

# Professional Cloud DevOps Engineer

## Certification exam guide

A Professional Cloud DevOps Engineer implements processes and capabilities throughout the systems development lifecycle using Google-recommended methodologies and tools. They enable efficient software and infrastructure delivery while balancing reliability with delivery speed. They optimize and maintain production systems and services.

### **Section 1: Bootstrapping and maintaining a Google Cloud organization (~15% of the exam)**

1.1 Designing the overall resource hierarchy for an organization. Considerations include:

- Projects and folders
- Shared networking
- Multi-project monitoring and logging
- Identity and Access Management (IAM) roles and organization-level policies
- Creating and managing service accounts
- Organizing resources by using an application-centric approach (e.g., App Hub)

1.2 Managing infrastructure. Considerations include:

- Infrastructure-as-code tooling (e.g., Cloud Foundation Toolkit, Config Connector, Terraform, Helm)
- Making infrastructure changes using Google-recommended practices and blueprints
- Automation with scripting (e.g., Python, Go)

1.3 Designing a CI/CD architecture stack in Google Cloud, hybrid, and multi-cloud environments. Considerations include:

- Continuous integration (CI) with Cloud Build
- Continuous delivery (CD) with Cloud Deploy, including Kustomize and Skaffold
- Widely used third-party tooling (e.g., Jenkins, Git, Argo CD, Packer)
- Security of CI/CD tooling

# Google Cloud

1.4 Managing multiple environments (e.g., staging, production). Considerations include:

- Determining the number of environments and their purpose
- Managing ephemeral environments
- Configuration and policy management
- Managing Google Kubernetes Engine (GKE) clusters across an enterprise
- Safe and secure patching and upgrading practices

1.5 Enabling secure cloud development environments. Considerations include:

- Configuring and managing cloud development environments (e.g., Cloud Workstations, Cloud Shell)
- Bootstrapping environments with required tooling (e.g., custom images, IDE, Cloud SDK)
- Leveraging AI to assist with development and operations (e.g., Cloud Code, Gemini Code Assist)

## **Section 2: Building and implementing CI/CD pipelines for applications and infrastructure (~27% of the exam)**

2.1 Designing and managing CI/CD pipelines. Considerations include:

- Artifact management with Artifact Registry
- Deployment to hybrid and multi-cloud environments (e.g., GKE Enterprise)
- CI/CD pipeline triggers
- Testing a new application version in the pipeline
- Configuring deployment processes (e.g., approval flows)
- CI/CD of serverless applications
- Applying CI/CD practices to infrastructure (e.g., GKE clusters, managed instance groups, Cloud Service Mesh configuration)

2.2 Implementing CI/CD pipelines. Considerations include:

- Auditing and tracking deployments (e.g., Artifact Registry, Cloud Build, Cloud Deploy, Cloud Audit Logs)
- Deployment strategies (e.g., canary, blue/green, rolling, traffic splitting)
- Troubleshooting and mitigating deployment issues

2.3 Managing CI/CD configuration and secrets. Considerations include:

- Key management (e.g., Cloud Key Management Service)
- Secret management (e.g., Secret Manager, Certificate Manager)
- Build versus runtime secret injection

2.4 Securing the CI/CD deployment pipeline. Considerations include:

- Vulnerability analysis with Artifact Registry
- Software supply chain security (e.g., Binary Authorization, Supply-chain Levels for Software Artifacts [SLSA] framework)
- IAM policies based on environment

## **Section 3: Applying site reliability engineering practices to applications (~23% of the exam)**

3.1 Balancing change, velocity, and reliability of the service. Considerations include:

- Defining SLIs (e.g., availability, latency), SLOs, and SLAs
- Error budgets
- Opportunity cost of risk and reliability (e.g., number of “nines”)

3.2 Managing service lifecycle. Considerations include:

- Service management (e.g., introduction of a new service by using a pre-service onboarding checklist, launch plan, or deployment plan, deployment, maintenance, and retirement)
- Capacity planning (e.g., quotas, limits)
- Autoscaling (e.g., managed instance groups, Cloud Run, GKE)

3.3 Mitigating incident impact on users. Considerations include:

- Draining/redirecting traffic
- Adding capacity
- Rollback strategies

## Section 4: Implementing observability practices (~20% of the exam)

### 4.1 Managing logs. Considerations include:

- Collecting and importing logs (e.g., Cloud Logging agent, Cloud Audit Logs, VPC Flow Logs, Cloud Service Mesh)
- Logging optimization (e.g., filtering, sampling, exclusions, cost, source considerations)
- Exporting logs (e.g., BigQuery, Pub/Sub, for auditing)
- Retaining logs
- Analyzing logs
- Handling sensitive data (e.g., personally identifiable information [PII], protected health information [PHI])

### 4.2 Managing metrics. Considerations include:

- Collecting and analyzing metrics (e.g., application, platform, networking, Cloud Service Mesh, Google Cloud Managed Service for Prometheus, hybrid/multi-cloud)
- Creating custom metrics from logs
- Using Metrics Explorer for ad hoc metric analysis
- Creating synthetic monitors

### 4.3 Managing dashboards and alerts. Considerations include:

- Managing dashboards (e.g., creating, filtering, sharing, playbooks)
- Configuring alerting and alerting policies (e.g., SLIs, SLOs, cost control)
- Widely used third-party alerting tools

## Section 5: Optimizing performance and troubleshooting (~15% of the exam)

### 5.1 Troubleshooting issues. Considerations include:

- Infrastructure issues
- Application issues
- CI/CD pipeline issues
- Observability issues
- Performance and latency issues

5.2 Implementing debugging tools in Google Cloud. Considerations include:

- Application instrumentation
- Cloud Trace
- Error Reporting

5.3 Optimizing resource utilization and costs. Considerations include:

- Observability costs
- Spot virtual machines (VMs)
- Infrastructure cost planning (e.g., committed-use discounts, sustained-use discounts, network tiers)
- Google Cloud recommenders (e.g., cost, security, performance, manageability, reliability)