Number: Professional Collaboration Engineer
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: Professional Collaboration Engineer
Exam Name: Professional Collaboration Engineer

Exam A

QUESTION 1
Your corporate LDAP contains the email addresses of several hundred non-employee business partners. You want to sync these contacts to Google Workspace so they appear in Gmail's address autocomplete for all users in the domain. What are two options to meet this requirement? (Choose two.)

A. Use the Directory API to upload a .csv file containing the contacts.
B. Configure GCDS to populate a Group with external members.
C. Use the People API to upload a .csv file containing the contacts.
D. Develop a custom application to call the Domain Shared Contacts API.
E. Configure GCDS to synchronize shared contacts.

Correct Answer: A, D
Section:

QUESTION 2
Your company uses a whitelisting approach to manage third-party apps and add-ons. The Senior VP of Sales & Marketing has urgently requested access to a new Marketplace app that has not previously been vetted. The company's Information Security policy empowers you, as a Google Workspace admin, to grant provisional access immediately if all of the following conditions are met:
Access to the app is restricted to specific individuals by request only.
The app does not have the ability to read or manage emails.
Immediate notice is given to the Infosec team, followed by the submission of a security risk analysis report within 14 days.
Which actions should you take first to ensure that you are compliant with Infosec policy?

A. Move the Senior VP to a sub-OU before enabling Marketplace Settings > "Allow Users to Install Any App from Google Workspace Marketplace."
B. Confirm that the Senior VP's OU has the following Gmail setting disabled before whitelisting the app: "Let users delegate access to their mailbox."
C. Add the Marketplace app, then review the authorized scopes in Security > Manage API client access.
D. Search the Google Workspace support forum for feedback about the app to include in the risk analysis report.

Correct Answer: A
Section:

QUESTION 3
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: "We are sorry, but you do not have access to Google Docs Editors.
Please contact your Organization Administrator for access." 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?

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.
B. In Apps > Google Workspace > Drive and Docs, select the organizational unit the users are in and enable Drive for the organizational unit.
C. In Apps > Google Workspace, determine the Group that has Drive and Docs enabled as a service. Add User A to this group.
D. 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.

Correct Answer: D
Section:

QUESTION 4
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.)

A. Disable Guest Mode and Public Sessions.
B. Enable a Device Policy of Sign In Screen and add the employee email address.
C. Enroll a 2-Factor hardware key on the device using the employee email address.
D. Enable a User Policy of Multiple Sign In Access and add just the employee email address.
E. Enable a Device Policy of Restrict Sign In to List of Users, and add the employee email address.

Correct Answer: B, C
Section:

QUESTION 5
You are supporting an investigation that is being conducted by your litigation team. 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 matter using Google Vault, and share the matter with the litigation team members.
C. Create a hold on the user's mailbox in Google Vault
D. Reset the user's password, and share the new password with the litigation team.
E. Copy the user's data to a secondary account.

Correct Answer: D, E
Section:

QUESTION 6
Your Accounts Payable department is auditing software license contracts companywide and has asked you to provide a report that shows the number of active and suspended users by organization unit, which has been set up to match the Regions and Departments within your company. You need to produce a Google Sheet that shows a count of all active user accounts and suspended user accounts by Org unit.
What should you do?

A. From the Admin Console Billing Menu, turn off auto-assign, and then click into Assigned Users and export the data to Sheets.
B. From the Admin Console Users Menu, download a list of all Users to Google Sheets, and join that with a list of ORGIDs pulled from the Reports API.
C. From the Google Workspace Reports Menu, run and download the Accounts Aggregate report, and export the data to Google Sheets.
D. From the Admin Console Users Menu, download a list of all user info columns and currently selected columns.

Correct Answer: D
Section:
Explanation:
Reference: https://support.google.com/a/answer/7348070?hl=en

QUESTION 7
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?

A. Use routing rules to dual-deliver mail to an on-premises SMTP server and Google Workspace.

B. Write a script and use Google Workspace APIs to access and download user data.
C. Use a third-party tool to configure secure backup of Google Workspace data.
D. Train users to use Google Takeout and store their archives locally.

Correct Answer: C
Section:

QUESTION 8
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's request? (Choose two.)

