?

A. Download and attach the documents to a Gmail message, and send them to the external vendor.
B. Move all users from the finance org unit to the HR org unit.
C. Enable 'Visitor Sharing' for the entire finance org unit.
D. Create a group with the finance and HR users who need to share externally.

Answer: D

Question: 3

As the newly hired Admin in charge of Google Workspace, you learn that the organization has been using Google Workspace for months and has configured several security rules for accessing Google Drive. A week after you start your role, users start to complain that they cannot access Google Drive anymore from one satellite office and that they receive an error message that "a company policy is blocking access to this app." The users have no issue with Gmail or Google Calendar. While investigating, you learn that both this office's Internet Service Provider (ISP) and the global IP address when accessing the internet were changed over the weekend. What is the most logical reason for this issue?

A. An access level was defined based on the IP range and applied to Google Drive via Context-Aware Access.
B. Under Drive and Docs > Sharing Settings, the "Whitelisted domains" list needs to be updated to add the new ISP domain.
C. The Network Mask defined in Security > Settings > SSO with 3rd Party IdPs should be updated to reflect the new IP range.
D. You need to raise a ticket to Google Cloud Support to have your new IP ranges registered for Drive API access.

Answer: A

Question: 4

An end user informs you that they are having issues receiving mail from a specific sender that is external to your organization. You believe the issue may be caused by the external entity's SPF record being incorrectly configured. Which troubleshooting step allows you to examine the full message headers for the offending message to determine why the messages are not being delivered?

A. Use the Postmaster Tools API to pull the message headers.
B. Use the Email Log Search to directly review the message headers.
C. Use the Security Investigation Tool to review the message headers.
D. Perform an SPF record check on the domain to determine whether their SPF record is valid.

Answer: D

Question: 5

You have been asked to support an investigation that your litigation team is conducting. The current default retention policy for mail is 180 days, and there are no custom mail retention policies in place. The litigation team has identified a user who is central to the investigation, and they want to investigate the mail data related to this user without the user's awareness. What two actions should you take? (Choose two.)

A. Move the user to their own Organization Unit, and set a custom retention policy.
B. Create a hold on the user's mailbox in Google Vault.
C. Reset the user's password, and share the new password with the litigation team.
D. Copy the user's data to a secondary account.
E. Create a matter using Google Vault, and share the matter with the litigation team members.

Answer: B,E

Question: 6

A recent legal investigation requires all emails and Google Drive documents from a specific user to be retrieved. As the administrator, how can you fulfill the legal team's request?

A. Use Security Investigation Tool to Search Google Drive events for all of the user's documents, and use Google Admin > Reports > Email Log Search to find their emails.
B. Search Google Drive for all of the user's documents, and ask them to forward all of their emails.
C. Use the Gmail API and Google Drive API to automatically collect and export data.
D. Utilize Google Vault to hold, search, and export data of interest.

Answer: A

Question: 7

What steps does an administrator need to take to enforce TLS with a particular domain?

A. Enable email safety features with the receiving domain.
B. Set up secure transport compliance with the receiving domain.
C. Configure an alternate secure route with the receiving domain.
D. Set up DKIM authentication with the receiving domain.

Answer: B

Question: 8

Your company's Google Workspace primary domain is "mycompany.com," and it has acquired a startup that is using another cloud provider with a domain named "mystartup.com." You plan to add all employees from the startup to your Google Workspace domain while preserving their current mail addresses. The startup CEO's email address is andrea@mystartup.com, which also matches your company CEO's email address as andrea@mycompany.com, even though they are different people. Each must keep the usage of their email. In addition, your manager asked to have all existing security policies applied for the new employees without any duplication. What should you do to implement the migration?

A. Create a secondary domain, mystartup.com, within your current Google Workspace domain, set up necessary DNS records, and create all startup employees with the secondary domain as their primary email addresses.
B. Create an alias domain, mystartup.com, in your existing Google Workspace domain, set up necessary DNS records, and create all startup employees with the alias domain as their primary email addresses.
C. Create a new Google Workspace domain with "mystartup.com," and create a trust between both domains for reusing the same security policies and sharing employee information within the companies.
D. Create the startup employees in the "mycompany.com' domain, and add a number at the end of the user name whenever there is a conflict. In Gmail > Routing, define a specific route for the OU that targets the startup employees, which will modify the email address domain to "mystartup.com," and

remove any numbers previously added. In addition, confirm that the SPF and DKIM records are properly set.

Answer: D

Question: 9

You are in charge of automating and configuring Google Cloud Directory Sync for your organization. Within the config manager, how can you proactively prevent applying widespread deletions within your Workspace environment if your company's LDAP undergoes a substantial modification?

A. Manually run Google Cloud Directory Sync only after performing a simulated sync.
B. Specify the minimum and maximum number of objects to synchronize in each configuration item.
C. Configure the tool to delete users only when run from the config manager.
D. Configure limits for the maximum number of deletions on each synchronization.

Answer: B

Question: 10

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.

Answer: A,D

Features:

Money Back Guarantee…………..……......

100% Course Coverage……………………

90 Days Free Updates……………………

Instant Email Delivery after Order……………