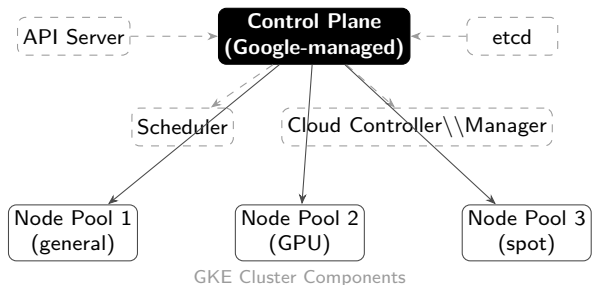




GKE Architecture

GCP Kubernetes & GKE | Cluster Modes, Node Pools, Networking & Security

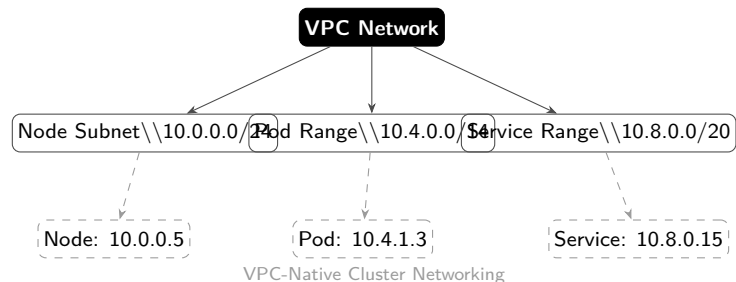
GKE Cluster Architecture



Feature	GKE Standard	GKE Autopilot
Node management	You create/manage node pools	Google auto-manages nodes
Pricing	Pay per node (VM)	Pay per pod CPU/mem/GPU
Security	You harden (CIS, PSP)	Pre-hardened, restricted
Node access	SSH, privileged pods allowed	No SSH, restricted pods
GPU/TPU	Full control via node pools	Supported with constraints
Scaling	Cluster autoscaler + NAP	Fully automatic
SLA	99.5% (zonal), 99.95% (regional)	99.9% (regional)
Best for	Custom configs, GPU, compliance	Most production workloads



Cluster Networking



VPC-native clusters	Pods get IPs from VPC secondary ranges (alias IPs). Required for Autopilot, private clusters, and most features.
Private cluster	Nodes have internal IPs only. Control plane accessible via authorized networks or Private Service Connect. Most secure option.
Authorized networks	Restrict control plane API access to specific CIDR ranges. Use with private clusters for maximum security.
Network policies	Kubernetes NetworkPolicy (Calico). Restrict pod-to-pod traffic by namespace, label, IP, port. Default: allow all.
Dataplane V2	eBPF-based networking (Cilium). Faster than iptables. Built-in network policy enforcement. Default for new clusters.
Services	ClusterIP (internal), NodePort (port on each node), LoadBalancer (provisions GCP LB). Ingress for L7 HTTP routing.

GKE Ingress & Gateway

Resource	Load Balancer	Use Case
Ingress (GKE)	External Application LB	External HTTP(S) routing
Internal Ingress	Internal Application LB	Internal microservices
Gateway API	Various (configurable)	Multi-tenant, advanced routing
NEG (Network Endpoint Group)	Direct pod routing	Container-native LB

Cluster Security

Workload Identity	Map K8s ServiceAccount to GCP ServiceAccount. Pods authenticate as GCP SA. No key files. Required for secure GKE workloads.
Binary Authorization	Only signed container images can deploy. Attestors verify images. Break-glass for emergencies.
GKE Sandbox (gVisor)	Kernel-level sandboxing for untrusted workloads. Extra isolation layer between containers and host kernel.
Pod Security Standards	Kubernetes-native security policies. Privileged, Baseline, Restricted profiles. Enforced at namespace level.
Shielded GKE Nodes	Secure Boot, vTPM on nodes. Verify node integrity. Protects against rootkits. Default for Autopilot.
Secret encryption	Encrypt K8s Secrets at rest with Cloud KMS (CMEK). Application-layer encryption on top of default etcd encryption.

- Use namespaces for multi-tenant isolation. Apply RBAC, network policies, resource quotas per namespace
- Scan images in Artifact Registry for vulnerabilities before deployment
- Enable GKE Security Posture Dashboard for visibility into cluster security
- Private clusters + authorized networks + Workload Identity = security baseline



GKE Security Layers

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

GKE Enterprise (Multi-Cluster)

Fleet management	Register clusters into a fleet. Manage multiple clusters (GKE, on-prem, multi-cloud) as one logical group.
Config Sync	GitOps for fleet. Sync Kubernetes configs from Git repo to all fleet clusters. Enforce consistency.
Policy Controller	OPA Gatekeeper-based policy enforcement. Define constraints (e.g., require labels, block privileged pods). Fleet-wide.
Multi-Cluster Services (MCS)	Expose Services across fleet clusters. Multi-cluster Ingress for global L7 routing across clusters.
Anthos Service Mesh	Managed Istio-based service mesh. mTLS between services, traffic management, observability. Fleet-wide mesh.
Connect Gateway	Securely access registered clusters via Google Cloud. No VPN needed. IAM-authenticated kubectl access.

F

Fleet Management

CS

Config Sync

PC

Policy Controller

MCS

Multi-Cluster Svc

ASM

Anthos Svc Mesh

CG

Connect Gateway

99.9%

Autopilot SLA

99.95%

Regional Standard SLA

99.5%

Zonal Standard SLA

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.

SERVICE	docs	reference	pricing	
Google Kubernetes Engine	docs	reference	Pricing	3/3
GKE Autopilot	docs	---	---	1/3
Kubernetes	docs	reference	---	2/3
gcloud CLI	docs	reference	---	2/3
Artifact Registry	docs	---	Pricing	2/3
per kind	5/5	3/5	2/5	

10 of 15 documentation links (67% coverage) · greyed: no official page given