A. Review who has viewed files using the Google Drive Activity Dashboard.
B. Create an alert from Drive Audit reports to notify of external file sharing.
C. Review total external sharing in the Aggregate Reports section.
D. Create a custom Dashboard for external sharing in the Security Investigation Tool.
E. Automatically block external sharing using DLP rules.

Correct Answer: B, E
Section:

QUESTION 9
Your organization'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?

A. Configure a Google Group as an email list.
B. Delegate email access to department employees.
C. Configure a Google Group as a collaborative inbox.
D. Configure a Google Group, and set the Access Level to Announcement Only.

Correct Answer: D
Section:

QUESTION 10
Your employer, a media and entertainment company, wants to provision Google Workspace Enterprise accounts on your domain for several world-famous celebrities. Leadership is concerned with ensuring that these VIPs are afforded a high degree of privacy. Only a small group of senior employees must be able to look up contact information and initiate collaboration with the VIPs using Google Workspace services such as Docs, Chat, and Calendar. You are responsible for configuring to meet these requirements.
What should you do?

A. In the Users list, find the VIPs and turn off the User setting "Directory Sharing."
B. Create a Group for the VIPs and their handlers, and set the Group Access Level to Restricted.
C. In Directory Settings, disable Contact Sharing.
D. Create separate Custom Directories for the VIPs and regular employees.

Correct Answer: B
Section:

QUESTION 11
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've avoided since putting the 2FA+Hardware Keys in place last month.
Where do you find the information your CISO is interested in seeing?

A. Security > Advanced Security Settings > Phishing Attempts
B. Apps > Google Workspace > Gmail > Phishing Attempts
C. Security > Dashboard > Spam Filter: Phishing
D. Reporting > Reports > Phishing

Correct Answer: A
Section:

QUESTION 12
Your company has received help desk calls from users about a new interface in Gmail that they had not seen before. They determined that it was a new feature that Google released recently. In the future, you'll need time to review the new features so you can properly train employees before they see changes.
What action should you take?

A. Company Profile > Profile > New User Features > Enable "Scheduled Release"
B. Apps > Google Workspace > Gmail > Uncheck "Enable Gmail Labs for my users"
C. Company Profile > Profile > New User Features > Enable "Rapid Release"
D. Device Management > Chrome > Device Settings > Stop auto-updates

Correct Answer: A
Section:

QUESTION 13
Your company frequently hires from five to ten interns for short contract engagements and makes use of the same generically named Google Workspace accounts (e.g., user1@your-company.com, user2@your-company.com, user3@yourcompany.com). The manager of this program wants all email to these accounts routed to the manager's mailbox account also.
What should you do?

A. Setup address forwarding in each account's GMail setting menu.
B. Set up recipient address mapping in GMail Advanced Settings.
C. Configure an Inbound Gateway route.
D. Give the manager delegated access to the mailboxes.

Correct Answer: C
Section:
Explanation:
Reference: https://support.google.com/a/answer/2685650?hl=en

QUESTION 14
Your company has sales offices in Madrid, Tokyo, London, and New York. The outbound email for those offices needs to include the sales person's signature and a compliance footer. The compliance footer needs to say "Should you no longer wish to receive emails about this offer, please reply with UNSUBSCRIBE."
You are responsible for making sure that users cannot remove the footer.
What should you do?

A. Send an email to each sales person with the instructions on how to add the footer to their Signature.

B. Ensure that each sales team is in their own OU, and configure the Append Footer with the signature and footer content translated for each locale.
C. Ensure that each sales team is in their own OU, and configure the Append Footer with footer content.
D. Ensure that each sales team is in their own OU, and configure the Append Footer with the footer content translated for each locale.

Correct Answer: D
Section:

QUESTION 15
What action should be taken to configure alerting related to phishing attacks?

A. Set up a Token audit log event alert.
B. Set up an Admin audit log event alert.
C. Set up an email settings changed alert.
D. Set up a suspicious login event alert.

Correct Answer: D
Section:
Explanation:
Reference: https://support.google.com/a/answer/9104586?hl=en

QUESTION 16
A company using Google Workspace has reports of cyber criminals trying to steal usernames and passwords to access critical business data. You need to protect the highly sensitive user accounts from unauthorized access. What should you do?

