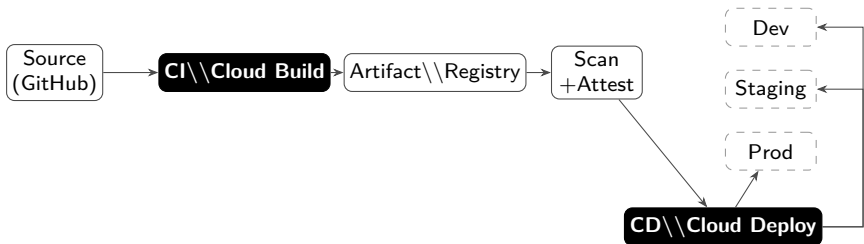




CI/CD Pipelines & Supply Chain Security

GCP Professional Cloud DevOps Engineer | Cloud Build, Cloud Deploy, Binary Authorization & SLSA

CI/CD Architecture on GCP



End-to-End CI/CD Pipeline

Cloud Build	CI service. Build, test, containerize. Triggers on git events. cloud-build.yaml defines steps. Private pools for VPC access.
Artifact Registry	Store Docker images, language packages. Vulnerability scanning (on-push + continuous). Regional or multi-regional.
Cloud Deploy	CD service. Delivery pipelines with ordered targets. Supports: canary, blue-green, rolling. Approval gates. Automatic rollback.
Scaffold	Cloud Deploy uses Scaffold for rendering manifests. scaffold.yaml defines build and deploy config. Render > deploy > verify.

Cloud Build Advanced

- 1 Parallel steps: multiple steps with same waitFor can run concurrently
- 2 Conditional execution: use bash if/then or Cloud Build --substitutions for branching
- 3 Build caching: kaniko cache for Docker layer caching, reducing build times
- 4 Build notifications: Pub/Sub on build status change. Trigger Slack, JIRA, etc.
- 5 Service account per trigger: different permissions for PR vs main branch builds

Cloud Build Artifact Registry Cloud Deploy Binary Auth

Cloud Deploy Strategies

Strategy	How	Verify	Rollback
Rolling	Update pods gradually	Health checks	Roll back to previous release
Canary	% traffic to new version	Cloud Monitoring metrics	Auto-rollback on failure
Blue-Green	Full parallel env, switch	Smoke tests on green	Switch back to blue

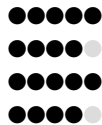
Delivery pipeline	YAML config. Defines progression: [dev, staging, prod]. Each target maps to a GKE cluster or Cloud Run service.
Promotion	Move a release from one target to next. Manual (gcloud deploy releases promote) or automatic with approval.
Canary deployment	Define canary percentage phases (10%, 25%, 50%, 100%). Verify at each phase with Cloud Monitoring SLOs.
Deploy hooks	Pre-deploy and post-deploy hooks. Run verification jobs (integration tests, smoke tests) before promoting.
Automation rules	Auto-promote when SLO targets are met. Auto-rollback when SLO is violated. Advance/Rollback based on Cloud Monitoring.

Canary deployment safety

Blue-green speed

Rolling update simplicity

Rolling update zero-downtime



Supply Chain Security



Software Supply Chain Security

SLSA (Supply-chain Levels for Software Artifacts)	Framework for supply chain integrity. Levels 1-4: from basic provenance to hermetic builds with two-party review. Cloud Build achieves SLSA L3.
Binary Authorization	Enforce deploy-time policy. Require attestations (signatures) on container images. Block unsigned images from GKE/Cloud Run.
Attestors	Entities that verify images. Cloud Build can auto-attest. Create attestors for: vulnerability scan pass, code review approval.
Assured Open Source Software	Google-curated OSS packages. Scanned, tested, signed by Google. Reduces risk from open-source dependencies.
Container Analysis	Vulnerability scanning in Artifact Registry. CRITICAL/HIGH/MEDIUM/LOW findings. Integrate into CI: fail build on CRITICAL.

