Number: GOOGLE WORKSPACE ADMINISTRATOR
Passing Score: 800.0
Time Limit: 120.0
File Version: 12.0

Exam Code: GOOGLE WORKSPACE ADMINISTRATOR
Exam Name: GOOGLE WORKSPACE ADMINISTRATOR

Exam A

QUESTION 1
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:
Explanation:
Subscribe to the Google Workspace Release Calendar:
Go to the Google Workspace Updates blog at https://workspaceupdates.googleblog.com/.
Click on 'Subscribe to updates' to get real-time notifications about new features, updates, and changes in Google Workspace.
This will ensure you and your team are informed about the latest security and collaboration features as they are announced.
Join the Google Cloud Connect Community:
Visit the Google Cloud Connect Community at https://cloudconnectcommunity.google/.
Join the community to engage with other Google Workspace administrators and users.
Participate in discussions, ask questions, and stay informed about best practices, upcoming features, and insights directly from Google Workspace experts and peers.
Google Workspace Updates Blog
Google Cloud Connect Community

QUESTION 2
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: D
Section:
Explanation:
Access the Admin Console:
Log in to the Google Workspace Admin console at https://admin.google.com/.
Configure Email Routing:
Navigate to 'Apps' > 'Google Workspace' > 'Gmail' > 'Default routing'.
Set Up Split Delivery:
Create a new default routing rule.
Under 'Add setting,' click on 'Routing.'

In the 'Add setting' box, under 'Inbound,' select 'Configure' next to 'Routing.'
Under 'Add setting,' name your routing policy.
In the 'Email messages to affect' section, specify the conditions for the rule (e.g., recipients in the new-company.com domain).
Route to On-Premises Server:
In the 'Route' section, select 'Modify message' > 'Add more recipients.'
Enter the on-premises email server information (e.g., SMTP relay server) to forward emails to the on-premises server.
Save the rule and ensure it is active.
Test the Configuration:
Send test emails to ensure that emails are correctly routed to the on-premises server as per the split delivery setup.
Monitor the email flow and make adjustments if necessary to ensure smooth operation during the peak season.
Google Workspace Admin Help: Set up routing for your domain or organization
Google Workspace Admin Help: Configure routing for mail in Google Workspace

QUESTION 3
Recently your organization has had an increase in messages marked as spam You need to quickly and efficiently obtain detailed information regarding each message What should you do?

A. Create an investigation by using a SQL query to search for all spam audit logs exported to BigQuery
B. Send an alert to all users to mark all suspicious Gmail messages as spam and review the Alert center messages
C. Use Google Vault to put all messages marked as spam in a legal hold and review the messages
D. Use the spam filter report in the security dashboard to see messages Google's spam filter marked as spam during a specific time period

Correct Answer: D
Section:
Explanation:
Access Security Dashboard: Go to the Google Admin console and navigate to the 'Security' section.
Open Spam Filter Report: In the security dashboard, open the spam filter report.
Filter by Time Period: Select the specific time period you want to analyze.
Review Spam Messages: Review the detailed information regarding each message marked as spam by Google's spam filter.
Take Necessary Actions: Use the information from the report to adjust spam filters, user alerts, or take other necessary actions to manage spam more effectively.
Security Dashboard
Email Log Search

QUESTION 4
You work for a midsize organization Your compliance and audit learn sees that users are frequently resetting their passwords You must provide accurate information and ensure that the compliance team is informed every time a user changes their password What should you do?

A. Create a new alert by using user log events and check that event Login type is Google password and include the compliance team in the email notifications
B. Check the User's password changed alert in the alert center and include the compliance team in the email notifications
C. Disable user account recovery so users must contact you before a reset
D. Enable user account recovery and forward any alert to the compliance team through the alert center

Correct Answer: B
Section:
Explanation:
Step by Step Comprehensive Detailed Explanation:
Access the Admin Console: Sign in to your Google Admin console.
Navigate to the Alert Center: Click on 'Security' and then 'Alert Center.'
Create New Alert: In the Alert Center, click on 'Manage alerts' and then 'Add alert rule.'
Configure Alert Rule: Select 'User's password changed' as the event type.

Include Compliance Team: In the alert configuration, add the compliance team's email addresses to the notification recipients.
Save the Alert: Save the configuration to ensure the compliance team is informed every time a user changes their password.
Google Workspace Admin Help: Alert Center

QUESTION 5
Your global marketing team has over 500 employees. They recently started working with Google Analytics and want to move to managed accounts You decide to use Google Cloud Directory Sync (GCDS) to sync users from your current identity provider Your organization currently has no Google Workspace licenses linked to the Admin console You run GCDS for the first lime and receive the following error. 'Domain user limit reached ' You need to identify and fix the problem What should you do?

A. Ensure that there is a subscription available and enough licenses to sync the new users
B. Check if GCDS has the correct permissions to run a sync on your domain
C. Wait 48 hours until the domain is fully provisioned
D. Update the delete limits of GCDS and try again

Correct Answer: A
Section:
Explanation:
Verify License Availability: Check the number of available licenses in your Google Workspace subscription.
Purchase Additional Licenses: If necessary, purchase additional licenses to cover the number of users you plan to sync.
Configure GCDS: Ensure that Google Cloud Directory Sync (GCDS) is properly configured to sync users from your identity provider.
Run GCDS: Run the GCDS sync again to sync the new users now that sufficient licenses are available.
Google Cloud Directory Sync Admin Help

QUESTION 6
Your organization has users in the United States and Europe For compliance reasons you want to ensure that user data is always stored in the region where the user is located What should you do?

A. Create two Google Groups titled 'United States' and 'Europe ' Assign users to either group based on location
B. Specify a data region policy for each Organizational Unit (OU) where users are grouped by location
C. Populate the Address field on each user record ensuring the country information is accurate
D. Do nothing No extra configuration is needed because user data is always stored in the region the user is located

Correct Answer: B
Section:
Explanation:
Step by Step Comprehensive Detailed Explanation:
Access the Admin Console: Sign in to your Google Admin console.
Navigate to Data Regions: Click on 'Account' and then 'Data Regions.'
Create Data Region Policy: Create a data region policy specifying where data should be stored.
Apply to OUs: Apply the data region policy to the organizational units (OUs) based on user location, ensuring data is stored in the respective regions.
Save Configuration: Save the settings to enforce the data region policies.
Google Workspace Admin Help: Data Regions

QUESTION 7
Several users in your organization reported an issue with receiving emails from one particular external sender You want to troubleshoot the issue and determine whether Google received these emails What should you do?

A. Check if your Google Workspace domain registration expired
B. Search for missing email messages by using email Log Search {ELS) and determine why messages weren't delivered
C. Update your MX records to make sure they point to Google mail servers

D. Open a support ticket with Google Workspace Support

Correct Answer: B
Section:
Explanation:
Step by Step Comprehensive Detailed Explanation:
Access Email Log Search: Sign in to the Google Admin console and navigate to 'Reports' then 'Audit' and select 'Email Log Search.'
Perform a Search: Enter the details of the external sender and the date range to search for the missing emails.
Analyze Results: Review the search results to see if the emails were received, bounced, or filtered.
Determine Cause: Identify any issues such as delivery errors or spam filtering that might have affected the emails.
Google Workspace Admin Help: Email Log Search

QUESTION 8
You are configuring a customer relationship management (CRM) solution to integrate with Google Workspace services for the sales department at your organization The CRM solution is in the Google Workspace Marketplace and you deploy the specific CRM solution Employees report that there are no contacts and documents visible in the CRM solution You must identify and fix the problem What should you do?

A. Check the OAuth scopes and ensure that Drive and Gmail scopes are granted for the CRM solution
B. Check if Manage access to apps is set to Allow users to install and run any app from the Marketplace
C. Revoke all OAuth scopes and reinstall the CRM solution for just the sales department.
D. Check if the App distribution settings are set to ON for everyone in your organization

Correct Answer: A
Section:
Explanation:
Access the Admin Console: Sign in to your Google Admin console.
Navigate to Security Settings: Click on 'Security' and then 'API controls.'
Manage Third-Party App Access: Click on 'Manage third-party app access.'
Check OAuth Scopes: Locate the CRM solution and ensure that it has the necessary OAuth scopes, particularly for Google Drive and Gmail.
Grant Access: If necessary, adjust the settings to grant the required scopes.
Verify Integration: Confirm that the CRM solution now has access to the necessary data and that employees can see contacts and documents.
Google Workspace Admin Help: Manage third-party app access

QUESTION 9
You have implemented a data loss prevention (DLP) policy for a specific finance organizational unit. You want to apply the same security policy to a shared drive owned by the finance department in the most efficient manner. What should you do?

A. In the Admin console sharing settings, select the finance organizational unit and deselect Allow users outside the domain to access files in shared drives
B. Assign the Shared Drive to the finance organizational unit
C. Create a new DLP policy for shared drive users
D. Change the scope of the policy to apply to all in the domain

Correct Answer: C
Section:
Explanation:
Access the Admin Console: Sign in to your Google Admin console.
Navigate to DLP Settings: Click on 'Security' and then 'Data protection' to access Data Loss Prevention (DLP) settings.
Create New DLP Policy: Click on 'Create policy' and configure the policy specifically for shared drive data.
Define Rules: Set up the necessary rules and conditions to match the existing DLP policy for the finance organizational unit.
Apply to Shared Drive: Apply this new policy to the shared drive used by the finance department.