A. Turn on password expiration.
B. Enforce 2FA with a physical security key.
C. Use a third-party identity provider.
D. Enforce 2FA with Google Authenticator app.

Correct Answer: D
Section:
Explanation:
Reference: https://support.google.com/a/answer/175197?hl=en

QUESTION 17
After migrating to Google Workspace, your legal team requests access to search all email and create litigation holds for employees who are involved with active litigation. You need to help the legal team meet this request. What should you do?

A. Add the legal team to the User Management Admin system role.
B. Add the legal team to the Google Vault Google Group.
C. Create a custom role with Google Vault access, and add the legal team.
D. Create a matter in Google Vault, and share with the legal team.

Correct Answer: C
Section:
Explanation:
Reference: https://gsuite.google.com/products/vault/

QUESTION 18
Your company's compliance officer has requested that you apply a content compliance rule that will reject all external outbound email that has any occurrence of credit card numbers and your company's account number syntax, which is AccNo. You need to configure a content compliance rule to scan email to meet these requirements.
Which combination of attributes will meet this objective?

A. Name the rule > select Outbound and Internal Sending > select If ANY of the following match > add two expressions: one for Simple Content Match to find AccNo, and one for predefined content match to select Credit Card Numbers >choose Reject.
B. Name the rule > select Outbound > select If ANY of the following match > add two expressions: one for Simple Content Match to find AccNo, and one for predefined content match to select Credit Card Numbers > choose Reject
C. Name the rule > select Outbound and Internal Sending > select If ALL of the following match > add two expressions: one for Advanced Content Match to find AccNo in the Body, and one for predefined content match to select Credit CardNumbers > choose Reject.
D. Name the rule > select Outbound > select If ALL of the following match > add two expressions: one for Advanced Content Match to find AccNo in the Body, and one for predefined content match to select Credit Card Numbers > chooseReject.

Correct Answer: D
Section:

QUESTION 19
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.)

A. Apps > add SAML apps to your domain.
B. Reconfigure user provisioning via Google Cloud Directory Sync.
C. Replace the third-party IDP verification certificate.
D. Disable SSO with third party IDP.
E. Enable API Permissions for Google Cloud Platform.

Correct Answer: A, C
Section:
Explanation:
Reference: https://support.google.com/a/answer/60224?hl=en

QUESTION 20
On which two platforms can you push WiFi connection information with Google Workspace? (Choose two.)

A. Mac OS
B. Windows
C. Chrome OS
D. iOS
E. Linux

Correct Answer: C, D
Section:
Explanation:
Reference: https://support.google.com/a/answer/2634553?hl=en

QUESTION 21
Your-company.com recently bought 2500 Chrome devices and wants to distribute them to various teams globally. You decided that enterprise enrollment would be the best way to enforce company policies for managed Chrome devices. You discovered that Chrome devices currently end up in the top-level organization unit, and this needs to change to the organizational unit of the device administrator.
What should you do?

A. Change Enrollment Permissions to only allow users in this organization to re-enroll existing devices.
B. Change Enrollment Controls to Place Chrome device in user organization.
C. Change Enrollment Controls to Keep Chrome device in current location.
D. Change Enrolment Permissions to not allow users in this organization to enroll new devices.

Correct Answer: A
Section:

QUESTION 22
A user has traveled overseas for an extended trip to meet with several vendors. The user has reported that important draft emails have not been saved in Gmail, which is affecting their productivity. They have been constantly moving between hotels, vendor offices, and airport lounges.
You have been tasked with troubleshooting the issue remotely. Your first priority is diagnosing and preventing this from happening again, and your second priority is recovering the drafts if possible. Due to time zone differences, and the user's busy meeting schedule, you have only been able to arrange a brief Hangouts Meet with the user to gather any required troubleshooting inputs. What two actions should be taken on this call with the user? (Choose two.)

A. Ask the user to send an email to you so you can check the headers.
B. Record a HAR file of the user composing a new email.
C. Take screenshots of the user's screen when composing an email.
D. Use the Email log search in the Admin panel.
E. Check the Users > App Users Activity report.

