vmexam.com
#1 Cloud and VM Certification Guide

Google GCP-PGWA

GOOGLE PROFESSIONAL GOOGLE WORKSPACE ADMINISTRATOR CERTIFICATION QUESTIONS & ANSWERS

Exam Summary – Syllabus – Questions

GCP-PGWA

Google Cloud Platform - Professional Google Workspace Administrator (GCP-PGWA)

50-60 Questions Exam – 70% Cut Score – Duration of 120 minutes

www.VMExam.com

Table of Contents

Know Your GCP-PGWA Certification Well:

The GCP-PGWA is best suitable for candidates who want to gain knowledge in the Google Professional. Before you start your GCP-PGWA preparation you may struggle to get all the crucial Professional Google Workspace Administrator materials like GCP-PGWA syllabus, sample questions, study guide.

But don't worry the GCP-PGWA PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the GCP-PGWA syllabus?
- How many questions are there in the GCP-PGWA exam?
- Which Practice test would help me to pass the GCP-PGWA exam at the first attempt?

Passing the GCP-PGWA exam makes you Google Cloud Platform - Professional Google Workspace Administrator (GCP-PGWA). Having the Professional Google Workspace Administrator certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Google GCP-PGWA Professional Google Workspace Administrator Certification Details:

Exam Name	Professional Google Workspace Administrator
Exam Code	GCP-PGWA
Exam Price	$200 USD
Duration	120 minutes
Number of Questions	50-60
Passing Score	Pass / Fail (Approx 70%)
Recommended Training / Books	**Google Cloud training** **Google Cloud documentation** **Google Cloud solutions**
Schedule Exam	**Google Cloud Webassessor**
Sample Questions	**Google GCP-PGWA Sample Questions**
Recommended Practice	**Google Cloud Platform - Professional Google Workspace Administrator (GCP-PGWA) Practice Test**

GCP-PGWA Syllabus:

Section	Objectives
Managing objects (20% of the exam)	
Managing account lifecycles by using provisioning and deprovisioning processes. Considerations include:	- Transferring ownership data to another account - Provisioning users based on a process determined by an organization's policy (for example, where to list accounts) - Provisioning and deprovisioning accounts, including: • Creating, reviewing, updating, deleting accounts (CRUD [create, read, update, and delete] operations). • Adding users (for example, individual, bulk, and automated) • Offboarding accounts (for example, suspending, deleting, and recovering) • Editing user attributes (for example, renaming, passwords, and aliases) • Creating administrative roles (for example, default roles, and custom roles) - Revoking account access outside of a typical organizational policy (for example, security reasons and personnel issues) - Configuring, monitoring, troubleshooting, and updating lifecycle management by using Google Cloud Directory Sync (GCDS) • Auditing and reviewing GCDS (for example, interpreting log data)
Configuring Google Drive. Consideration include:	- Managing the lifecycle of shared drives based on user requests and organizational policies (for example, OU [organizational unit] placements) - Configuring shared drive permissions, given specific requirements or scenarios - Implementing shared drive membership permissions based on organizational policies - Transferring user data from one user's drive to another drive - Applying security best practices for shared drives based on the business need
Managing calendar and calendar resources. Considerations include:	- Creating and managing calendar resources - Managing and delegating calendar access and resources - Managing the lifecycle of both individual and shared calendars (for example, differentiating between an individual's calendar and a calendar resource) - Configuring Google video conference room options (for

Section	Objectives
	example, Jamboard, Google Meet) - Scheduling Google Meet conferences and livestream meetings or events - Monitoring usage reports and recommending changes - Troubleshooting calendar issues
Configuring and managing Groups for business. Considerations include:	- Configuring memberships and advanced settings, including: • Adding users to groups • Implementing current Google Workspace APIs • Automating tasks by using Apps Script - Using a Google group to apply membership permissions for a shared drive - Creating specific types of Google-native groups (for example, dynamic, security, identity-mapped, and POSIX) - Implementing Google group security access controls to restrict members - Troubleshooting issues in a Google group (for example, calendar invites not expanding, invites unable to be sent to a group)
Configuring services (18% of the exam)	
Implementing and managing Google Workspace configurations based on corporate policies. Considerations include:	- Assigning and configuring permissions to Google Workspace tools by using organizational units (OUs) and Google groups - Modifying OU policies - Implementing application and security settings according to OU inheritance and override settings in parent OUs - Delegating granular Identify and Access Management (IAM) administrator roles and permissions to users in a domain - Implementing security configuration options for installing or using Google Cloud Marketplace applications or add-ons - Configuring Drive labels for data organization - Configuring a Rapid Release or Scheduled Release for feature releases - Configuring Google Meet to align with corporate policies and requirements - Creating and configuring security and data region settings - Implementing security integration protocols and addressing questions and objections from users - Managing content compliance rules - Investigating and remediating an issue by using Security Health Analytics check results
Configuring Gmail. Considerations	- Configuring basic mail routing scenarios for split delivery - Configuring a mail host