Save and Activate: Save the policy and ensure it is active and enforced for the shared drive.
Google Workspace Admin Help: Set up and manage DLP

QUESTION 10
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:
Identify Suspicious Login Activity:
Google Workspace triggers a suspicious login activity alert when a user signs in from an unusual location or device that is not part of their regular sign-in pattern.
Review Alerts:
Go to the Google Workspace Admin console.
Navigate to 'Security' > 'Dashboard' > 'Suspicious login activity'.
Review the details of the alert to determine the nature of the suspicious login.
Take Appropriate Actions:
Investigate the alert to ensure that the login attempt is legitimate.
If the login is deemed suspicious, follow security protocols to secure the user account, such as resetting the password or enabling two-factor authentication.
Google Workspace Admin Help: Review security alerts

QUESTION 11
You are the administrator of a domain that requires iOS mobile device management. What initial steps should be taken to ensure that you can properly manage end-user iOS devices?

A. Follow the prompts under 'company owned devices,' and select 'iOS Management.' Select the option to 'enforce management on iOS devices.'
B. Configure an Apple Push Certificate, and select 'certificate never expires.'
C. Configure an Apple Push Certificate, and be sure to use a work address that can be accessed in the future.
D. In the Admin console, navigate to iOS management, and enable the Apple Push Certificate connector.

Correct Answer: C
Section:
Explanation:
To ensure proper management of iOS devices, follow these steps:
Sign in to the Google Admin console: Use an account with super administrator privileges.
Navigate to Device Management: Go to Devices > Mobile and endpoints > Settings > iOS settings.
Configure Apple Push Certificate:
Click on 'Apple Push Certificate.'
Follow the instructions to create and upload an Apple Push Certificate. Ensure that you use a work email address that will be accessible in the future for renewal purposes.
Enable iOS Management:
Once the Apple Push Certificate is configured, enable iOS device management.
Optionally, enforce management on iOS devices to ensure all devices are compliant.
Google Workspace Admin Help - Set up Apple Push Certificate
Google Workspace Admin Help - Manage iOS devices

QUESTION 12
Your executive team has asked you to export all available data for 1,200 of your 1,500 Google Workspace Domain users. How should you proceed to export the data with the least amount of effort?

A. Perform a search in Google Vault for the 500 users and export all of the results.
B. Create a shared drive for the exports. Instruct end users to manually use Google Takeout to export the data and place the exported files in the shared drive.
C. Contact Google Cloud support to perform the export for you.
D. Contact Google Cloud Support to enable the Data Export tool for your organization, because you have more than 1,000 users, then use the tool to export data for the domain, and remove any unnecessary user data.

Correct Answer: D
Section:
Explanation:
To export data for a large number of users efficiently, follow these steps:
Contact Google Cloud Support: Since your organization has more than 1,000 users, you need to request access to the Data Export tool. This tool is not automatically available for large domains.
Enable the Data Export tool: Google Cloud Support will enable the tool for your organization.
Use the Data Export tool:
Once enabled, sign in to the Google Admin console with super administrator privileges.
Navigate to the Data Export tool under Tools.
Initiate the export process, selecting the data for the 1,200 users.
Manage the exported data: After the export is complete, review the data and remove any unnecessary user data to streamline the results.
Google Workspace Admin Help - Data Export
Google Workspace Admin Help - Contact support

QUESTION 13
Your organization has been using Google Workspace for almost a year, and your annual security and risk assessment initiative is approaching in preparation for the risk assessment you want to quickly review all the security-related settings for Gmail, Drive and Calendar and identify the ones that may be posing risk What should you do?

A. Review all the alerts in the Alert center
B. Review the Security health page in the Admin console
C. Review all settings for each organizational unit (OU) separately because it is the only way to see the security settings tor Workspace apps
D. Review the Gmail Drive, and Calendar reports in the Reporting section in the Admin console.

Correct Answer: B
Section:
Explanation:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Navigate to Security Health Page: In the Admin console, go to the Security section and select Security health. This page provides a comprehensive overview of your organization's security settings.
Review Security Settings: The Security health page lists various security settings for Gmail, Drive, and Calendar. It highlights settings that might pose a risk and provides recommendations for improvement.
Identify and Mitigate Risks: Carefully review the highlighted settings. Follow the recommendations to enhance your organization's security posture. This ensures that any potential risks are identified and mitigated promptly.
Google Workspace Admin Help: Security health
Google Workspace Security Best Practices

QUESTION 14
Your organization has a data loss prevention (DLP) rule to detect and warn users about external sharing of sensitive files in Google Drive You also want to prevent external users from downloading files with viewer permissions to their local machines What should you do?

A. Do nothing. View-only Drive files automatically prevent the user from downloading the files
B. Modify the existing DLP rule to Disable download, print, and copy for commenters and viewers
C. Create a new DLP rule by using the existing content detector conditions but change the action for the new rule to Disable download. print, and copy for commenters and viewers

D. Create a new DLP rule and set the scope to the organizational unit or group that you want to restrict

Correct Answer: C
Section:
Explanation:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Navigate to DLP Rules: Go to Apps > Google Workspace > Drive and Docs > Data loss prevention.
Create a New Rule: Click on Create a rule and choose to start with a template or create a custom rule.
Set Content Detector Conditions: Use the existing content detector conditions that identify sensitive files.
Configure Actions: Set the action to Disable download, print, and copy for commenters and viewers. This ensures that external users with viewer permissions cannot download the files.
Apply Rule to Relevant OUs/Groups: Set the scope of the rule to the specific organizational units or groups where you want this restriction to apply.
Save and Implement: Save the rule and ensure it is activated. This will enforce the new restrictions for sensitive files shared externally.
Google Workspace Admin Help: Data loss prevention for Drive
Google Workspace DLP Best Practices

QUESTION 15
Your organization wants to grant Google Vault access to an external regulatory authority. In an effort to comply with an investigation, the external group needs the ability to view reports in Google Vault. What should you do?

A. Create accounts for external users and assign Vault privileges.
B. Share Vault access with external users.
C. Assign an Archived User license to the external users.
D. Temporarily assign the super admin role to the users

Correct Answer: A
Section:
Explanation:
Create External Accounts: In the Google Admin console, create new Google Workspace accounts for the external regulatory authority members.
Assign Vault Privileges: Navigate to the Admin roles and assign the necessary Google Vault privileges to these accounts, ensuring they have the access needed to view reports and data for the investigation.
Configure Security Settings: Ensure that the external users have secure access, potentially with additional security measures such as two-factor authentication.
Monitor Access: Regularly audit and monitor the activity of the external users to ensure compliance with your organization's data policies and security requirements.
Revoke Access When Done: Once the investigation is complete, promptly revoke access to ensure continued security of your data.
Google Vault Help - Assign Vault Privileges
Google Workspace Admin Help - Add Users

QUESTION 16
Your organization recently bought 1.000 licenses for Cloud Identity Premium. The company's development team created an application in the enterprise service bus (ESB) that will read user data in the human resources information system (HRIS) and create accounts via the Google Directory REST API.
While doing the original test before production use, the team observes a 503 error coming from Google API response after a few users are created The team believes the ESB is not the cause, because it can perform 100 requests per second without any problems. What advice would you give the development team in order to avoid the issue?

A. Use the domain-wide delegation API to avoid the limitation per account.
B. Use an exponential back-off algorithm to retry failed requests.
C. Switch from REST API to gRPC protocol for performance improvement
D. Use the batch request architecture, because it can pack 1,000 API calls in one HTTP request.

Correct Answer: B
Section:
Explanation:
Understand the Error:

A 503 error indicates that the service is unavailable, often due to temporary overloading or maintenance of the server.
This can happen when API rate limits are exceeded.
Exponential Back-Off Algorithm:
This algorithm helps manage retries after a request fails, by exponentially increasing the waiting time between retries.
Start with a short delay and increase it exponentially with each subsequent retry.
Implementation:
Modify the ESB application to include the exponential back-off algorithm.
Ensure that the retries are limited to a reasonable number to avoid indefinite looping.
This approach will help mitigate the temporary overloads by spreading out the request attempts.
Google Workspace Admin Help: Handle API Errors
Google Developers: Exponential Backoff

QUESTION 17
You want to create a list of IP addresses that are approved to send email to your domain. To accomplish this, what section of the Google Workspace Admin console should you update?

A. Bypass spam filter
B. Content compliance rule
C. Approved email denylist
D. Email allowlist

Correct Answer: D
Section:
Explanation:
Access Email Allowlist Settings:
Navigate to the Google Admin console.
Go to Apps > Google Workspace > Gmail > Spam, Phishing, and Malware.
Update Allowlist:
In the Spam section, find the 'Email allowlist' option.
Add the IP addresses that are approved to send email to your domain.
Save Changes:
Save the settings to ensure the allowlist is updated.
This configuration will allow emails from the specified IP addresses to bypass spam filters and be delivered to your domain.
Google Workspace Admin Help: Configure Email Allowlists

QUESTION 18
The compliance team at your organization is conducting a legal investigation into some concerning sales activities of an employee eight months ago The compliance team contacted you for assistance on the situation You set up the default Google Vault retention rules so all data is retained only for one year You must assist the compliance team with the investigation What should you do1?

A. Do nothing The retention period has already ended and the evidence has already been purged
B. Suspend the employee and export all data by using Google Takeout
C. Assign the compliance team a Google Vault administrator role and create a legal hold for the employee
D. Assign the compliance team a Google Vault administrator role and change the default retention rules to three years.

Correct Answer: C
Section:
Explanation:
Assign Vault Administrator Role: In the Google Admin console, assign the compliance team members the Google Vault administrator role to give them the necessary permissions.
Access Google Vault: Have the compliance team access Google Vault.
Create a Matter: In Google Vault, create a new matter for the investigation.

Create a Hold: Within the matter, create a legal hold specifically targeting the employee's email and any other relevant data. This will preserve all the necessary information beyond the default retention period.
Review Data: The compliance team can now review the preserved data as part of their investigation.
Google Vault Help: Assign Vault privileges
Google Vault Help: Create and manage holds

QUESTION 19
Your team is collaborating on a new project by using a Google Doc They are using Doc comments to add numerous questions and suggestions You want to ensure that sensitive data in the Doc comments does not appear in the recipients' inboxes when a user is notified that a comment has been assigned to them What should you do?