- Enforce: only images from specific Artifact Registry repos can deploy
- Break-glass: emergency bypass for Binary Authorization with audit logging
- SBOM: Software Bill of Materials generation during build for dependency tracking
- VEX: Vulnerability Exploitability eXchange for prioritizing vulnerability remediation

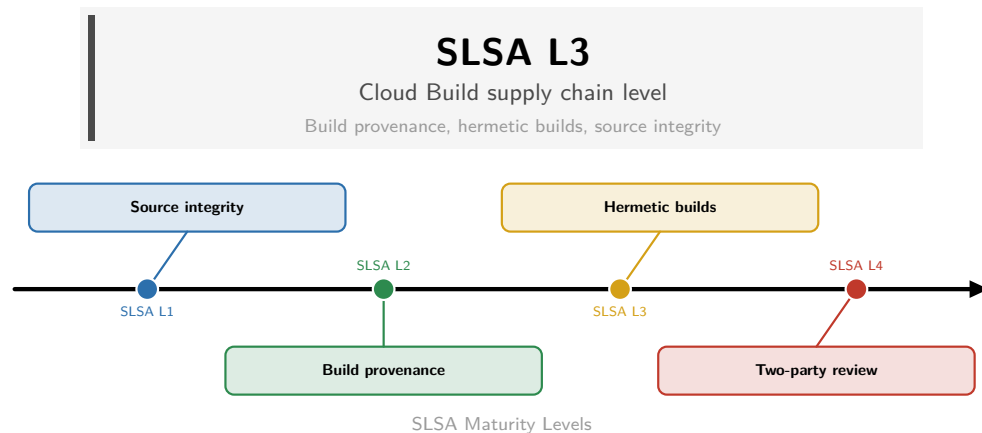
⚠ Security

Apply principle of least privilege. Use service accounts, not user accounts for workloads.

Infrastructure as Code

Terraform	Declarative IaC. HCL language. State in GCS backend. Google provider for all GCP resources. Modules for reusability.
Config Connector	Manage GCP resources via Kubernetes CRDs. Apply with kubectl. State in K8s. Good for GKE-centric teams.
Pulumi	IaC with general-purpose languages (Python, TypeScript, Go). Alternative to Terraform for teams preferring code over HCL.
GitOps	Git as source of truth for infrastructure. Config Sync (Anthos) auto-applies K8s manifests from Git repo. ArgoCD alternative.

- Terraform CI/CD: plan on PR, apply on merge. Use Cloud Build for automation
- State locking: GCS backend with locking prevents concurrent modifications
- Module registry: registry.terraform.io/GoogleCloudPlatform for Google-maintained modules
- Policy as code: Sentinel (Terraform Cloud) or OPA/Gatekeeper (GKE) for compliance enforcement



Official resources

⚠ Check the current exam guide

Google Cloud is updating its exams to the products announced at Google Cloud Next '26 (Gemini Enterprise Agent Platform, the data and analytics stack), per the certification hub checked 2026-10-05: read the current exam guide before these sheets.

- [1] **Professional Cloud DevOps Engineer exam guide**
Google Cloud · accessed 2026-10-05 · services.google.com/fh/files/misc/profession...ops_engineer_exam_guide_english.pdf
Supports: domains and topics
- [2] **Professional Cloud DevOps Engineer certification page**
Google Cloud · accessed 2026-10-05 · cloud.google.com/learn/certification/cloud-devops-engineer
Supports: format, price, sample questions link, renewal
- [3] **Professional Cloud DevOps Engineer learning path**
Google Skills · accessed 2026-10-05 · skills.google/paths/20
Supports: Google Skills (ex Cloud Skills Boost)
- [4] **gcloud CLI cheat sheet**
Google Cloud · accessed 2026-10-05 · cloud.google.com/sdk/docs/cheatsheet
Supports: the commands on one page
- [5] **Site Reliability Engineering books**
Google · accessed 2026-10-05 · sre.google/books
Supports: SRE, workbook: SLOs, error budgets
- [6] **Cloud Build documentation**
Google Cloud · accessed 2026-10-05 · cloud.google.com/build/docs
Supports: CI
- [7] **Cloud Deploy documentation**
Google Cloud · accessed 2026-10-05 · cloud.google.com/deploy/docs
Supports: CD to GKE / Cloud Run
- [8] **Cloud Monitoring documentation**
Google Cloud · accessed 2026-10-05 · cloud.google.com/monitoring/docs
Supports: SLO monitoring, alerting

8 sources · 3 publishers · last accessed 2026-10-05