Correct Answer: C, E
Section:

QUESTION 23
Your company recently migrated to Google Workspace and wants to deploy a commonly used third-party app to all of finance. Your OU structure in Google Workspace is broken down by department. You need to ensure that the correct users get this app.
What should you do?

A. For the Finance OU, enable the third-party app in SAML apps.
B. For the Finance OU, enable the third-party app in Marketplace Apps.
C. At the root level, disable the third-party app. For the Finance OU, allow users to install any application from the Google Workspace Marketplace.
D. At the root level, disable the third-party app. For the Finance OU, allow users to install only whitelisted apps from the Google Workspace Marketplace.

Correct Answer: B
Section:
Explanation:
Reference: https://support.google.com/a/answer/6089179?hl=en

QUESTION 24
The CEO of your company has indicated that messages from trusted contacts are being delivered to spam, and it is significantly affecting their work. The messages from these contacts have not always been classified as spam. Additionally, you recently configured SPF, DKIM, and DMARC for your domain. You have been tasked with troubleshooting the issue.
What two actions should you take? (Choose two.)

A. Obtain the message header and analyze using Google Workspace Toolbox.
B. Review the contents of the messages in Google Vault.
C. Set up a Gmail routing rule to whitelist the sender.
D. Conduct an Email log search to trace the message route.
E. Validate that your domain is not on the Spamhaus blacklist.

Correct Answer: A, C
Section:

QUESTION 25
Security and Compliance has identified that data is being leaked through a third-party application connected to Google Workspaceю You want to investigate using an audit log.
What log should you use?

A. Admin audit log
B. SAML audit log
C. Drive usage audit log
D. OAuth Token audit log

Correct Answer: D
Section:
Explanation:
Reference: https://support.google.com/a/answer/6124308?hl=en

QUESTION 26
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
Section:

QUESTION 27
A company wants to distribute iOS devices to only the employees in the Sales OU. They want to be able to do the following on these devices:
Control password policies.
Make corporate apps available to the users.
Remotely wipe the device if it's lost or compromised
What two steps are required before configuring the device policies? (Choose two.)

A. Turn on Advanced Mobile Management for the domain.
B. Turn on Advanced Mobile Management for Sales OU
C. Set up Device Approvals.

D. Set up an Apple Push Certificate.
E. Deploy Apple Certificate to every device.

Correct Answer: A, C
Section:

QUESTION 28
Your client is a 5,000-employee company with a high turn-over rate that requires them to add and suspend user accounts. When new employees are onboarded, a user object is created in Active Directory. They have determined that manually creating the users in Google Workspace Admin Panel is time-consuming and prone to error. You need to work with the client to identify a method of creating new users that will reduce time and error.
What should you do?

A. Install Google Cloud Directory Sync on all Domain Controllers.
B. Install Google Workspace Sync for Microsoft Outlook on all employees' computers.
C. Install Google Cloud Directory Sync on a supported server.
D. Install Google Apps Manager to automate add-user scripts.

Correct Answer: A
Section:

QUESTION 29
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?

A. Randomly scatter auto-updates.
B. Update over cellular.
C. Disable Auto update.
D. Throttle the bandwidth.

Correct Answer: A
Section:
Explanation:
Reference: https://support.google.com/chrome/a/answer/3168106?hl=en

QUESTION 30
Your company moved to Google Workspace last month and wants to install Hangouts Meet Hardware in all of their conference rooms. This will allow employees to walk into a room and use the in-room hardware to easily join their scheduled meeting. A distributed training session is coming up, and the facilitator wants to make remote room joining even easier. Participants in remote rooms should walk into their room and begin receiving the training without having to take any actions to join the session.
How should you accomplish this?

A. In the Admin Console, select the devices in Meeting Room Hardware, select Call, and Enter the meeting code.
B. Room participants will need to start the meeting from the remote in the room.
C. By adding the rooms to the Calendar invite, they will all auto-join at the scheduled time.
D. Select Add Live Stream to the Calendar invite; all rooms added to the event will auto-join at the scheduled time.