A. Set up an email quarantine to quarantine all incoming emails that contain sensitive data
B. Disable comments in the Google Doc for your users
C. Create a Gmail content compliance rule and turn oft dynamic email for your team
D. Create a Gmail content compliance rule to block incoming messages that contain sensitive data

Correct Answer: C
Section:
Explanation:
Create a Content Compliance Rule:
Access the Google Admin console.
Go to Apps > Google Workspace > Gmail > Compliance.
Click on 'Add another rule' to create a new content compliance rule.
Define the conditions to detect sensitive data within email content.
Set actions to quarantine or reject emails that contain sensitive information.
Turn Off Dynamic Email:
In the Admin console, go to Apps > Google Workspace > Gmail > User settings.
Turn off dynamic email for your organization or specific organizational units.
Save and Apply:
Save the compliance rule and dynamic email settings.
These configurations ensure that sensitive data in Doc comments does not appear in recipient inboxes.
Google Workspace Admin Help: Set up content compliance
Google Workspace Admin Help: Turn dynamic email on or off

QUESTION 20
Your organization was recently targeted by a phishing attempt that affected several users You must efficiently determine the full extent of the phishing attempt and prevent further issues from occurring What should you do?

A. * 1 Search BigQuery 0Q9 Km b I message marked as phishing * 2 Require Transport Layer Security (TLS) for all email communications * 3 Instruct all users to reset their passwords
B. * 1 Use email log search to pull all emails for the past three days * 2 Analyze logs of common emails received and contact users. * 3 Instruct users on how to create a Gmail filter to block malicious email addresses
C. * 1 Use the security dashboard to view the number of messages showing evidence ot potential spoofing and then use the investigation tool on affected users to remove malicious email * 2 Enable advanced phishing and malware protection * 3 Deploy Google s Password Alert extension for Chrome
D. * 1 Collect phishing samples forwarded from users * 2 Add IP addresses and email addresses to your denylist * 3. Enroll only affected users to multi-factor authentication (MFA)

Correct Answer: C
Section:
Explanation:
Use the Security Dashboard:
Access the Google Admin console and go to Security > Dashboard.
Review metrics and logs for phishing and spoofing activities.
Identify affected users and potential threats.
Use the Investigation Tool:

From the Security dashboard, access the investigation tool.
Search for and isolate malicious emails sent to affected users.
Take action to remove these emails.
Enable Advanced Protection:
In the Admin console, go to Apps > Google Workspace > Gmail > Safety.
Enable advanced phishing and malware protection features.
Deploy Password Alert Extension:
Ensure the Password Alert Chrome extension is deployed across the organization to help detect password compromises.
Google Workspace Admin Help: Security dashboard
Google Workspace Admin Help: Investigation tool
Google Workspace Admin Help: Phishing and malware protection
Google Workspace Admin Help: Deploy Password Alert

QUESTION 21
Your organization has offices in Canada Italy and the United States You want to ensure that employees can access corporate Gmail and Drive from these three geographic locations only What should you do?

A. Require the use of corporate devices for any access to corporate Gmail and Drive
B. Use context-aware access to create access levels based on the geographic location and assign them to corporate Gmail and Drive
C. Create address lists to restrict the delivery of incoming and outgoing messages and to block notifications from Google Doc comments
D. Create data protection rules in Google Workspace that allow data access from only three geographic locations

Correct Answer: B
Section:
Explanation:
Enable Context-Aware Access:
In the Google Admin console, go to Security > Context-Aware Access.
Enable the context-aware access feature.
Create Access Levels:
Define access levels based on geographic locations (Canada, Italy, and the United States).
Use IP address ranges or other location indicators to specify these regions.
Assign Access Levels:
Assign the created access levels to the Google Workspace services, specifically corporate Gmail and Drive.
Ensure that only users accessing from the specified regions can access these services.
Apply and Monitor:
Save and apply the settings.
Monitor access logs to ensure compliance and security.
Google Workspace Admin Help: Set up context-aware access
Google Workspace Admin Help: Manage context-aware access levels

QUESTION 22
Your organization has upgraded to a Google Workspace edition with Vault and has hired a new audit team You are configuring access for this audit team with these privileges
* Chief legal executive - reporting privileges
* Legal audit manager - full Vault privileges
* Data reviewer - searching privileges
You must enable access for these three roles What should you do?

A. Set up Google Vault service as On for these specific users.
B. Assign Google Vault licenses to these users that allow all privileges required for access
C. Set up an Admin role with minimal Vault privileges and assign the rote to all Vault users Approve additional privileges that are requested through a formal approval process

D. Set up three different Admin roles with specific privileges that match the audit teams responsibilities Assign these Admin roles to the respective users.

Correct Answer: D
Section:
Explanation:
Navigate to Admin Roles: Go to the Google Admin console and navigate to the 'Admin roles' section.
Create Admin Roles: Create three separate admin roles:
Chief Legal Executive: Assign reporting privileges only.
Legal Audit Manager: Assign full Vault privileges.
Data Reviewer: Assign searching privileges.
Assign Roles to Users: Assign the created roles to the respective users (Chief Legal Executive, Legal Audit Manager, Data Reviewer).
Set Up Google Vault Access: Ensure the Google Vault service is turned on for these users by navigating to 'Apps' > 'Google Workspace' > 'Google Vault' and verifying that the service is enabled for their organizational unit.
Manage admin roles
Google Vault permissions

QUESTION 23
Employees at your organization frequently and mistakenly delete important emails that they receive from your payroll department The employees have to file support tickets for the IT team to find and restore these emails You must provide an automated solution that minimizes IT overhead and prevents these emails from being permanently deleted from their inboxes What should you do?

A. Create a content compliance rule that targets internal messages Use an advanced content match for the sender header to match the payroll department's email Quarantine the message so that administrators can review the email before they release it to the user
B. Create an Apps Script project that uses the Gmail API to find any recently deleted emails and automatically restore them to the inboxes Set the script trigger to be time-driven and run every hour
C. Create a content compliance rule that targets all internal messages that are sent from the payroll department Modify the message by prepending a custom subject line to all payroll emails so that employees know not to delete them
D. Create an activity rule by using Gmail log events with two conditions one for the event of an email deletion and another that matches the header address to the payroll department's email Create an action that restores messages Set the rule to run every hour

Correct Answer: D
Section:
Explanation:
Access Admin Console: Go to the Google Admin console and navigate to the 'Reports' section.
Activity Rule Setup: Select 'Manage Rules' and create a new rule.
Define Conditions:
Condition 1: Event equals 'Email Deletion'.
Condition 2: Header address matches the payroll department's email address.
Set Action: Define the action to restore the messages to the inbox.
Schedule the Rule: Set the rule to run every hour.
Test and Monitor: Ensure the rule is working as expected by monitoring the results and making adjustments if necessary.
Create and manage activity rules
Gmail API

QUESTION 24
You are the administrator for a 30.000-user organization. You have multiple Workspace licensing options available to end users in your domain, according to their work responsibilities. A user may be transitioned to a different license type multiple times in a given year. Your organization has a high turnover rate for employees. What is the most efficient way to manage your organization's licensing?

A. Use the Directory API to create a custom batch script that modifies the users license on a daily basis
B. Create a license assignment rule in the Google Admin console to set user licensing based on directory attributes.
C. Use Google Cloud Directory Sync to modify user licensing with each sync, according to information available in the organization's LDAP

D. Update user licensing in the user portion of the Admin console on an as-needed basis.

Correct Answer: B
Section:
Explanation:
To efficiently manage licensing in an organization with a high turnover rate and multiple license types, the best approach is to create a license assignment rule in the Google Admin console based on directory attributes. This method automates the process of assigning licenses according to the user's role and other directory attributes, ensuring that each user gets the appropriate license type without manual intervention. This approach is scalable and minimizes the administrative overhead associated with frequent changes in user roles and turnover.
Google Workspace Admin Help - Assign, change, or remove a user's license
Google Workspace Admin Help - Set up automated user provisioning to third-party applications

QUESTION 25
Your organization is planning to remove any dependencies on Active Directory (AD) from all Cloud applications they are using You are currently using Google Cloud Directory Sync (GCDS) with on-premises AD as a source to provision user accounts in Google Workspace. Your organization is also using a software-as-a-service (SaaS) human resources information system (HRIS) that offers integration via CSV export and Open API standard.
Additional requirements for the solution include:
* It should not require a subscription to any additional third-party service.
* The process must be automated from beginning to end.
You are tasked with the design and implementation of a solution to address user provisioning with these requirements.
What solution should you implement?

A. Set up Azure AD and federate on-premises AD with it. Provision user accounts from Azure AD with the Google-recommended process.
B. Modify the GCDS configuration to use the HRIS application as the data source and complete any necessary adjustments
C. Export HRIS data to a CSV file every day. and build a solution to define the delta with the previous day; import the result as a CSV file via the Admin console.
D. Build an application that will fetch updated data from the HRIS system via Open API. and then update Google Workspace with the Directory API accordingly.

Correct Answer: D
Section:
Explanation:
Given the requirements to eliminate dependencies on Active Directory, automate the process, and avoid third-party subscriptions, the best solution is to build an application that will fetch updated data from the HRIS system via its Open API. This application will then use the Directory API to update Google Workspace user accounts accordingly. This approach leverages existing tools (HRIS Open API and Google Directory API), ensures full automation from start to end, and does not require additional subscriptions.
Google Workspace Admin Help - Directory API
Google Workspace Admin Help - Google Cloud Directory Sync overview

QUESTION 26
Multiple users across the organization are experiencing video degradation in Meet video calls. As an administrator, what steps should you take to start troubleshooting?

