Google Cloud Professional Collaboration Engineer

Introduction

A Professional Collaboration Engineer transforms business objectives into tangible configurations, policies, and security practices as they relate to users, content, and integrations. Collaboration Engineers leverage their understanding of their organization's mail routing and identity management infrastructure to enable efficient and secure communication and data access. Operating with an engineering and solutions mindset, they use tools, programming languages, and APIs to automate workflows. They look for opportunities to educate end-users and increase operational efficiency while advocating for Google Workspace and the Google toolset.

The Professional Collaboration Engineer exam assesses your ability to:

- Plan and implement Google Workspace authorization and access
- Manage user, resource, and Shared Drive lifecycles
- Manage mail
- Control and configure Google Workspace services
- Configure and manage endpoint access
- Monitor organizational operations
- Advance Google Workspace adoption and collaboration

Course Objective

This course teaches you about core aspects such as;

- Planning and implementing multiple applications with G workshops
- Synchronizing and managing resources and Shared drives
- Managing mail
- Administering and configuring Google Workspace services
- Configuring and managing vault including multiple activities
- Setting up and using operational reports
- Building business solutions and processes

Course Outline

1. Planning and implementing Google Workspace authorization and access

1.1 Implementing authorization policies. Considerations include:

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

1.2 Using Google Workspace as a service provider. Considerations include:

- Configuring third-party SSO for Google Workspace
- Integrating with the third party for provisioning

1.3 Using Google Workspace as an identity provider. Considerations include:

- Configuring and managing SSO for common third-party applications
- Configuring and managing to provision

1.4 Managing access to third-party applications and sites. Activities include:

- Granting API access to applications that need access
- Revoking third-party OAuth access
- Removing connected applications and sites

2. Managing user, resource, and Shared Drive lifecycles

2.1 Managing users. Considerations include:

- Adding users (e.g., individual, bulk, automated)
- Removing users (e.g., suspending, deleting, recovering)
- Transferring user data from one user to another
- Editing user attributes (e.g., renaming, passwords, aliases)
- Creating administrative roles (e.g., default roles, custom roles)
- Managing user licenses (e.g., licensing models, Google Workspace SKUs)
- Troubleshooting conflicting accounts
- Implications of current Google Workspace APIs to development efforts
- Using Google Apps Script to automate tasks

2.2 Synchronizing data in your Google domain with your Microsoft® Active Directory® or LDAP server. Considerations include:

- Integrating LDAP with Google Workspace
- Configuring and troubleshooting GSPS and GCDS
- Implications of current Google Workspace APIs to development efforts
- Using Apps Script to automate tasks

2.3 Managing organizational structure. Considerations include:

- Designing efficient organizational unity (OU) structure based on business needs
- Assigning users to relevant OUs
- Modifying OU policies
- Implications of current Google Workspace APIs to development efforts
- Using Apps Script to automate tasks
- Managing and verifying domains
- Using Google Takeout to export data
- Managing company profile settings

2.4 Managing groups. Considerations include:

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

2.5 Managing contacts. Considerations include:

- Creating contacts
- Sharing contacts
- Implications of current Google Workspace APIs to development efforts
- Using Apps Script to automate tasks

3. Managing mail

3.1 Managing mail-related DNS settings. Activities include:

- Managing domain MX records
- Managing domain SPF records
- Managing domain DKIM records
- Managing domain DMARC records

3.2 Diagnosing and resolving mail routing issues. Considerations include:

- Analyzing mail flow
- Analyzing email headers
- Email log search
- Disparate email services
- Using Google Workspace Toolbox

3.3 Configuring and managing security, compliance, and spam rules. Activities include:
- Configuring attachment compliance
- Configuring blocked senders
- Configuring email allow a list
- Configuring objectionable content
- Configuring phishing settings
- Configuring spam settings
- Managing admin quarantine
- Configuring secure transport compliance
- Configuring safety settings

3.4 Configuring mail routing rules. Considerations include:

- Configuring split and dual delivery scenarios
- Implications of integrating third-party mail services
- Configuring routing rules
- Configuring recipient map
- Configuring non-Gmail mailbox
- Configuring hosts