Correct Answer: D
Section:

QUESTION 31
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: A
Section:

QUESTION 32
You have configured your Google Workspace account on the scheduled release track to provide additional time to prepare for new product releases and determine how they will impact your users. There are some new features on the latest roadmap that your director needs you to test as soon as they become generally available without changing the release track for the entire organization.
What should you do?

A. Create a new OU and tum on the rapid release track just for this OU.
B. Create a new Google Group with test users and enable the rapid release track.
C. Establish a separate Dev environment, and set it to rapid release.
D. Ask Google for a demo account with beta access to the new features.

Correct Answer: A
Section:
Explanation:
Reference: https://support.google.com/a/answer/172177?hl=en

QUESTION 33
You are using Google Cloud Directory Sync to manage users. You performed an initial sync of nearly 1,000 mailing lists to Google Groups with Google Cloud Directory Sync and now are planning to manage groups directly from Google. Over half the groups have been configured with incorrect settings, including who can post, who can join, and which groups can have external members. You need to update groups to be configured correctly.
What should you do?

A. Use the bulk upload with CSV feature in the Google Workspace Admin panel to update all Groups.
B. Update your configuration file and resync mailing lists with Google Cloud Directory Sync.
C. Create and assign a custom admin role for all group owners so they can update settings.
D. Use the Groups Settings API to update Google Groups with desired settings.

Correct Answer: A
Section:

QUESTION 34
Your client is a multinational company with a single email domain. The client has compliance requirements and policies that vary by country. You need to configure the environment so that each country has their own administrator and no administrator can manage another country.
What should you do?

A. Establish a new GSuite tenant with their own admin for each region.

B. Create an OU for each country. Create an admin role and assign an admin with that role per OU.
C. Create Admin Alerts, and use the Security Center to audit whether admins manage countries other than their own.
D. Create a Team Drive per OU, and allow only country-specific administration of each folder.

Correct Answer: B
Section:

QUESTION 35
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'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?

A. Export log data to BigQuery with custom scopes.
B. Use a third-party tool.
C. Use App Script and filter views within a Google Sheet.
D. Create an app using AppMaker and App Script.

Correct Answer: C
Section:

QUESTION 36
Your organization has been on Google Workspace Enterprise for one year. Recently, an admin turned on public link sharing for Drive files without permission from security. Your CTO wants to get better insight into changes that are made to the Google Workspace environment. The chief security officer wants that data brought into your existing SIEM system.
What are two ways you should accomplish this? (Choose two.)

A. Use the Data Export Tool to export admin audit data to your existing SIEM system
B. Use Apps Script and the Reports API to export admin audit data to your existing SIEM system.
C. Use Apps Script and the Reports API to export drive audit data to the existing SIEM system
D. Use the BigQuery export to send admin audit data to the existing SIEM system via custom code
E. Use the BigQuery export to send drive audit data to the existing SIEM system via custom code.

Correct Answer: C, E
Section:

QUESTION 37
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: D
Section:

QUESTION 38
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
Section:

QUESTION 39
Security and Compliance has identified secure third-party applications that should have access to Google Workspace data. You need to restrict third-party access to only approved applications
What two actions should you take? (Choose two.)

A. Whitelist Trusted Apps
B. Disable the Drive SDK
C. Restrict API scopes
D. Disable add-ons for Gmail
E. Whitelist Google Workspace Marketplace apps

Correct Answer: A, C
Section:

QUESTION 40
Your-company.com recently started using Google Workspace. The CIO is happy with the deployment, but received notifications that some employees have issues with consumer Google accounts (conflict accounts). You want to put a plan in place to address this concern. What should you do?

A. Use the conflict account remove tool to remove the accounts from Google Workspace.
B. Rename the accounts to temp@your-company.com, and recreate the accounts.
C. Ask users to request a new Google Workspace account from your local admin.
D. Use the Transfer tool for unmanaged users to find the conflict accounts.

Correct Answer: A
Section:

QUESTION 41
HR informs you that a user has been terminated and their account has been suspended. The user is part of a current legal investigation, and HR requires the user's email data to remain on hold. The terminated user's team is actively working on a critical project with files owned by the user. You need to ensure that the terminated user's content is appropriately kept before provisioning their license to a new user. What two actions should you take? (Choose two.)