A. Troubleshoot network bandwidth for the organizer of the meeting.
B. Push the Meet quality tool to end user devices and run local reports to determine connectivity issues.
C. Locate the Meet quality tool, and review the output for issues with quality.
D. Update the Admin Console Meet settings to disable streaming.

Correct Answer: C
Section:
Explanation:
To troubleshoot video degradation issues in Google Meet, the first step should be to locate the Meet Quality Tool and review the output for issues with quality. This tool provides detailed insights into the performance and quality of Meet calls, including network metrics, device performance, and user feedback. By analyzing this data, administrators can identify specific causes of degradation and take appropriate actions to resolve them.
Google Workspace Admin Help - Use the Google Meet quality tool

QUESTION 27
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 Google Workspace 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:
Explanation:
Create Organizational Units (OUs):
In the Google Workspace Admin console, go to 'Directory' > 'Organizational units'.
Create separate OUs for each country.
Assign Admin Roles:
Go to 'Admin roles' in the Admin console.
Create custom admin roles with permissions restricted to managing users, groups, and settings within their specific OU.
Ensure that the role does not grant permissions to manage other OUs.
Assign Country-Specific Admins:
Assign the newly created admin roles to the appropriate administrators, ensuring they have control only over their respective country's OU.
Google Workspace Admin Help: Create and manage organizational units
Google Workspace Admin Help: Admin roles

QUESTION 28
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:
Explanation:
Develop an App Script:
Write an App Script to retrieve user data from the Google Workspace directory, including license type and last login date.
Ensure the script filters data based on the team leader's direct reports.
Create a Google Sheet:
Set up a Google Sheet to display the retrieved data.

Use filter views to restrict the data visible to each team leader, showing only their direct reports.
Automate Data Refresh:
Schedule the App Script to run periodically (e.g., once a week) to ensure the data is up-to-date.
Share with Team Leaders:
Share the Google Sheet with team leaders, ensuring they have view-only access to the relevant filter views.
Google Workspace Admin Help: App Script
Google Workspace Admin Help: Filter views in Google Sheets

QUESTION 29
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: A, E
Section:
Explanation:
To ensure that the Context-Aware Access policy is working correctly, perform the following checks:
Confirm Google Workspace License:
Verify that the user has a Google Workspace Enterprise Plus license. Context-Aware Access is a feature available only to Enterprise Plus customers.
In the Admin console, navigate to Billing > Subscriptions and confirm the license type assigned to the user.
Check Endpoint Verification:
Ensure that Endpoint Verification is installed and active on users' desktops.
Go to the Admin console, navigate to Devices > Endpoint Verification.
Check the list of devices to confirm that Endpoint Verification is installed and reporting the status of users' devices.
Additional Steps:
Ensure that policies are correctly configured and applied to the relevant Organizational Units (OUs).
Verify that the Context-Aware Access policies are correctly set up in Security > Context-Aware Access.
By confirming the correct license and ensuring Endpoint Verification is installed, you can troubleshoot and resolve issues related to Context-Aware Access policy enforcement.
Set up Context-Aware Access
Endpoint Verification overview

QUESTION 30
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.

Correct Answer: D
Section:
Explanation:

Access Admin Console: Log into your Google Workspace Admin Console.
Navigate to Security Settings: Go to Security > Gmail > Safety.
Modify Spoofing Protection: Locate the spoofing protection settings.
Change Delivery Method: Change the setting from quarantining emails to delivering them to inboxes with a custom warning. This way, users can review the emails and determine if they are legitimate while still being alerted to potential issues.
Save Settings: Save the changes to apply the new delivery method.
Google Support: Protect against spoofing & identity deception

QUESTION 31
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: A
Section:
Explanation:
Access Admin Console: Log into your Google Workspace Admin Console.
Navigate to User Management: Go to Directory > Users.
Select the User: Find and select the temporary user account you need to delete.
Initiate Deletion Process: Click on the user to open the account details and select the option to delete the user.
Transfer Data: During the deletion process, you will see an option to transfer data. Select ''Transfer'' in the data in other apps section and enter the marketing manager's email address.
Complete Deletion: Complete the user deletion process. The user's Drive documents will be transferred to the marketing manager's account.
Google Support: Delete a user from your organization

QUESTION 32
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.

Correct Answer: A
Section:
Explanation:
Access Admin Console: Log into your Google Workspace Admin Console.
Navigate to Security Settings: Go to Security > API Controls.
Manage Third-Party App Access: Select 'App Access Control' and then click on 'Manage Third Party App Access'.
Review Authorized Apps: Here you will find a list of third-party apps that have been authorized to access your Google Workspace data.
Evaluate Access: Review the permissions and access scopes of each third-party app to determine if they should continue to have access or need to be restricted.
Google Support: Control which third-party & internal apps access Google Workspace data

QUESTION 33
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. Most Voted
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: A
Section:
Explanation:
Access Admin Console: Log into your Google Workspace Admin Console.
Navigate to Audit Logs: Go to Reports > Audit > Access Transparency Logs.
View Logs: In the Access Transparency Logs, you can see the actions performed by Google staff on your data.
Monitor Actions: Review the logs to understand the actions taken by Google support staff in relation to your support cases.
Google Support: Access Transparency

QUESTION 34
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: C
Section:
Explanation:
Access Admin Console: Log into your Google Workspace Admin Console.
Navigate to Security Settings: Go to Security > Gmail > Safety.
Enable Security Sandbox: Locate the 'Security Sandbox' setting and enable it. Security Sandbox provides an additional layer of protection by analyzing attachments for malware in a controlled environment before they reach users.
Save Settings: Save the changes to ensure the new protection layer is active.
Google Support: Gmail security sandbox

QUESTION 35
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
Section:
Explanation:
To audit if user1@example.com has shared any sensitive documents outside the organization, use the Security Investigation Tool in the Google Admin console. This tool allows administrators to investigate and take action on

security issues within the organization.
Open Security Investigation Tool:
Go to the Google Admin console.
Navigate to Security > Investigation tool.
Set Conditions in Drive Log Events:
In the Investigation Tool, select the data source as 'Drive Log Events'.
Add the following conditions:
Visibility Is External: This filters the events to show only documents that have been shared externally.
Actor Is user1@example.com: This specifies that the actions performed by the user1@example.com should be displayed.
Run the Investigation:
Click on ''Search'' to run the investigation with the specified conditions.
Review the results to identify any documents that have been shared externally by the user.
Remediate:
For any documents that were shared inappropriately, you can take corrective actions such as changing permissions or removing external sharing.
Security Investigation Tool
Audit Drive log events

QUESTION 36
A user is reporting that external, inbound messages from known senders are repeatedly being incorrectly classified as spam. What steps should the admin take to prevent this behavior in the future?

A. Modify the SPF record for your internal domain to include the IPs of the external user's mail servers.
B. Update the spam settings in the Admin Console to be less aggressive.
C. Add the sender's domain to an allowlist via approved senders in the Admin Console.
D. Instruct the user to add the senders to their contacts.

Correct Answer: C
Section:
Explanation:
To prevent external, inbound messages from known senders from being incorrectly classified as spam, add the sender's domain to an allowlist in the Admin console.
Access Gmail Settings in Admin Console:
Go to the Google Admin console.
Navigate to Apps > Google Workspace > Gmail > Spam, Phishing, and Malware.
Add Approved Senders:
In the Spam settings, find the section for ''Email whitelist'' or ''Approved senders''.
Click on ''Configure'' to add a new entry.
Specify the Sender's Domain:
Enter the domain of the external sender that needs to be allowed.
Save the changes to update the whitelist.
Verify and Monitor:
Ensure that the settings are applied and monitor the spam filter to confirm that the known sender's emails are no longer being flagged as spam.
By adding the sender's domain to an allowlist, you instruct the spam filter to accept emails from this domain, reducing false positives.
Prevent mail from being marked as spam
Approved sender list in Gmail

QUESTION 37
You are the Workspace administrator for an international organization with Enterprise Plus Workspace licensing. A third of your employees are located in the United States, another third in Europe, and the other third geographically dispersed around the world. European employees are required to have their data stored in Europe. The current OU structure for your organization is organized by business unit, with no attention to user location. How do you configure Workspace for the fastest end user experience while also ensuring that European user data is contained in Europe?

A. Configure a data region at the top level OU of your organization, and set the value to ''Europe''.
B. Add three additional OU structures to designate location within the current OU structure. Assign the corresponding data region to each.
C. Configure a configuration group for European users, and set the data region to ''Europe''.
D. Configure three configuration groups within your domain. Assign the appropriate data regions to each corresponding group, but assign no preference to the users outside of the United States and Europe.

Correct Answer: B
Section:
Explanation:
Assess Current OU Structure: Begin by evaluating the current organizational unit (OU) structure, which is organized by business unit.
Create Location-Based OUs: Add three additional OUs under the existing structure to categorize users based on their geographical location: United States, Europe, and Other Regions.
Assign Users to New OUs: Move users into the newly created location-based OUs according to their physical location.
Set Data Regions: Assign the appropriate data region for each new OU. For the European OU, set the data region to 'Europe' to ensure compliance with data residency requirements.
Validate Configuration: Ensure that the configuration is correctly implemented and verify that European user data is being stored in Europe.
Monitor Performance: Regularly monitor and optimize the system to ensure the fastest end-user experience globally.
Google Workspace Admin Help - Manage Data Regions
Google Workspace Admin Help - Organizational Units

QUESTION 38
As a team manager, you need to create a vacation calendar that your team members can use to share their time off. You want to use the calendar to visualize online status for team members, especially if multiple individuals are on vacation What should you do to create this calendar?