Section	Objectives
include:	- Configuring end-user access to Gmail by using Google Workspace Sync for Microsoft Outlook (GWSMO) or email client (for example, POP, IMAP, Thunderbird, Outlook) - Configuring POP and IMAP access to align with corporate policies and requirements - Configuring administrator access for mail forwarding by using advanced Gmail settings (for example, compliance rules, default routing, APIs) - Managing and understanding all available spam controls (for example, allowlist, denylist, inbound gateway, and IP allowlist) - Enabling email delegation for an OU - Managing Gmail archives
Troubleshooting (24% of the exam)	
Troubleshooting mail delivery problems reported by users. Considerations include:	- Determining whether user behavior or a broader issue (for example, rules, or Cloud Data Loss Prevention [DLP]) is causing an error - Determining whether an issue is an expected behavior (for example, a missing attachment, or an attachment filter issue) - Auditing and reviewing mail flow structure and end-user actions to determine the root cause of delivery issues - Analyzing message headers or email audit logs by using Google Workspace tools or security investigation tools - Recommending and/or implementing an appropriate course of action related to mail delivery issues (for example, implementing mail policy changes)
Troubleshooting and collecting logs and reports needed to engage with the support team. Considerations include:	- Documenting steps taken by end user to reproduce an issue - Collecting appropriate log file types - Searching for known issues and application status - Generating HAR files
Identifying, classifying, troubleshooting, and mitigating basic email attacks. Considerations Include:	- Configuring: • Blocked senders • Email allowlist • Objectionable content • Phishing settings • Spam settings • Gmail safety settings

Section	Objectives
	• Administrator quarantine • Attachment compliance • Secure transport compliance - Implementing Sender Policy Framework (SPF); Domain-based Message Authentication, Reporting, and Conformance (DMARC); Mail Transfer Agent Strict Transport Security (MTA-STS); and DomainKeys Identified Mail (DKIM) to secure email transmission - Investigating whether custom configurations are responsible for any issues or vulnerability (for example, email allowlist and IP addresses) - Investigating the scope of email attacks by using available Google Workspace email tools - Analyzing message contents for common attack patterns (for example, name, domain, and brand spoofing) - Mitigating successful attacks and preventing future attacks by using Google Workspace email tools (for example, identifying the issue and responding)
Troubleshooting Google Workspace access and performance issues. Considerations include:	- Identifying why a user is having an issue when they access a single Google application (for example, Drive) - Identifying the root cause of a performance issue when accessing a Google Workspace application (for example, a known issue, an outage, a network, or a device) - Analyzing, evaluating, and modifying settings to ensure delivery of critical emails (for example, specific IP ranges, X-headers) - Troubleshooting authentication issues that users reported - Troubleshooting issues that users reported when they set up Google Workspace on a mobile device - Troubleshooting Google Meet video call issues from the administrator console - Troubleshooting Google Meet device issues by using the administrator console - Troubleshooting network configuration issues to ensure high-quality meetings by using Google Meet - Troubleshooting Jamboards - Troubleshooting access to Google Workspace services (for example, Gmail and Drive) - Troubleshooting data visibility issues by enabling/disabling licenses or services - Investigating access issues in applications for OUs - Interpreting and responding to alerts in the Alert Center API
Data access and authentication (24% of the exam)	
Configuring policies	- Configuring:

Section	Objectives
for all devices (for example, mobile device, desktop, Chrome OS, Google Meet Hardware, Jamboard, Google Voice, and browser). Considerations include:	• Chrome user and browser policy settings • ChromeOS device policy settings (for example, Enterprise) • Windows 10 login and device policies (for example, Google Credential Provider for Windows (GCPW) • Managed Chrome browsers (for example, Chrome Browser Cloud Management) • Basic device management • Basic and advanced device management for Android and iOS • Company-owned device management for Android and iOS • Context-aware access policies • Personal device settings for Android and iOS (for example, password, advanced, device approvals, application management, and insights) - Enabling Endpoint Verification security by using BeyondCorp
Configuring and implementing Gmail DLP and sharing access control lists (ACLs) based on governance policies. Considerations include:	- Identifying areas of improvement for secure collaboration based on data exfiltration reports - Scanning emails by using Gmail DLP - Implementing Gmail DLP policies to prevent the over-sharing of sensitive data - Configuring and implementing Gmail DLP options for data classification - Configuring and implementing data classification settings on Drive - Implementing context-aware access policies based on data governance policies - Configuring settings to limit external sharing on Drive based on organizational policies - Configuring settings to limit email delivery based on organizational policies - Configuring and implementing client-side encryption services for Drive
Managing third-party applications. Considerations include:	- Implementing automatic releases of a browser extension to OUs within the domain - Implementing security configuration options for installing or using Google Cloud Marketplace applications or add-ons - Reviewing and authorizing user requests for a new Google Workspace Marketplace application, Google Play, or a Chrome extension

Section	Objectives
	- Pushing an application to a user's phone by using Google's mobile device management (MDM) - Configuring Google as a Security Assertion Markup Language (SAML) provider for a third-party application - Deploying password-vaulted apps - Deploying and restricting Google Workspace Marketplace and Google Play Store applications - Granting API access to applications - Integrating third-party user provisions - Integrating third-party marketplace applications to specific OUs in Google Workspace - Managing access to additional Google services (for example, AdSense and YouTube) for a specific set of users - Revoking third-party author access - Removing connected applications and sites
Configuring user authentication. Considerations include:	- Configuring: • 2-step Verification for the administrator and high-risk accounts (for example, requiring a physical key or not allowing SMS) • 2-step Verification for low-risk and standard accounts (for example, Google Authenticator) • Google-side connection to third-party single sign-on (SSO) providers • Google Multi-IdP options for SSO • Basic SAML SSO configuration for third-party application authentication when Google is the SSO provider • Third-party SSO for Google Workspace • Access control based on the use of the security functionality within API Controls • Google session control based on a company's legal policies - Implementing basic user security controls (for example, password length enforcement) - Implementing security aspects of identity management, perimeter security, and data protection
Supporting business initiatives (14% of the exam)	
Using Vault to support legal initiatives. Considerations	- Configuring retention rules based legal security policies (for example, setting retention rules, placing legal holds, exporting data for additional processing and review, auditing reports, and searching a domain's data by user account, OU, date, or

Section	Objectives
Include:	keyword) - Assisting with or creating: • Legal matters to hold data • Export matter content (data) for analysis • Delegation protocols for Vault access • Google Workspace content by using Vault (searching) • Legal holds for Google Workspace content by using Vault • Vault audit reports (running)
Creating and interpreting reports for the business. Considerations include:	- Generating and interpreting user adoption reports (for example, Work Insights) - Investigating issues by using the Alert Center - Investigating and monitoring a service outage for a specific Google Workspace application - Investigating issues by using data objects and metrics available within activity reports - Configuring group alerts triggered by a specific event - Creating and reviewing audit logs - Using BigQuery to combine multiple Google Workspace logs and usage reports to provide actionable insights
Supporting data import and export. Considerations include:	- Assisting with off-boarding employees and transferring data (for example, Drive, Calendar, and Google Data Studio) - Migrating Gmail data between Google Workspace accounts - Exporting data from Google Workspace offline or to other platforms

Google GCP-PGWA Sample Questions:

Question: 1

Your Communications and Training Department has a Google Site that provides updated critical business information to all employees. They want to learn how often the site is being visited and how it is used.

What should you do?

a) Embed a JavaScript page counter showing usage statistics.
b) Export the Apps Usage Activity Report showing Sites activity and send the daily report to the Communications and Training Department.
c) Add a Google Analytics Web Property ID to the Site.
d) Export the Drive Audit Log filtered to show Site Views.

Answer: c

Question: 2

A company has reports of users sharing sensitive Google Drive content outside their domain through third-party add-ons. You need to control which third-party apps are allowed to access users' G Suite data.

Which security feature should you use to achieve this?

a) OAuth Whitelisting
b) Configure DLP policies to prevent sharing of sensitive content with external parties.
c) Block specific API scopes for each user.
d) In the Drive SDK section, clear 'Allow users to access Google Drive with the Drive SDK API.'

Answer: a

Question: 3

The organization is concerned with third-party applications accessing contact information. As a G Suite Super Admin, you are tasked to restrict third-party access without limiting users' ability to share contacts manually.

What should you do?

a) Disable Contact Sharing.
b) Disable API access to Google Contacts and enable Directory Sharing.
c) Enable API access to Google Contacts and disable Directory Sharing.
d) Enable Contact Sharing.

Answer: b

Question: 4

Your company uses Google Workspace and has acquired a subsidiary that, for business reasons, will remain indefinitely on its existing third-party collaboration platform and legacy LDAP system.

This subsidiary operates autonomously with a separate, unfederated Active Directory forest. It is anticipated that interaction between the two companies will be infrequent and primarily conducted via email.

Leadership’s minimum requirement is adding employees of that subsidiary to your corporate global address book (GAL). What should you do?

a) Configure GCDS on the subsidiary LDAP to provision their users with Cloud Identity licenses on the parent domain.
b) Create a script that uses the Directory API to sync the subsidiary’s contact list as shared contacts.
c) Publish a CSV file containing the subsidiary’s directory for your users to upload into Google Contacts.
d) Provision the subsidiary users with G Suite accounts on the parent domain for the additional benefit of allowing collaboration in Drive.

Answer: b

Question: 5

Your compliance officers want to implement a new retention policy. Email will be retained for only 180 days for most users except for VIPs, who need to retain some messages indefinitely. Your VIPs' mail is already in a separate sub-organizational unit called VIPs.

Which two configurations would meet your retention needs? (Choose two.)

a) Create a custom retention rule for the root OU of 180 days.
b) Create a custom retention rule for the VIP OU of indefinite.
c) Create a default retention rule of 180 days.
d) Create a custom retention rule for the VIP OU to indefinitely retain messages with a given label.
e) Create a default retention rule for the VIP OU to indefinitely retain messages with a given label.

Answer: c, d

Question: 6

External Company is reporting that they are not receiving messages from your users. Your users are reporting that everything is sending fine and they are not receiving bounceback messages or any notifications.

You need to determine what could be causing the non-delivery and why they aren't receiving the notifications. What should you do?

a) Ask other customers on Cloud Connect Community if they are experiencing outages.
b) Using MX Toolbox, ensure that your SPF, DKIM, and DMARC records are up to date.
c) Review the affected sent messages in the email audit log.
d) Connect to the user’s mailbox and review the headers using the Google Workspace Toolbox.

Answer: c

Question: 7

An organization is pushing for an effective way to manage how users access corporate data from mobile devices.

A recent change to the organization's wireless settings is allowing WiFi access to users who have personal devices but preventing them from accessing corporate applications and data sources.

Users with company-owned devices are not experiencing the same issue. You are tasked with troubleshooting this issue. What should you do?

a) Enable Advanced Mobile Management and approve the device.
b) Disable Advanced Mobile Management and activate the device.
c) Enable Advanced Mobile Management and unblock the device.
d) Disable Advanced Mobile Management and approve the device.

Answer: a

Question: 8

A company needs to create a Google group for the customer service team. The members in that group should be able to assign and track received messages, mark a topic as resolved, and add/edit tags to a topic.

What group type should you use?

a) Web forum
b) Email List
c) Q&A Forum
d) Collaborative Inbox

Answer: d

Question: 9

Your-company. com is currently migrating to Google Workspace. Some legacy applications are still using an on-premises exchange server to send emails.

You enabled the SMTP Relay service in Google to route the messages. During an investigation it was determined that these messages are not discoverable in Google Vault.

For compliance reasons, the Legal team is requiring that these messages are retained and discoverable. What should you do?

a) Add the Exchange Server's IP as an Inbound Gateway.
b) Enable comprehensive mail storage.
c) Create a Content Compliance rule to forward a copy of every message to a Google Group.
d) Enable Gmail forwarding for exchange server.

Answer: b

Question: 10

Your company has purchased a new six-story building that has 20 meeting rooms of various sizes. One of the meeting rooms is an executive conference room that only one person should be able to see and book.

You have created that executive conference room in the Google Workspace > Calendar > Resources menu and need to restrict the sharing settings for that executive conference room.

What two actions should you take?

a) Delete the resource and create the meeting room as a secondary calendar on the person's Calendar account.
b) Show the meeting room as busy all the time so it never shows up as an available room.
c) Access the Settings of the Resource to assign the person permission to make changes.
d) Clear the options under Access Permissions in the Settings of the Resource so no one else has access.
e) Show the person how to monitor meetings scheduled in the room and how to cancel them.

Answer: c, d

Study Guide to Crack Google Professional Google Workspace Administrator GCP-PGWA Exam:

- Getting details of the GCP-PGWA syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the GCP-PGWA exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Google provided training for GCP-PGWA exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the GCP-PGWA sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on GCP-PGWA practice tests is must. Continuous practice will make you an expert in all syllabus areas.