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.geekcert.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 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?

A. Use the login audit report to export all suspicious login details for analysis.

B. Create a custom dashboard with the security investigation tool showing suspicious logins.

C. Use the account activity report to export all suspicious login details for analysis.

D. Create a custom query in BigQuery showing all suspicious login details.

Correct Answer: A

Explanation: 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

QUESTION 2

Your Security Officer ran the Security Health Check and found the alert that "Installation of mobile applications from unknown sources" was occurring. They have asked you to find a way to prevent that from happening.

Using Mobile Device Management (MDM), you need to configure a policy that will not allow mobile applications to be installed from unknown sources.

What MDM configuration is needed to meet this requirement?

A. In the Application Management menu, configure the whitelist of apps that Android and iOS devices are allowed to install.

B. In the Application Management menu, configure the whitelist of apps that Android, iOS devices, and Active Sync devices are allowed to install.

C. In Android Settings, ensure that "Allow non-Play Store apps from unknown sources installation" is unchecked.

D. In Device Management > Setup > Device Approvals menu, configure the "Requires Admin approval" option.

Correct Answer: C

Reference: https://support.google.com/a/answer/7491893?hl=en

QUESTION 3

The company\\'s ten most senior executives are to have their offices outfitted with dedicated, standardized video conference cameras, microphones, and screens. The goal is to reduce the amount of technical support they require due to frequent, habitual switching between various mobile and PC devices throughout their busy days. You must ensure that it is easier for the executives to join Meet video conferences with the dedicated equipment instead of whatever device they happen to have available.

What should you do?

A. Set up unmanaged Chromeboxes and set the executives\\' homepage to meet.google.com via Chrome settings.

B. Set up the executive offices as reservable Calendar Resources, deploy Hangouts Meet Hardware Kits, and associate the Meet hardware with the room calendars.

C. Deploy Hangouts Meet Hardware Kits to each executive office, and associate the Meet hardware with the executives\\' calendars.

D. Provision managed Chromeboxes and set the executives\\' Chrome homepage to meet. google.com via device policy.

Correct Answer: C

Explanation: https://support.google.com/meethardware/answer/3341435?hl=en If the device is for a single user, such as in a home office or other remote location, you can associate the device with their personal calendar. Whenever an organizer adds that user to a Calendar event, the meeting name appears on their device.

QUESTION 4

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

https://support.google.com/a/answer/6258071?hl=en#zippy=%2Cgoogle-group-deletion- policy

Don\\'t delete Google Groups not found in LDAP If checked, Google Group deletions in your Google domain are disabled, even when the Groups aren\\'t in your LDAP server.

QUESTION 5

You recently started an engagement with an organization that is also using Google Workspace. The engagement will

involve highly sensitive data, and the data needs to be protected from being shared with unauthorized parties both internally and externally. You need to ensure that this data is properly secured.

Which configuration should you implement?

A. Turn on external sharing with whitelisted domains, and add the external organization to the whitelist.

B. Provision accounts within your domain for the external users, and turn off external sharing for that Org.

C. Configure the Drive DLP rules to prevent the sharing of PII and PHI outside of your domain.

D. Create a Team Drive for this engagement, and limit the memberships and sharing settings.

Correct Answer: D

Explanation: https://support.google.com/a/users/answer/9310352#1.1