A. Request the creation of a calendar resource, configure the calendar to ''Auto-accept invitations that do not conflict,'' and give your team ''See all event details'' access.
B. Create a secondary calendar under your account, and give your team ''Make changes to events'' access.
C. Request the creation of a calendar resource, configure the calendar to ''Automatically add all invitations to this calendar,'' and give your team ''See only free/busy'' access.
D. Create a secondary calendar under your account, and give your team ''See only free/busy'' access

Correct Answer: B
Section:
Explanation:
Create Secondary Calendar: As the team manager, create a new calendar under your Google account specifically for tracking team vacations.
Access Settings: Go to the calendar settings and navigate to 'Share with specific people'.
Grant Access: Add your team members and give them 'Make changes to events' access, allowing them to add their vacation times directly to the calendar.
Educate Team: Inform team members on how to use this calendar to add their vacation times and check others' schedules.
Monitor Usage: Regularly review the calendar to ensure it is being used correctly and effectively by all team members.
Google Workspace Admin Help - Share a Calendar
Google Workspace Admin Help - Create a Team Calendar

QUESTION 39
Your Finance team has to share quarterly financial reports in Sheets with an external auditor. The external company is not a Workspace customer and allows employees to access public sites such as Gmail and Facebook. How can you provide the ability to securely share content to collaborators that do not have a Google Workspace or consumer (Gmail) account?

A. Allow external sharing with the auditor using the 'Trusted Domains' feature.
B. Enable the 'Visitor Sharing' feature, and demonstrate it to the Finance team.
C. Use the 'Publish' feature in the Sheets editor to share the contents externally.
D. Attach the Sheet file to an email message, and send to the external auditor.

Correct Answer: B
Section:

Explanation:
Enable Visitor Sharing: In the Google Admin console, go to Apps > Google Workspace > Drive and Docs > Sharing settings. Enable the 'Visitor Sharing' feature.
Configure Visitor Sharing: Ensure that the sharing settings allow sharing with external users who do not have a Google account.
Demonstrate to Finance Team: Conduct a training session with the Finance team to demonstrate how to use the Visitor Sharing feature securely.
Share Reports: When sharing the quarterly financial reports, use the Visitor Sharing option to generate a secure sharing link that can be accessed by the external auditor without requiring a Google account.
Monitor and Review: Regularly review shared documents to ensure that access is being appropriately managed and that the security of shared data is maintained.
Google Workspace Admin Help - Visitor Sharing
Google Workspace Admin Help - Sharing Settings

QUESTION 40
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: B, D
Section:
Explanation:
Admin Console: Log into the Google Admin console at admin.google.com.
Enable Advanced Mobile Management for Sales OU:
Navigate to Devices > Mobile & endpoints > Settings.
Select the Sales OU and turn on Advanced Mobile Management.
Set Up an Apple Push Certificate:
Go to Devices > Mobile & endpoints > Apple certificates.
Follow the instructions to obtain and upload an Apple Push Certificate.
Device Policies:
After setting up the Apple Push Certificate, configure the desired device policies such as password policies, app distribution, and remote wipe capabilities.
Google Workspace Admin: Set up advanced mobile management
Google Workspace Admin: Set up an Apple Push Certificate

QUESTION 41
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: C
Section:
Explanation:
Prepare Environment: Ensure you have a supported server to install Google Cloud Directory Sync (GCDS).
Download GCDS:
Download Google Cloud Directory Sync from the Google Workspace Downloads page.
Install GCDS:
Follow the installation instructions provided by Google to install GCDS on the server.
Configuration:
Configure GCDS to synchronize user data from Active Directory to Google Workspace.
Set up synchronization rules and schedules to ensure that user data is kept up to date automatically.
Testing and Deployment:
Test the synchronization to ensure that new user accounts are created accurately in Google Workspace.
Deploy GCDS in the production environment after successful testing.
Google Workspace Admin: About Google Cloud Directory Sync
Google Workspace Admin: Install and Set Up GCDS

QUESTION 42
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:
Admin Console: Log into the Google Admin console at admin.google.com.
Devices Management: Navigate to Devices > Chrome > Settings.
Configuration:
Under the 'Chrome management' section, select 'User & browser settings'.
Choose the organizational unit where you want to apply this setting.
Auto-Updates Settings:
Scroll down to the 'Auto-update settings' section.
Enable the 'Randomly scatter auto-updates' option. This setting will spread out the updates over a period of time, reducing the load on your network.
Save Changes: Click 'Save' to apply the changes.
Google Workspace Admin: Manage automatic updates

QUESTION 43
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:
Explanation:
Google Calendar Live Stream:
When you create a Calendar event, you have the option to add a live stream. This feature allows participants to watch the event without having to actively join the meeting.
By adding the live stream to the Calendar invite and including the conference rooms, the rooms will automatically start the live stream at the scheduled time.
Adding Live Stream:
In the Google Calendar event, select the option to 'Add live stream'.
Add the conference rooms to the event as participants. These rooms will automatically connect to the live stream when the event starts.
Advantages:
This method ensures that participants in remote rooms can receive the training session without any manual intervention.
It simplifies the process for users, providing a seamless experience.
Google Workspace Admin Help: Add live streaming to an event
Google Meet hardware overview

QUESTION 44
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: D, E
Section:
Explanation:
Develop Custom Application:
Use the Domain Shared Contacts API to create a custom application.
The application should read the contacts from your corporate LDAP and upload them to Google Workspace.
This will ensure that these contacts appear in the address autocomplete for all users.
Configure Google Cloud Directory Sync (GCDS):
Install and configure GCDS on a supported server.
Set up synchronization to include shared contacts from your LDAP directory.
This will automatically keep the contacts updated and available in Gmail's address autocomplete.
Google Workspace Admin: Google Cloud Directory Sync
Google Workspace Admin: Domain Shared Contacts API

QUESTION 45
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: B, C
Section:
Explanation:
Create a Matter in Google Vault:
Log into Google Vault.
Click on 'Matters' and then 'Create'.
Name the matter appropriately (e.g., User Investigation).
Share the matter with the litigation team members by adding their email addresses under the 'Sharing' settings.
Create a Hold on the User's Mailbox:
In the created matter, go to the 'Holds' tab.
Click on 'Create Hold'.
Specify the user's email address to place their mailbox under hold.
Set the parameters for the hold to ensure all relevant data is preserved and cannot be tampered with.
Google Workspace Admin: Create and manage matters in Google Vault
Google Workspace Admin: Create and manage holds in Google Vault

QUESTION 46
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: C
Section:
Explanation:
Admin Console: Log into the Google Admin console at admin.google.com.
Reports Menu: Navigate to Reports > Reports.
Accounts Aggregate Report:
Under the ''Reports'' section, select ''Accounts''.
Click on ''Aggregate'' to view the report.
Download Data:
Click on the download icon and choose ''Google Sheets'' as the format to export the data.
This report includes a count of active and suspended users by organizational unit.
Google Sheets:
Open the downloaded report in Google Sheets.
Review and organize the data as needed to present it by Org unit, ensuring it matches the Regions and Departments within your company.
Google Workspace Admin: Reports overview
Google Workspace Admin: Aggregate reports

QUESTION 47
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
Section:
Explanation:
https://support.google.com/a/users/answer/9310352#1.1

QUESTION 48
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:
Explanation:
Access the Admin Console:
In the Google Workspace Admin console, navigate to 'Reports' > 'Audit' > 'Login'.
Generate a Login Audit Report:
Customize the report to include details about suspicious login attempts.
Set the time frame to the past year and filter the results to show only suspicious logins.
Export the Report:
Export the login audit report in a suitable format (e.g., CSV) for further analysis.
Ensure the report includes user account details and the number of suspicious login attempts for each account.
Analyze the Data:
Review the exported data to identify patterns and determine how frequently suspicious login attempts occur within the organization.
Provide the analysis to the CISO with the required details for each user account.
Google Workspace Admin Help: View and analyze login audit logs

QUESTION 49
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: B
Section:
Explanation:
Access the Transfer Tool:
In the Google Workspace Admin console, go to 'Users' > 'Transfer tool for unmanaged users'.
Identify Unmanaged Accounts:
Use the tool to search for unmanaged accounts (consumer Google accounts) that have corporate email addresses.
Send Transfer Requests:
Send transfer requests to the identified unmanaged accounts, asking the former users to transfer their accounts to your managed domain.
Monitor and Complete Transfers:
Monitor the transfer process and ensure that the accounts are successfully transferred.
Verify that the transferred accounts are now managed under your Google Workspace domain, preventing unauthorized access to services.
Google Workspace Admin Help: Transfer tool for unmanaged users

QUESTION 50
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:
https://support.google.com/a/answer/2463723?hl=en

QUESTION 51
You work for an organization that is headquartered in Washington DC You want to reliably send email announcements to all employees in the area and update membership automatically What should you do?

A. Create a Dynamic Group by using the location condition to keep the distribution list automatically updated based on the employees work locations
B. Create a Security Group and apply the Location label to allow employees to join based on the specified location
C. Create a Google Group and add all employees in the Washington DC work location
D. Create a Google Group and set permissions to invite employees to join the group

Correct Answer: A
Section:
Explanation:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Navigate to Groups: Go to Directory > Groups.
Create Dynamic Group: Click on Create group and select Dynamic group.
Set Location Condition: Define the membership condition based on the work location attribute. Set the condition to include employees located in Washington DC.
Configure Group Settings: Set up the necessary group settings such as permissions and access controls.
Automatic Updates: The group membership will be automatically updated based on the employees' work locations, ensuring that the distribution list always reflects the current employee locations.
Google Workspace Admin Help: Create dynamic groups

Google Workspace Dynamic Groups Overview

QUESTION 52
You work for an international organization and your CEO frequently travels to other countries You need to enable email access and configure the account for multiple administrative assistants What should you do?