3.5 Configuring general mail settings. Activities include:

- Configuring append footer setting
- Configuring forwarding
- Configuring SMTP relay
- Enabling email delegation for an OU
- Disabling IMAP and POP
- Managing Gmail archives

4. Controlling and configuring Google Workspace services:

4.1 Administering Google Workspace Services. Activities include:

- Managing rollout of new Google functionality to end-users
- Troubleshooting Google Workspace services (e.g., performance issues for services suite, Google Workspace apps for OUs)
- Configuring services

4.2 Configuring and managing Google Workspace core apps. Considerations include:

- Contacts/Directory (e.g., ability to make updates to Directory services or contact support or contacts sharing settings)
- Calendar (e.g., Calendar sharing settings and delegations, Calendar resource management, Calendar invitations sent to Groups, troubleshooting calendar interoperability)
- Drive/Shared Drive (e.g., storage limitations in Basic plan)
- Groups (e.g., creating and editing groups, banning group members from posting to the group)
- Chat/Meet (e.g., disabling Hangouts voice calls for organization, designing video conferencing integration of Hangouts with different endpoints, disabling bot access on new Hangouts chat)
- Sites (e.g., usage and implementation)

4.3 Managing services integrations. Activities include:

- Integrating third-party marketplace apps to specific OUs in Google Workspace
- Evaluating Marketplace and Connected app landscape
- Adding SP to Cloud Identity

4.4 Implementing automation. Considerations include:

- API permissions
- Able to interact with APIs and lightweight scripting
- Service Accounts

5. Configuring and managing content access

5.1 Configuring and managing Vault. Activities 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 Configuring and managing Drive and Shared Drive. Activities include:

- Configuring sharing settings (e.g., updating sharing settings to external domains, controlling file access with Information Rights Management)
- Managing Drive folder structure (e.g., using Google Drive native file formats, recommending Google Drive and Shared Drive file structures)

5.3 Ensuring compliance with regulatory requirements. Activities include:

- Scanning email with Data Loss Prevention (DLP)
- Managing content compliance rules

5.4 Implementing and monitoring data security. Activities include:

- Configuring security and data region
- Monitoring security health check
- Configuring security settings
- Creating security records
- Designing security integration and addressing objections.

5.5 Managing third-party applications and access. Activities include:

- Backing up solutions of Google Workspace data for compliance
- Allow list OAuth apps

6. Configuring and managing endpoint access

6.1 Configuring mobile devices. Considerations include:

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

6.2 Provisioning, deprovisioning, and enabling Chrome devices

6.3 Managing Google meeting room hardware (e.g., provisioning, deprovisioning, hanging up, calling, rebooting)

6.4 Managing Chrome apps, extensions, and Android apps

6.5 Configuring network settings (e.g., Wi-Fi, Ethernet, VPN, certificates, and general)

7. Monitoring organizational operations

7.1 Setting up and using reports (e.g., creating usage reports, measuring adoption and satisfaction)

7.2 Setting up and using audits (e.g., auditing document sharing, auditing Gmail and drive, auditing users)

7.3 Interpreting report and audit data and taking appropriate action. Examples include:

- Troubleshooting and escalating support issues to Google Partner support or Google Engineering
- Troubleshooting error logs
- Identifying data leakage scenarios and implementing ways to prevent
- Streaming audit data to BigQuery

7.4 Managing alerts (e.g., suspicious logging activity, apps outages, TLS failure, user deleted)

8. Advancing Google Workspace adoption and collaboration

8.1 Building business solutions and processes. Examples include:

- Creating simple processes using Apps Script
- Creating team project sites

8.2 Staying up-to-date with Google Workspace. Examples include:

- Using Google and partner support channels
- Accessing and interpreting Google Workspace roadmap
- Staying aware of new features and functionality in Google Workspace

Prerequisites

There are no formal prerequisites required for taking this certification course.

Recommended Experience

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

Target Audience

This certification is intended for;

- Engineers who successfully wish to collaborate and establish an efficient and secure data flow with GCP
- People preparing for the Google Collaboration Engineer exam
- Software Engineers
- Network Engineer
- Cloud Developers
- System Engineers

Duration

3 days training course