A. Extend the legal hold on the user's email data.
B. Move project files to a Shared Drive or transfer ownership.
C. Rename the account to the new user starting next week.
D. Delete the account, freeing up a Google Workspace License.
E. Assign the terminated user account an Archive User license.

Correct Answer: A, E
Section:

QUESTION 42
The executive team for your company has an extended retention policy of two years in place so that they have access to email for a longer period of time. Your COO has found this useful in the past but when they went to find an email from last year to prove details of a contract in dispute, they were unable to find it. It is no longer in the Trash. They have requested that you recover it.
What should you do?

A. Using Vault, perform a search for the email and export the content to a standard format to provide for investigation.
B. Using the Gmail Audit log, perform a search for the email, export the results, then import with Google Workspace Migration for Microsoft Outlook.
C. Using the Message ID, contact Google Google Workspace support to recover the email, then import with Google Workspace Migration for Microsoft Outlook.
D. Using the Vault Audit log, perform a search for the email, export the results. then import with Google Workspace Migration for Microsoft Outlook.

Correct Answer: A
Section:

QUESTION 43
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
Section:

QUESTION 44
In the years prior to your organization moving to Google Workspace, it was relatively common practice for users to create consumer Google accounts with their corporate email address (for example, to monitor Analytics, manage AdSense, and collaborate in Docs with other partners who were on Google Workspace.) You were able to address active employees' use of consumer accounts during the rollout, and you are now concerned about blocking former employees who could potentially still have access to those services even though they don't have access to their corporate email account.
What should you do?

A. Contact Google Enterprise Support to provide a list of all accounts on your domain(s) that access non-Google Workspace Google services and have them blocked.
B. Use the Transfer Tool for Unmanaged Accounts to send requests to the former users to transfer their account to your domain as a managed account.
C. Provide a list of all active employees to the managers of your company's Analytics, AdSense, etc. accounts, so they can clean up the respective access control lists.
D. Provision former user accounts with Cloud Identity licenses, generate a new Google password, and place them in an OU with all Google Workspace and Other Google Services disabled.

Correct Answer: C

Section:

QUESTION 45
Your organization has implemented Single Sign-On (SSO) for the multiple cloud-based services it utilizes. During authentication, one service indicates that access to the SSO provider cannot be accessed due to invalid information.
What should you do?

A. Verify the NameID Element in the SAML Response matches the Assertion Consumer Service (ACS) URL.
B. Verify the Audience Element in the SAML Response matches the Assertion Consumer Service (ACS) URL.
C. Verify the Subject attribute in the SAML Response matches the Assertion Consumer Service (ACS) URL.
D. Verify the Recipient attribute in the SAML Response matches the Assertion Consumer Service (ACS) URL.

Correct Answer: B
Section:
Explanation:
Reference: https://auth0.com/docs/protocols/saml/saml-configuration/troubleshoot/auth0-as-sp

QUESTION 46
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?

A. Download the Google Workspace roadmap, and work together with a deployment specialist for new features.
B. Create a support ticket for the Google Workspace roadmap, and ask to enable the latest release of Google Workspace.
C. Subscribe to the Google Workspace release calendar, and Join the Google Cloud Connect Community.
D. Change Google Workspace release track to: Rapid Release for faster access to new features.

Correct Answer: C
Section:

QUESTION 47
Your company (your-company.com) just acquired a new business (new-company.com) that is running their email on-premises. It is close to their peak season, so any major changes need to be postponed. However, you need to ensure that the users at the new business can receive email addressed to them using your-company.com into their on-premises email server. You need to set up an email routing policy to accomplish this.
What steps should you take?

A. Set up an Outbound Mail Gateway to route all outbound email to the on-premises server.
B. Set up accounts for the new employees, and use mail forwarding rules to send to the on-premises server.
C. Set up an Inbound Mail Gateway to reroute all inbound email to the on-premises server.
D. Set up a Default route with split delivery to route email to the on-premises server.

Correct Answer: C
Section:

QUESTION 48
A user does not follow their usual sign-in pattern and signs in from an unusual location.
What type of alert is triggered by this event?