A. Log into the Gmail account of the CEO Set up and share two separate email aliases
B. Enable users to specify what sender information is included in delegated messages sent from their account.
C. Create a group of administrative assistants Enable delegated access to the mailbox of the CEO for that group
D. Provide the executive administrative assistants with the account password of the CEO

Correct Answer: C
Section:
Explanation:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Create a Group: Go to Directory > Groups and create a new group for the administrative assistants.
Add Members: Add the administrative assistants to this group.
Enable Delegated Access: Go to Users > [CEO's account] > Account and click on Email delegation.
Delegate Mailbox Access: Enter the email address of the newly created group. This allows all members of the group to access the CEO's mailbox.
Save Changes: Confirm and save the changes. The administrative assistants will now have delegated access to the CEO's email account, allowing them to manage emails while the CEO is traveling.
Google Workspace Admin Help: Email delegation
Google Workspace Best Practices for Email Delegation

QUESTION 53
Your organization is working on a confidential project with details that cannot be shared through email with anyone outside your organization You want to add controls in Gmail that prevent any mention of the project from being sent by employees Only the CEO and the CFO can send information about the project over email and without a delay What should you do?

A. Configure the Gmail Restrict delivery setting and add an allowlist with all domains that your employees are allowed to send emails to Include the CEO and CFO email addresses to the allowlist
B. Configure a Gmail Content compliance rule for outbound email that quarantines all email mentioning the project Bypass the rule by using the address list with the CEO and CFO email addresses.
C. Configure a Gmail Content compliance rule for outbound email that quarantines all email mentioning the project Manually review all quarantined emails and choose to deliver the ones sent by the CEO and CFO
D. Configure the Gmail Restrict delivery setting for all outgoing messages, except the internal emails Add the CEO and CFO email

Correct Answer: B
Section:
Explanation:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Navigate to Gmail Settings: Go to Apps > Google Workspace > Gmail > Compliance.
Create Content Compliance Rule: Click on Configure and select Add another rule under Content compliance.
Set Conditions: Define conditions to detect mentions of the confidential project in outbound emails.
Set Actions: Configure the rule to quarantine emails that match the conditions.
Bypass Rule for Specific Users: Use the address list feature to bypass the rule for the CEO and CFO email addresses.
Save and Implement: Save the rule and ensure it is activated. This will quarantine emails about the project, except those sent by the CEO and CFO.
Google Workspace Admin Help: Set up rules for content compliance
Google Workspace Email Compliance Best Practices

QUESTION 54
An employee at your organization is resigning They are in charge of organizing and maintaining recurring team events You want to preserve the existing meetings and transfer ownership to the resigning employee's manager What should you do?

A. Assign an Archived User (AU) license for the resigning employee
B. Delete the existing calendar events and instruct the manager to create new events as the owner
C. Instruct the resigning employee to share free busy details for their calendar with their manager
D. Transfer both the events and the resources owned by the resigning employee to their manager by using the Admin console

Correct Answer: D
Section:
Explanation:
To transfer ownership of the existing meetings and resources from the resigning employee to their manager, follow these steps:
Sign in to the Google Admin console: Use an account with super administrator privileges.
Navigate to the Calendar settings:
Go to Apps > Google Workspace > Calendar > Manage resources.
Transfer calendar events:
Go to Tools > Data Transfer.
Select the user whose data you want to transfer (the resigning employee).
Choose 'Calendar' as the service to transfer.
Enter the email address of the manager who will receive the ownership.
Initiate the transfer.
Verify transfer completion:
Once the transfer is complete, check that the manager now owns the calendar events and resources.
Ensure that all recurring events and resources are correctly transferred.
Google Workspace Admin Help - Transfer Calendar events
Google Workspace Admin Help - Data Transfer Tool

QUESTION 55
Your organization has hired a recruiting firm that is responsible for reviewing resumes and job descriptions of prospective summer interns. Employees at your organization need to collaborate with the external firm on these documents. You must set permissions and ensure the recruiting firm employees can't remove the files. What should you do?

A. Create a Google Group, add the HR team, and create a shared folder for content storage and editing
B. Enable client-side encryption for the organizational unit (OU) for which the HR team are members
C. Create a Shared Drive and grant Content Manager access to the HR team
D. Create a Shared Drive and grant Contributor access to the HR team

Correct Answer: D
Section:
Explanation:
To set permissions and ensure that the recruiting firm employees can't remove the files, follow these steps:
Sign in to the Google Admin console: Use an account with super administrator privileges.
Create a Shared Drive:
Go to Drive and Docs > Manage shared drives.
Click on 'Create a shared drive' and give it a name relevant to the recruiting project.
Add members and set permissions:
Click on the shared drive.
Add the HR team and the recruiting firm employees as members.
Grant 'Contributor' access to the HR team, which allows them to edit and collaborate on documents but not delete them.
Grant 'Viewer' or 'Commenter' access to the recruiting firm employees if they only need to review the documents without editing.
Google Workspace Admin Help - Shared Drives
Google Workspace Admin Help - Permissions for shared drives

QUESTION 56
Users at your organization are reporting issues with Google Voice including disconnected calls and overall connection issues. You want to identify whether these issues affect just your organization or whether it's a global Google issue What should you do?

A. Use the Security Investigation Tool with Voice Log Events as the data source field In the search operator fields select Event is and Network Statistics (client) Analyze the packet loss
B. Verify if there is a service outage for Google Voice reported on the Google Workspace Status Dashboard
C. Use the Security investigation Tool with User Log Events as the data source field In the search operator fields select Event is and Call failed Analyze the packet loss
D. Verify if there is a service interruption for Google Voice reported on the Google Workspace Updates Blog website

Correct Answer: B
Section:
Explanation:
To identify whether the Google Voice issues are affecting just your organization or if it's a global issue, follow these steps:
Check the Google Workspace Status Dashboard:
Go to the Google Workspace Status Dashboard.
Look for any reported outages or issues specifically for Google Voice.
The status dashboard provides real-time information on service availability and any ongoing issues affecting Google Workspace services.
Google Workspace Status Dashboard

QUESTION 57
A user named Alice is leaving your organization You need to transfer all of Alice's data from her Drive to Bob's Drive in the most simple and efficient manner possible What should you do?

A. Use the Google Admin console to move the files from Alice's Drive to Bob's Drive
B. Use the Google Takeout service to export Alice's data to a zip file and instruct Bob to import the zip file into his Drive
C. Use the Google Drive API to programmatically transfer the files from Alice's Drive to Bob's Drive
D. Instruct Alice to download all of her files from her Drive and upload them to Bob's Drive

Correct Answer: A
Section:
Explanation:
To transfer all of Alice's data from her Drive to Bob's Drive in the most simple and efficient manner, follow these steps:
Sign in to the Google Admin console: Use an account with super administrator privileges.
Navigate to the Data Transfer tool:
Go to Apps > Google Workspace > Drive and Docs.
Click on 'Transfer ownership.'
Initiate the transfer:
Enter Alice's email address as the current owner.
Enter Bob's email address as the new owner.
Select the option to transfer all files and folders from Alice's Drive to Bob's Drive.
Click on 'Transfer files' to initiate the process.
Verify the transfer:
Once the transfer is complete, confirm that all files and folders are now owned by Bob and accessible in his Drive.
Google Workspace Admin Help - Transfer Drive files

QUESTION 58
You have enrolled a new Google Meet hardware device for an existing conference room in your building Your users report that the new hardware in the conference does not show the expected calendar events You need to investigate and fix the problem What should you do?

A. Make sure that the conference room resource calendar has been created and that the Meet Hardware is associated with that resource
B. Create a brand new resource calendar and associate the Meet Hardware with that new resource
C. Use the Meet Quality Tool in the control panel to search for the newly installed Meet Hardware
D. Make sure the Access permissions for the resource calendar is set to 'See all event details

Correct Answer: A
Section:
Explanation:
To investigate and fix the issue where the new hardware does not show the expected calendar events, follow these steps:
Sign in to the Google Admin console: Use an account with super administrator privileges.
Verify the resource calendar:
Go to Apps > Google Workspace > Calendar > Resources.
Ensure that the conference room resource calendar has been created.
Associate the Meet hardware:
Go to Devices > Google Meet hardware.
Find the new hardware device and check its settings.
Ensure the device is associated with the correct conference room resource calendar.
Check calendar permissions:
Go to Calendar > Manage resources.
Ensure the calendar associated with the Meet hardware has the appropriate access permissions set to 'See all event details.'
Google Workspace Admin Help - Manage resources
Google Workspace Admin Help - Google Meet hardware

QUESTION 59
You work at a large global holding firm with multiple companies that are united under one Google Workspace deployment. You must ensure that employees can only access documents at the company in which they are employed What should you do?

A. Create a User group for each company and change Google Drive sharing settings to block external sharing
B. Create an organizational unit (OU) for each company and disable file sharing.
C. Set up data loss prevention (DLP) rules to prevent specific documents from being shared
D. Set up Google Drive trust rules to prevent access to documents from individual companies

Correct Answer: D
Section:
Explanation:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Navigate to Drive and Docs: Go to Apps > Google Workspace > Drive and Docs.
Set Up Drive Trust Rules: Select Sharing settings > Sharing options.
Configure Trust Rules: Set up trust rules to define which organizational units (OUs) or groups can share documents with each other. Ensure that each company's OU has rules that restrict access to documents only within that company.
Apply and Save Changes: Implement these settings and save. This ensures that employees can only access documents within their respective companies.
Google Workspace Admin Help: Drive trust rules
Google Workspace Drive Sharing Settings

QUESTION 60
An employee at your organization is experiencing video call issues in Google Meet and they were unable to resolve the issues by themselves You need to troubleshoot the issue What should you do first?

