Customers run MinIO on Google Kubernetes Engine (GKE) for three reasons.

01.

MinIO serves as a consistent storage layer in a hybrid-cloud or multi-cloud deployment scenario.

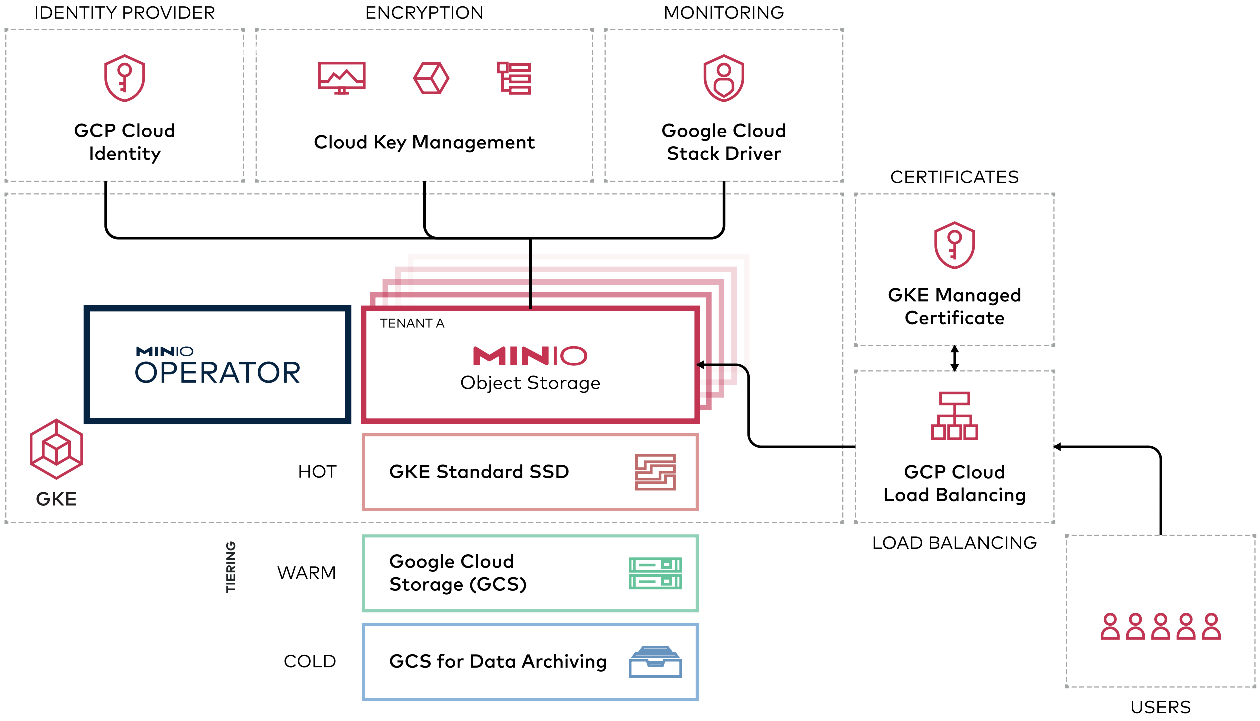
02.

MinIO is Kubernetes native and high performance it can deliver predictable performance across public, private and edge cloud environments.

03.

Running MinIO on GKE provides control over the software stack with the attendant flexibility necessary to avoid cloud lock-in.

Google Kubernetes Engine (GKE) offers a highly automated secure and fully managed Kubernetes platform. GKE leverages a high-availability control plane to support multi-zonal and regional clusters. MinIO Operator integrates natively with GKE using standard Kubernetes constructs like StorageClass and Annotations.



MinIO provides a portable high-performance object storage system across all of the major Kubernetes platforms (AWS, Azure, Tanzu, OpenShift). Developers can easily get an Amazon S3 compatible persistent storage service for all of their cloud native applications running on GKE. Unlike AWS S3, MinIO enables the applications to scale across any multi-cloud and hybrid cloud infrastructure, without requiring expensive software rewrites or proprietary integrations.

MinIO Operator integrates natively with GKE and GCP features to provide:

Storage Classes and Tiering

Tier across GKE Standard SSD, Google Cloud Storage and GCS for Data Archiving.

The key requirement to deploy MinIO at scale on GKE and GCP is the ability tier across storage classes (SSD, GCS, GCS for Data Archive). This allows enterprises to manage both cost and performance.

MinIO can be configured to automatically transition aged objects from the fast SSD tier to a more cost-efficient GCS tier and even the cost-optimized GCS for Data Archive storage tier. For example, MinIO tiering policy can be configured with SSD as the primary tier, GCS as the secondary tier and GCS for Data Archive as the tertiary, or archival tier.

When tiering, MinIO maintains a single object storage namespace by transparently retrieving transitioned objects without additional client-side logic. MinIO also supports using the S3 restore API for bringing objects back onto the "hot" performance-optimized storage infrastructure.

This same capability also extends to hybrid cloud environments where the JBOD/JBOF act as the hot tier on the private cloud side and GCS acts as the warm and cold tier. The data on the public cloud remains encrypted - ensuring that data is safe at rest and in flight.

Encryption Key Management

Manage encryption keys with GCP Cloud Key Management.

MinIO recommends using Google Cloud Key Management to store keys outside of the object storage system. For those with more stringent security requirements or for consistency purposes, MinIO integrates with a number of external Key Management Services that operate outside of GCP.

For all production environments we recommend enabling encryption on all buckets by default. MinIO uses AES-256-GCM or ChaCha20-Poly1305 encryption to protect data integrity and confidentiality with negligible performance impact.

MinIO supports setting a bucket-level default encryption key in the KMS with support for AWS-S3 semantics (SSE-S3). Clients can also specify a separate key on the KMS using SSE-KMS request headers.

MinIO will use this KMS to bootstrap its internal key encryption server (KES service) to enable high-performance, per object encryption. Each tenant runs its own KES server in an isolated namespace.

External Load Balancing

Load balance incoming requests with GCP Cloud Load Balancing.

The MinIO Operator integrates tightly with GCP Cloud Load Balancing (CLB) to provide automatic load balancing and routing service across multiple MinIO tenants for applications accessing the storage service from outside of GKE. Exposing a MinIO tenant to external traffic can be done by simply adding annotations to a MinIO tenant.

Identity Management

Manage identity and policy with GCP Cloud Identity

When running MinIO on GCP GKE, customers can manage single sign-on (SSO) through Google's hosted GCP Cloud Identity or third party OpenID Connect/LDAP compatible identity providers like Okta/Auth0, Google, Facebook, Keycloak, ActiveDirectory and OpenLDAP.

A single, centralized IDP allows administrators to add, change privileges for, or eliminate a user, service account, or group once - and have it be enforced across all public cloud, private cloud and edge MinIO servers. The ability to have a unified identity and access management (IAM) layer independent of the infrastructure provides significant architectural flexibility.

Certificate Management

Configure and manage certificates with GKE Managed Certificates.

All traffic from the application to MinIO, including internode traffic, is encrypted with TLS. TLS certificates are used to secure network communications and establish the identity of network-connected resources, such as a MinIO Server.

MinIO integrates with GKE Managed Certificates to configure, provision, manage and update certificates for the MinIO tenants. The tenants are completely isolated from each other in their own Kubernetes namespace with their own certificates for improved security.

Logging and Auditing

Output logs to GCP Cloud Logging or an Elastic Stack for analysis.

Enabling MinIO auditing generates a log for every operation on the object storage cluster. In addition to the audit log, MinIO also logs console errors for operational troubleshooting purposes.

MinIO recommends outputting logs to GCP Cloud Logging or an Elastic Stack depending on architectural goals.

Monitoring and Alerting

Track metrics and issue alerts using Google Cloud Stackdriver.

GCP provides robust monitoring capabilities for GKE using Google Cloud Stackdriver. We recommend using Google Cloud Stackdriver as a Prometheus-compatible system for monitoring and alerting when deploying MinIO on GKE. The reason for this recommendation is that MinIO publishes every object storage related Prometheus metric imaginable, from bucket capacity to access metrics. Those metrics can be collected and visualized in any Prometheus-compatible tool (Stackdriver being native to GCP) or in the MinIO Console.

Monitoring services scrape the MinIO Prometheus endpoint at regular intervals. These same tools can also be used to establish baselines and set alert thresholds for notifications, which can then be routed to a notification platform such as PagerDuty or Freshservice.

MinIO offers the most deployment options of any object storage across hybrid, multicloud and edge environments using Kubernetes. Google Kubernetes Engine users can quickly and easily deploy multi-tenant MinIO object storage within their existing environment.

The MinIO Kubernetes Operator supports end-to-end configuration and deployment of MinIO tenants, seamlessly integrating with supporting infrastructure for storage tiering, monitoring, audit logging, identity management, certificate management, key management for automatic server-side object encryption and load balancing and ingress.

Learn more at **min.io** or try it for yourself at **min.io/download**. Join the conversation at **minio.slack.com**.