A. Suspicious mobile activity alert.

B. Suspicious login activity alert.
C. Leaked password alert.
D. User sign-in alert.

Correct Answer: B
Section:
Explanation:
Reference: https://support.google.com/a/answer/7102416?hl=en

QUESTION 49
Your large organization, 80,000 users, has been on Google for two years. Your CTO wants to create an integrated team experience with Google Groups, Teams Drives, and Calendar. Users will use a Google Form and Apps Script to request a new "G-Team." A "G-Team' is composed of a Google Group and a Team Drive/Secondary Calendar that is shared using that Google Group. What two design decisions are required to implement this workflow securely? (Choose two.)

A. The Apps Script will need to run as a Google Workspace admin.
B. You will need a Cloud SQL instance to store "G-Team' data.
C. The Google Form will need to be limited to internal users only.
D. The Apps Script will need to run on a timed interval to process new entries.
E. The Google Form will need to enforce Group naming conventions.

Correct Answer: C, D
Section:

QUESTION 50
The application development team has come to you requesting that a new, internal, domain-owned Google Workspace app be allowed to access Google Drive APIs. You are currently restricting access to all APIs using approved whitelists, per security policy. You need to grant access for this app.
What should you do?

A. Enable all API access for Google Drive.
B. Enable "trust domain owned apps" setting.
C. Add OAuth Client ID to Google Drive Trusted List.
D. Whitelist the app in the Google Workspace Marketplace.

Correct Answer: C
Section:

QUESTION 51
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.)

A. Change the password for suspected compromised account accounts.receivable@yourcompany.com.
B. Configure a Sender Policy Framework (SPF) record for your domain.
C. Configure Domain Keys Identified Mail (DKIM) to authenticate email.
D. Disable mail delegation for the accounts.receivable@yourcompany.com account.
E. Disable "Allow users to automatically forward incoming email to another address."

Correct Answer: A, C
Section:

QUESTION 52
Your organization has recently gone Google, but you are not syncing Groups yet. You plan to sync all of your Active Directory group objects to Google Groups with a single GCDS configuration.
Which scenario could require an alternative deployment strategy?

A. Some of your Active Directory groups have sensitive group membership.
B. Some of the Active Directory groups do not have owners.
C. Some of the Active Directory groups have members external to organization.
D. Some of the Active Directory groups do not have email addresses.

Correct Answer: C
Section:

QUESTION 53
Your company has just received a shipment of ten Chromebooks to be deployed across the company, four of which will be used by remote employees. In order to prepare them for use, you need to register them in Google Workspace.
What should you do?

A. Turn on the Chromebook and press Ctrl+Alt+E at the login screen to begin enterprise enrollment.
B. In Chrome Management | Device Settings, enable Forced Re-enrollment for all devices.
C. Turn on the chromebook and log in as a Chrome Device admin. Press Ctrl+Alt+E to begin enterprise enrollment.
D. Instruct the employees to log in to the Chromebook. Upon login, the auto enrollment process will begin.

Correct Answer: A
Section:
Explanation:
Reference: https://support.google.com/chrome/a/answer/4600997?hl=en

QUESTION 54
All Human Resources employees at your company are members of the "HR Department" Team Drive. The HR Director wants to enact a new policy to restrict access to the "Employee Compensation" subfolder stored on that Team Drive to a small subset of the team.
What should you do?

A. Use the Drive API to modify the permissions of the Employee Compensation subfolder.
B. Use the Drive API to modify the permissions of the individual files contained within the subfolder.
C. Move the contents of the subfolder to a new Team Drive with only the relevant team members.
D. Move the subfolder to the HR Director's MyDrive and share it with the relevant team members.

Correct Answer: B
Section:

QUESTION 55
Your company policy requires that managers be provided access to Drive data once an employee leaves the company.
How should you grant this access?

A. Make the manager a delegate to the former employee's account.

B. Copy the data from the former employee's My Drive to the manager's My Drive.
C. Transfer ownership of all Drive data using the file transfer ownership tool in the Google Workspace Admin console.
D. Login as the user and add the manager to the file permissions using the "Is owner' privilege for all Drive files.

Correct Answer: C
Section: