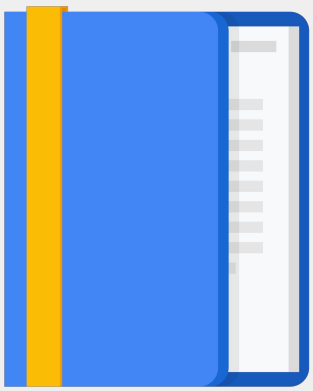
Architecting Hybrid Infrastructure with Anthos

Managing Hybrid Clusters using Kubernetes Engine

Agenda



- **Anthos Compute Layer**
- GKE On Prem Architecture
- Network Connectivity

Google Cloud

Containers and Kubernetes as a Compute Layer

Platform independence

Write once, run anywhere

Support a wide variety of application workloads

Kubernetes is the most popular, open source orchestrator for containers

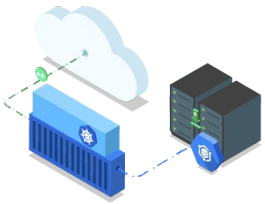
Google Kubernetes Engine

- Fully Managed, production-ready Kubernetes environment
- Operate Seamlessly with High Availability and SLA
- Runs Certified Kubernetes ensuring portability across clouds and on-premises.
- Auto node repair, auto upgrade, auto scaling
- Regional clusters for high availability with multiple masters

Google Cloud

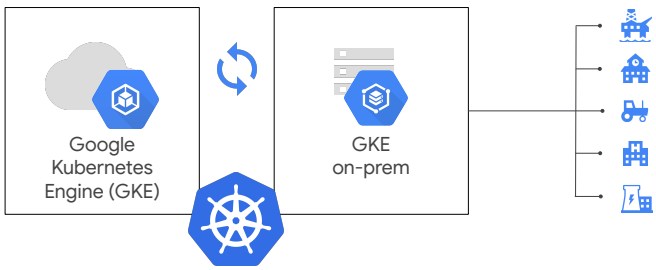
GKE On-Prem

- Turn-key, production-grade, conformant Kubernetes with best-practice configuration
- Automatic node management functionality
- Easy upgrade path to the latest Kubernetes releases that have been validated and tested by Google
- Based on a software stack, no need to buy new hardware
- Integrated Istio, Knative and Marketplace Solutions, as well as GCP Container services like Cloud Build, Container Registry, Logging and Monitoring, and more.



GKE On-Prem and GKE

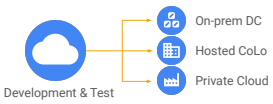
- Identity and access management based on Cloud Identity or on premises identity provider
- Secure connection across environments without the need for complicated VPNs
- Multi-cluster dashboard



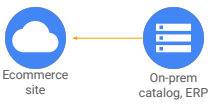
Cluster Sprawl Across Environments

Cloud Bursting

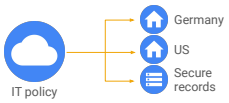
Cross-environment execution



Invoke legacy dependencies



Jurisdictional / Data Sovereignty

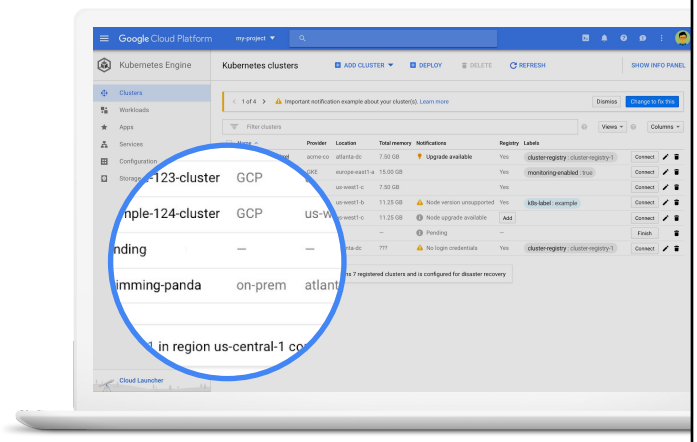


Invoke cloud services

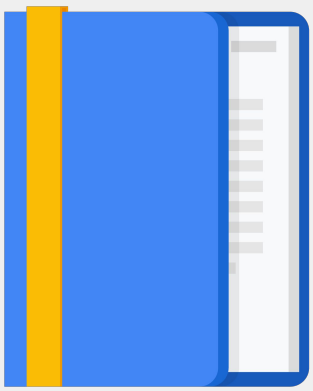
Multi-Site Deployment

GKE Dashboard

- Orchestrate and manage on-prem containers just like GKE in the cloud
- Consistent operating model with access to GCP services across hybrid environments
- Single-pane-of-glass for multiple Kubernetes clusters, no matter where



Agenda



- Anthos Compute Layer
- **GKE On Prem Architecture**
- Network Connectivity

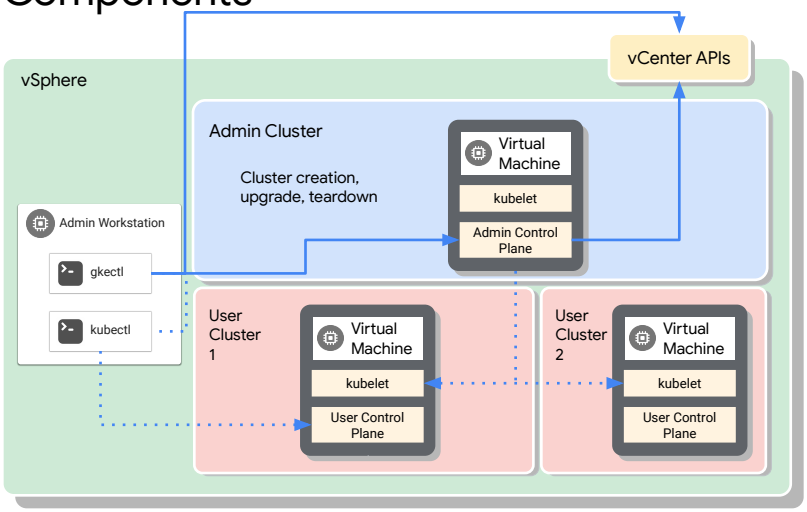
Google Cloud

GKE On-Prem Components

Admin Cluster

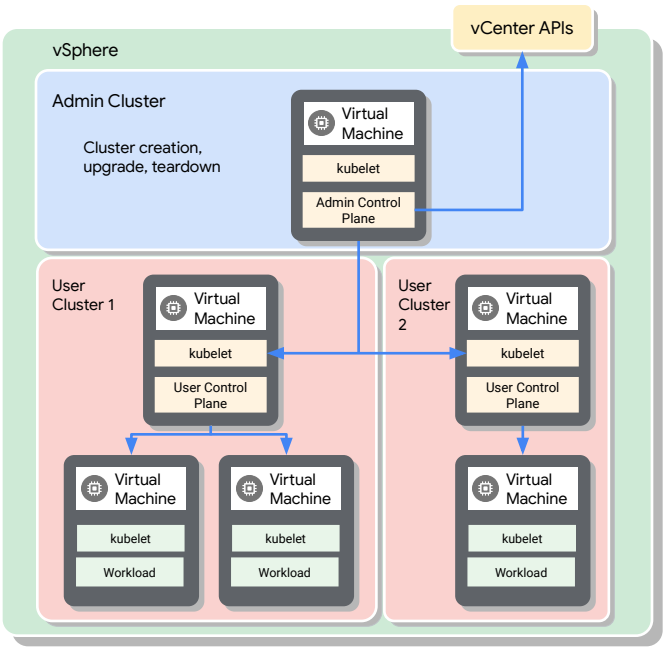
- Control plane handles all administrative API calls to and from GKE On-Prem

- Utilizes `gkectl` which is responsible for:
  - Cluster creation, management, and deletion
  - Troubleshooting
  - Capturing and exporting cluster logs



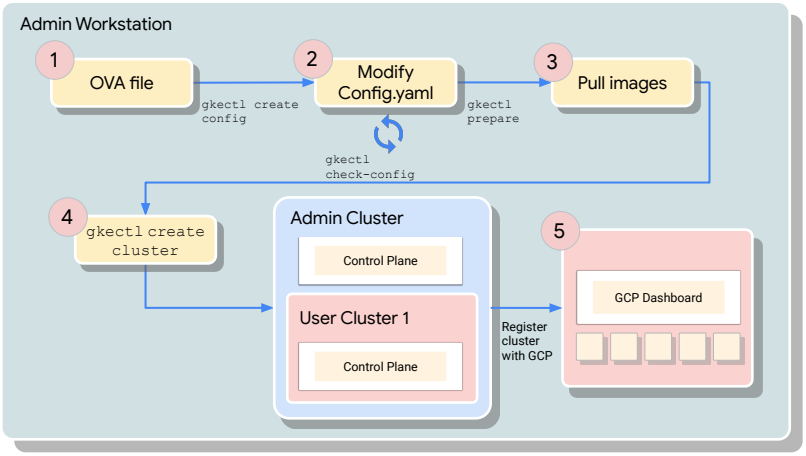
GKE On-Prem Components

- User Cluster
- One or more Kubernetes clusters running on premise on vSphere
- Control plane is part of and fully managed by the Admin Cluster which
  - Manage the machines that run the user cluster control planes
  - Create, update, and delete the control plane components
  - Expose the Kubernetes API server to the user cluster
  - Manage cluster certificates

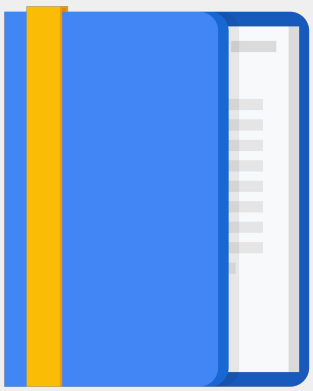


GKE On-Prem Installation

- Automated deployment on top of vSphere shipped as a virtual appliance
- Simple CLI installation with local masters
- DHCP or Static IP allocation support
- Integration with existing private or public container registry



Agenda

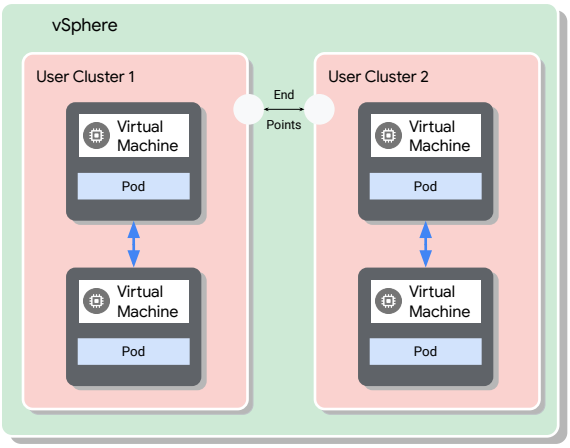


- Anthos Compute Layer
- GKE On Prem Architecture
- **Network Connectivity**

Google Cloud

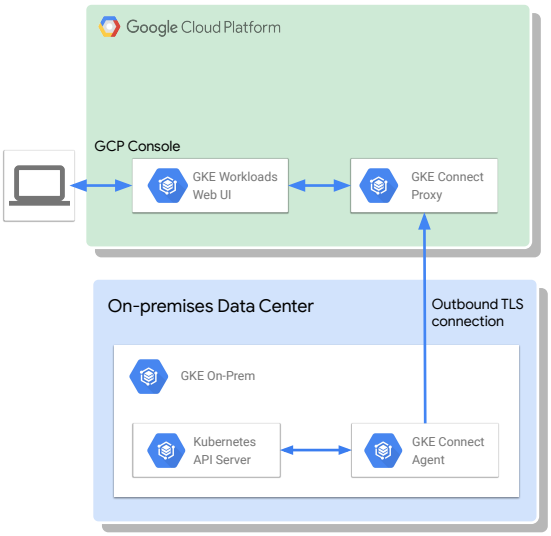
GKE On-Prem Networking

- Each cluster operates in Island mode
- Pods within a cluster can directly reach other pods
- Full node to node mesh across the cluster nodes allowing pods within to communicate directly
- Pod CIDR block is non-routable, and each node is allocated /24 block
- Node IP addresses must be routable within the data center. You can manually assign static IPs or use DHCP



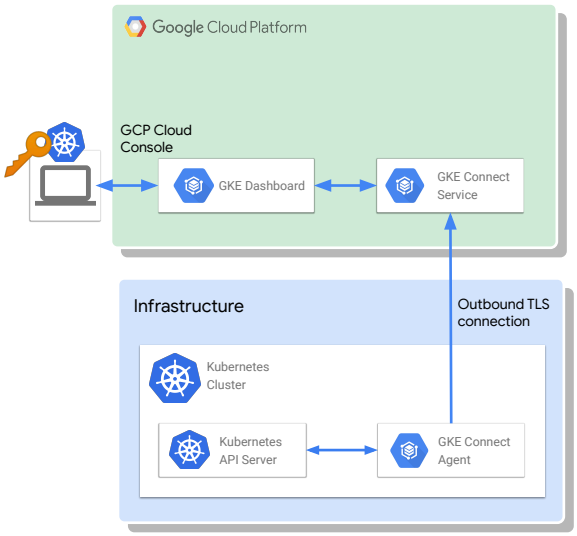
Control Plane Hybrid Connection

- GKE Connect Agent installed in your cluster
- No public IP required for your cluster
- Authenticated and encrypted connection from the Kubernetes cluster to GCP using TLS
- Can traverse NATs and firewalls
- User interactions with clusters are visible in Kubernetes Audit Logs



User Admin Access to Clusters

- Users interact with Kubernetes clusters using their own credentials and RBAC permissions
- Authenticated login from the Cloud Console
- Best practices on privileges
- Kubernetes Audit Logs



Data Plane Hybrid Connection

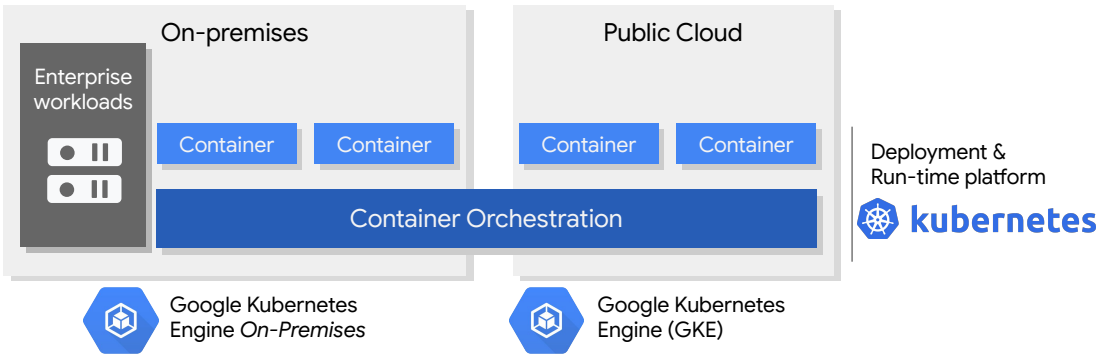
Ways you can connect GKE On-Prem clusters to Google's network.

Connection Type	Use case
Cloud VPN	Private IP access over the internet with static or dynamic routing over BGP
Partner Interconnect	Private IP access through a partner, data does not traverse through the public internet.
Dedicated interconnect	Private IP over a direct physical connection to Google's network. For 10Gb connection and above.

After your fundamental connection is in place, you can add features that enhance access, security, and visibility. For example, you could enable Private Google Access or Connect.

Conclusion

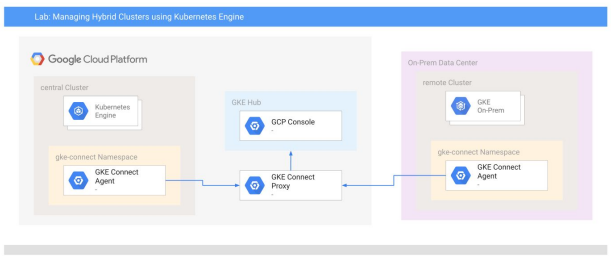
GKE On-Prem and GKE provides a consistent and collaborative compute layer of Anthos, enabling true workload mobility and operational agility



Lab

Managing Hybrid Clusters using Kubernetes Engine

20 min



Objectives

- Understand an installed multi-cluster Kubernetes environment
- Use GKE Hub to authenticate and register a non-GKE Kubernetes cluster using GKE Connect
- Add metadata for the remote cluster
- Review GKE & non-GKE clusters with GKE Dashboard
- Review workloads running in multiple locations across all your clusters