Google Cloud

Professional Collaboration Engineer

Certification page

A Professional Collaboration Engineer transforms business objectives into tangible configurations, policies, and security practices as they relate to users, content, and integrations. Through understanding of an organization's infrastructure, they enable people to work together, communicate, and access data in a secure and efficient manner. Operating with an engineering and solutions mindset, they use tools, programming languages, and APIs to automate workflows. They also educate end users and increase operational efficiency while advocating for Google Workspace and the Google toolset.

DURATION
2 hours

LEVEL
Professional

TESTING FORMAT
Online Proctored
or Testing Center
Proctored

LANGUAGES
- English
- Japanese

This certification assesses:

- ✓ Plan and implement Google Workspace authorization and access
- ✓ Manage user, resource, and shared drive life cycles
- ✓ Control and configure Google Workspace services
- ✓ Configure and manage endpoint access
- ✓ Monitor organizational operations
- ✓ Advance Google Workspace adoption and collaboration

Recommended experience: 3+ years of industry experience including 1+ year Google Workspace (formerly G Suite) administration experience

Recommended learning path: Collaboration Engineer learning path

Certification Exam Guide

Section 1: Object management

1.1 Manage user lifecycles with provisioning and deprovisioning processes. Considerations include:

- Adding users (e.g., individual, bulk, automated)
- Removing users (e.g., suspending, deleting, recovering)
- Editing user attributes (e.g., renaming, passwords, aliases)
- Creating administrative roles (e.g., default roles, custom roles)

1.2 Configure shared drives. Considerations include:

- Transferring user data from one user to another

1.3 Manage calendar resources

1.4 Configure and manage Google Groups for Business. Considerations include:

- Configuring Google Groups
- Adding users to groups
- Implications of current Google Workspace APIs to development efforts
- Using Apps Script to automate tasks

Section 2: Service configuration

2.1 Implement and manage Google Workspace configurations based on corporate policies. Considerations include:

- Managing company profile settings
- Modifying OU policies
- Managing rollout of new Google functionality to end users
- Troubleshooting Google Workspace services (e.g., performance issues for services suite, apps for OUs)

2.2 Demonstrate how to set up and configure Gmail. Considerations include:

- Enabling email delegation for an OU
- Managing Gmail archives

Section 3: Troubleshooting

3.1 Troubleshoot user reports of mail delivery problems

3.2 Collect log files or reports needed to engage with support

3.3 Classify and mitigate basic email attacks. Considerations Include:

- Configuring attachment compliance
- Configuring blocked senders
- Configuring email allowlist
- Configuring objectionable content
- Configuring phishing settings
- Configuring spam settings
- Managing admin quarantine
- Configuring Secure Transport compliance
- Configuring safety settings

3.4 Troubleshoot workspace access and performance

Section 4: Data access and authentication

4.1 Configure policies for all devices (mobile, desktop, Chrome OS, Meet, Chrome Browser). Considerations include:

- Company-owned vs. personal devices
- Configuring personal device settings (e.g., password, Android, iOS, advanced, device approvals, app management, insights

4.2 Configure and implement data governance policies

4.3 Describe how to manage third-party applications. Considerations include:

- Configuring third-party SSO for Google Workspace
- Integrating with third-party for provisioning
- Integrating third-party marketplace apps to specific OUs in Google Workspace
- Granting API access to applications that need access
- Revoking third-party author access
- Removing connected applications and sites

4.4 Configure user authentication. Considerations include:

- Basic user security controls (e.g., password length enforcement and 2-Step Verification)
- Security aspects of identity, perimeter security, and data protection

---

Section 5: Support business initiatives

5.1 Use Vault to assist legal teams. Considerations Include:

- Setting retention rules (e.g., Setting retention rules, placing legal holds, searching your domain's data by user account, OU, date, or keyword, exporting data for additional processing and review, auditing reports)

- Holding and exporting data
- Running Vault audit reports

5.2 Interpret reports for the business. Considerations Include:

- Scanning email with Data Loss Prevention (DLP)
- Managing content compliance rules
- Configuring security and data region
- Monitoring security health check
- Configuring security settings
- Creating security records
- Designing security integration and addressing objections

5.3 Describe how to import and export data