A. View the Meet quality report of the employee

B. Ask your network administrator to add the dedicated Meet IP address range for your users
C. Restart the device of the employee
D. Check the Meet settings of the employee

Correct Answer: A
Section:
Explanation:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Navigate to Meet Quality Tool: Go to Apps > Google Workspace > Google Meet > Meet quality tool.
Search for the Employee: Use the search function to locate the employee's recent meeting reports.
Analyze the Report: Review the quality report, which includes metrics such as network connectivity, audio and video quality, and any issues encountered during the call.
Identify and Troubleshoot Issues: Based on the report findings, identify the specific issues affecting the video calls and take appropriate actions to resolve them, such as checking network connections or adjusting Meet settings.
Google Workspace Admin Help: Meet quality tool
Google Meet Quality Troubleshooting

QUESTION 61
Your organization is migrating to Google Workspace and wants to improve how newly created files are classified You must find a scalable solution to improve security and transparency on how to handle sensitive files What should you do?

A. Set data loss prevention (DLP) policies to label data automatically disable label locking, and educate users
B. Create classification labels enable automatic classification, and educate users
C. Migrate data to Google Workspace map classifications and migrate with the Drive Labels API
D. Integrate with the Cloud DLP API map identifiers and classifications install the Google Drive label client and run the application

Correct Answer: B
Section:
Explanation:
Step by Step Comprehensive Detailed Explanation:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Navigate to Labels: Go to Apps > Google Workspace > Drive and Docs > Labels.
Create Classification Labels: Define and create classification labels that correspond to different levels of sensitivity and types of files.
Enable Automatic Classification: Configure settings to enable automatic classification of newly created files based on predefined criteria and patterns.
Educate Users: Conduct training sessions or distribute documentation to educate users on how to use classification labels effectively and understand their importance in maintaining data security.
Google Workspace Admin Help: Drive labels
Google Workspace DLP and Classification

QUESTION 62
As a Workspace Administrator you want to keep an inventory of the computers and mobile devices your company owns in order to track details such as device type and who the device is assigned to. How should you add the devices to the company-owned inventory?

A. Download the company-owned inventory template CSV file from the Admin panel enter the serial number of the devices and upload the
B. completed file to the company-owned inventory in the admin panel B O Download the company-owned inventory template CSV file from the Admin panel enter the device OSs. and serial numbers and upload the
C. completed file to the company-owned inventory in the admin panel. C O Download the company-owned inventory template CSV file from the Admin panel enter the asset tags of the devices, and upload the
D. completed file to the company-owned inventory in the admin panel D O Download the company-owned inventory template CSV file from the Admin panel, enter the device OSs. and asset tags, and upload the

Correct Answer: A
Section:

Explanation:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Navigate to Devices: Go to Devices > Mobile and endpoints.
Download Inventory Template: Click on Manage company-owned inventory > Download template CSV.
Enter Device Details: Fill in the template with the serial numbers and other relevant information of the devices.
Upload Completed File: Once the CSV file is completed with all device details, upload it back to the Admin console under Manage company-owned inventory.
Verify and Save: Ensure that the uploaded data is correct and save the inventory. This keeps a record of all company-owned devices.
Google Workspace Admin Help: Manage company-owned devices
Google Workspace Device Inventory Management

QUESTION 63
The Google Analytics service is set to OFF for your entire organization All users in the marketing team OU and a subset of users in the sales OU need access to Analytics The rest of the organization should not have access You must configure access in Additional Google services What should you do?

A. Enable Google Analytics at the top of the OU structure
B. Enable Google Analytics for the marketing and sales OUs Create a group to deny access to Google Analytics and assign it to the sales users who should not have access
C. Enable Google Analytics for the marketing OU. Create a sub-OU for the sales users under the marketing OU
D. Enable Google Analytics for the marketing OU Create a group from the Admin console that includes the sales users, and set GoogleAnalytics to On for that group

Correct Answer: D
Section:
Explanation:
Access Admin Console: Log in to the Google Admin console using your administrator account.
Navigate to Additional Google Services: Go to Apps > Additional Google services > Google Analytics.
Enable for Marketing OU: Select the marketing OU and turn on Google Analytics.
Create Group for Sales Users: Go to Directory > Groups and create a new group for the sales users who need access to Google Analytics.
Assign Google Analytics Access: In the Google Analytics settings, turn on access for the newly created sales group.
Verify Settings: Ensure that only users in the marketing OU and the specific sales group have access to Google Analytics while the rest of the organization does not.
Google Workspace Admin Help: Turn Additional Google services On or Off
Google Workspace Service Access Management

QUESTION 64
Your organization has a strict requirement that your temporary employees can only send emails to and receive emails from specific external domains You must define a policy in Google Workspace that meets this requirement for users in the temporary employee organizational unit (OU) What should you do?

A. Create a policy in Gmail settings that rewrites the recipient for outbound messages and quarantines incoming messages to review before delivery
B. Add the allowed domains when configuring the restrict delivery setting in Gmail settings, and select the box to bypass for internal emails
C. Restrict sending and receiving to Google Groups, and carefully curate the temporary employees' memberships
D. Configure the restrict delivery setting to limit domains that the temporary employees can communicate with Allow Google Docs sharing

Correct Answer: B
Section:
Explanation:
Access the Admin Console: Sign in to your Google Admin console.
Navigate to Apps: Click on 'Apps' and then 'Google Workspace.'
Select Gmail: In the Google Workspace section, click on 'Gmail.'
Gmail Settings: Click on 'Compliance' under the 'Advanced settings' section.
Restrict Delivery Setting: Scroll down to the 'Restrict delivery' section and click 'Configure.'
Define Policy: Enter the specific external domains you want to allow the temporary employees to communicate with.

Bypass for Internal Emails: Make sure to select the option to bypass the restriction for internal emails, ensuring internal communication is not affected.
Apply to OU: Apply this setting to the organizational unit (OU) containing the temporary employees.
Save the Configuration: Save the changes and ensure the policy is active.
Google Workspace Admin Help: Set up compliance rules for Gmail

QUESTION 65
Your default Vault retention policy for Gmail is set to 365 days Your legal department has just informed you that emails sent and received by the customer support department are sensitive and must be retained for only 30 days You must enforce this new retention policy in the simplest way What should you do?

A. Change the current default retention policy in Vault for Gmail to 30 days and apply it to the customer support organizational unit (OU) Configure a custom retention policy for Gmail for 365 days for your domain
B. Create two custom retention policies in Vault one for 30 days that is applied to the customer support organizational unit (OU) and one for 365 days that is applied to all other OUs in your directory
C. Change the current default retention policy for Gmail to 30 days Configure two custom retention policies in Vault one for 30 days that is applied to the customer support organizational unit (OU) and one for 365 days that is applied to all other OUs in your directory
D. Create a custom retention policy in Vault for Gmail for 30 days and apply it to the customer support organizational unit (OU)

Correct Answer: D
Section:
Explanation:
Step by Step Comprehensive Detailed Explanation:
Access Google Vault: Sign in to Google Vault.
Retention Policies: Navigate to 'Retention' from the side menu.
Create New Retention Rule: Click on 'Create retention rule.'
Set Duration: Set the retention period to 30 days.
Apply to OU: Apply this retention rule specifically to the organizational unit (OU) for the customer support department.
Exclude Default Rule: Ensure that this custom rule overrides the default 365-day retention policy for the customer support OU.
Save and Activate: Save the rule and ensure it is activated.
Google Vault Help: Set retention rules

QUESTION 66
Your organization has confidential internal content for which only authorized employees are allowed to access Access to this content is managed by using Google Groups Only administrators can create and manage membership You need to provide only the necessary functionality and follow the principle of least privilege What should you do?

A. Make a dynamic group so security team members are automatically added
B. Make a moderated group so all incoming communications can be monitored
C. Use a group as a collaborative inbox that allows easier sharing
D. Make a security group to apply access policies

Correct Answer: D
Section:
Explanation:
Navigate to Groups: Go to the Google Admin console and navigate to 'Groups'.
Create a Security Group: Create a new group and set it as a security group.
Assign Permissions: Set the appropriate permissions and policies that restrict access to only authorized employees.
Manage Membership: Ensure that only administrators can manage the group membership, adhering to the principle of least privilege.
Apply Policies: Apply access policies to the security group, ensuring that the confidential content is accessible only to authorized members.
Create and manage security groups
Google Groups for Business

QUESTION 67

An employee has left your organization and their Drive data must be retained for three years The retention rule has been set for three years You must ensure the employee's data is visible in Vault and accessible to the Vault Administrator in the most cost-effective way What should you do?

A. Export the users Drive data from Vault, then delete the user.
B. Assign an Archive User (AU) license to the user
C. Change ownership of the Drive data to the user's Manager, then delete the user
D. Suspend the user until the end of the three-year period

Correct Answer: B
Section:
Explanation:
Step by Step Comprehensive Detailed Explanation
Navigate to Users: Go to the Google Admin console and navigate to the 'Users' section.
Select the User: Find and select the user who has left the organization.
Assign Archive User License: Assign an Archive User (AU) license to the user, ensuring their data is retained and accessible in Vault.
Verify Access in Vault: Go to Google Vault and verify that the data is visible and accessible to the Vault Administrator.
Cost-effective Data Retention: Using an AU license is cost-effective as it retains the data without needing an active Google Workspace license.
Assign licenses to users
Google Vault Archive User

QUESTION 68
Your organization has a group of users who interact with sensitive information and their accounts contain valuable files You need to protect these users from targeted online attacks What should you do?

A. Enable 2-Step Verification for those users and recommend they use Google Authenticator
B. Enable 2-Step Verification for those users and recommend they use SMS codes
C. Disable password recovery for end users
D. Enroll all accounts for those users in the Advanced Protection Program

Correct Answer: D
Section:
Explanation:
Understanding the Requirement:
The scenario involves a group of users who handle sensitive information and have valuable files in their accounts.
The goal is to protect these users from targeted online attacks.
Options Analysis:
Option A: Enable 2-Step Verification for those users and recommend they use Google Authenticator
2-Step Verification (2SV) enhances security by adding an extra layer of authentication. Google Authenticator is a reliable method, but it may not be sufficient against highly targeted attacks.
Option B: Enable 2-Step Verification for those users and recommend they use SMS codes
While SMS codes are a form of 2SV, they are considered less secure than other methods due to potential vulnerabilities like SIM swapping.
Option C: Disable password recovery for end users
Disabling password recovery can prevent unauthorized access through recovery options but does not provide active protection against targeted attacks.
Option D: Enroll all accounts for those users in the Advanced Protection Program
The Advanced Protection Program (APP) is designed specifically to protect users at high risk of targeted attacks. It includes strong measures such as requiring a physical security key for login, blocking unauthorized access attempts, and restricting access to sensitive data.
Recommended Solution:
Enrolling users in the Advanced Protection Program (APP):
Step 1: Identify High-Risk Users:
Identify users who handle sensitive information and have valuable files.
Step 2: Enroll in APP:

Go to the Google Admin console.
Navigate to the Security section and find the Advanced Protection Program.
Enroll the identified high-risk users in APP.
Step 3: Implement Security Keys:
Ensure users have security keys (e.g., Titan Security Keys) for login.
Guide users through the process of setting up and using security keys.
Step 4: User Education:
Educate users on the importance of APP and how it protects their accounts.
Provide training on recognizing phishing attempts and other security best practices.
Benefits of APP:
Enhanced Security:
APP provides the highest level of security for Google accounts, requiring security keys for authentication.
Protection Against Phishing:
Security keys are highly resistant to phishing attacks, which are common in targeted online attacks.
Limited Access:
APP restricts access to sensitive data, ensuring that only trusted apps and services can interact with the protected accounts.
Google Workspace Admin Help: Advanced Protection Program
Google Workspace Security: Advanced Protection Program
Google Security Blog: Advanced Protection Program

QUESTION 69
Your organization is moving from a legacy mail system to Google Workspace This move will happen in phases During the first phase, some of the users in the domain are set up to use a different identity provider (IdP) for logging in You need to set up multiple idPs for various users What should you do?

A. Enable single sign-on (SSO) with third-party identity providers and exclude the users who are using a different provider
B. Enable single sign-on (SSO) with Cloud Identity and use Cloud Directory Sync to manage multiple identity providers
C. Create Security Assertion Markup Language (SAML) based single sign-on (SSO) profiles and assign them to specific organizational units or groups of users.
D. Nothing Google uses cookies to establish a user's relationship to a device This will cover multiple identity providers

Correct Answer: C
Section:
Explanation:
Access Admin Console: Sign in to your Google Admin console.
Navigate to Security: Click on 'Security' and then 'Set up single sign-on (SSO) with a third party IdP.'
Add SAML Apps: Click on 'Add SAML app' and select the app to configure.
Create SSO Profiles: Set up SSO profiles for each identity provider by entering the required SAML details such as ACS URL, Entity ID, etc.
Assign to OUs/Groups: Assign the created SSO profiles to specific organizational units (OUs) or groups of users based on their IdP.
Verify Configuration: Ensure that each profile is properly configured and tested.
Google Workspace Admin Help: Set up SSO via SAML for single sign-on

QUESTION 70
An employee at your organization is having trouble playing a video stored in Google Drive that is embedded in their Google Slides presentation You need to collect the necessary details to troubleshoot the issue What should you do?

A. Confirm that the source video is in a supported format and resolution and that the user has permission to play the video Have a screen share session to confirm the behavior
B. Instruct the employee to give you edit access to the presentation to review the revision history See if the error message changes when you delete and add the slides back
C. Check the Google Drive audit logs for any error entries on the Slides presentation Check the help center for the appropriate error message
D. Create a copy of the presentation to see if you can replicate the problem, and document any errors you see

Correct Answer: A
Section:
Explanation:
Verify Video Format: Ensure that the video format is supported by Google Drive (e.g., .mp4, .mov).
Check Video Resolution: Make sure the video resolution is supported and not too high for smooth playback.
Permission Check: Confirm that the user has the necessary permissions to access and play the video.
Screen Share Session: Arrange a screen sharing session with the user to observe the issue firsthand.
Replication of Issue: During the session, attempt to play the video to confirm the behavior and identify any error messages.
Troubleshoot: Based on the findings, guide the user on possible fixes such as re-uploading the video, adjusting permissions, or converting the video to a supported format.
Google Workspace Admin Help: Supported video formats

QUESTION 71
The helpdesk at your organization reports that many users in multiple locations are not able to access Gmail, but can access other Workspace services. You must troubleshoot the issue What should you do first?

A. Open a ticket with Google Support listing the affected users.
B. Check the Google Workspace status dashboard to see whether there is a disruption in Gmail service availability
C. Check the Google Workspace release calendar to ensure there's not a Gmail upgrade scheduled
D. Check network connectivity of the affected users

Correct Answer: B
Section:
Explanation:
Access Status Dashboard: Open the Google Workspace Status Dashboard.
Check Service Status: Look for any reported issues or outages specifically for Gmail.
Verify Timing: Check the timing of the reported issues to see if they correlate with the time when users reported problems.
Additional Information: Review any additional details or updates provided by Google regarding the service disruption.
Communicate Status: Inform the affected users about the service status and any expected resolution time.
Open Ticket if Necessary: If no issues are reported on the status dashboard, proceed with other troubleshooting steps such as checking network connectivity or opening a ticket with Google Support.
Google Workspace Status Dashboard

QUESTION 72
An employee has been leaking confidential salary information to an external party. You must use Vault to preserve the messages for an investigation. What should you do?

A. Create a matter and add a hold on the employee's email
B. Use the security investigation tool to find the messages Create a hold to preserve the messages
C. Create a custom retention policy Use the audit feature to view captured email logs
D. Use the search and export features to find all the messages sent externally

Correct Answer: A
Section:
Explanation:
Access Google Vault: Go to Google Vault from the Google Admin console.
Create a Matter: Click on 'Matters' and create a new matter to hold the case details and any relevant information.
Add a Hold: Within the matter, create a hold specifically on the employee's email account. This ensures that all emails sent and received by the employee are preserved.
Configure the Hold: Specify the criteria for the hold, such as the employee's email address, and set the scope to include all messages.
Save the Hold: Once configured, save the hold. This will preserve all relevant messages for the investigation.
Google Vault Help: Create and manage matters
Google Vault Help: Place data on hold

QUESTION 73
An employee at your company does not need access to their Workspace account while they are on leave for a year When they return you need to ensure they have access to their account and that all their data and current emails remain intact Also their shared documents must be available to other users You must accomplish this goal in the most cost-effective way What should you do?

A. Assign an Archive User license
B. Suspend their account in the Admin console
C. Delete the user after copying their emails and reassigning their documents to their manager
D. Remove the user license in the Admin console

Correct Answer: B
Section:
Explanation:
Access the Admin Console: Sign in to your Google Admin console.
Navigate to Users: Click on 'Directory' and then 'Users.'
Find the User Account: Locate the user who is going on leave.
Suspend Account: Click on the user's name to open their account details, then click 'Suspend user.'
Confirm Suspension: Confirm the suspension, which retains all data and settings while disabling access to the account.
Shared Documents: Ensure that their shared documents remain accessible to other users without any interruptions.
Google Workspace Admin Help: Suspend a user

QUESTION 74
After making a recent migration to Google Workspace, you updated your Google Cloud Directory Sync configuration to synchronize the global address list. Users are now seeing duplicate contacts in their global directory in Google Workspace. You need to resolve this issue.
What should you do?

A. Train users to use Google Workspace's merge contacts feature.
B. Enable directory contact deduplication in the Google Workspace Admin panel.
C. Update shared contact search rules to exclude internal users.
D. Create a new global directory, and delete the original.

Correct Answer: C
Section:
Explanation:
Access Admin Console: Log into your Google Workspace Admin Console.
Update GCDS Configuration: Open the Google Cloud Directory Sync (GCDS) configuration.
Modify Search Rules: Update the shared contact search rules within GCDS.
Exclude Internal Users: Modify the rules to exclude internal users from being synchronized as shared contacts.
Save and Sync: Save the updated configuration and perform a sync to apply the changes, which should resolve the issue of duplicate contacts in the global directory.
Google Support: Google Cloud Directory Sync

QUESTION 75
The organization has conducted and completed Security Awareness Training (SAT) for all employees. As part of a new security policy, employees who did not complete the SAT have had their accounts suspended. The CTO has requested to be informed of any accounts that have been re-enabled to ensure no one is in violation of the new security policy.
What should you do?

A. Enable ''Suspicious login'' rule - Other Recipients: CTO
B. Enable ''Suspended user made active'' rule - Other Recipients: CTO

C. Enable ''Email settings changed'' rule - -Other Recipients: CTO
D. Enable ''Suspended user made active'' rule and select ''Deliver to'' Super Administrator(s)

Correct Answer: B
Section:
Explanation:
Access Admin Console: Log into your Google Workspace Admin Console.
Navigate to Alert Center: Go to Security > Alert Center.
Enable Alert Rule: Find and enable the ''Suspended user made active'' rule.
Configure Recipients: In the alert rule settings, add the CTO as an additional recipient under the ''Other Recipients'' section.
Save Settings: Save the configuration. The CTO will now receive notifications whenever a suspended user's account is re-enabled, ensuring compliance with the new security policy.
Google Support: Alert Center