Kubernetes and beyond Breakout Session

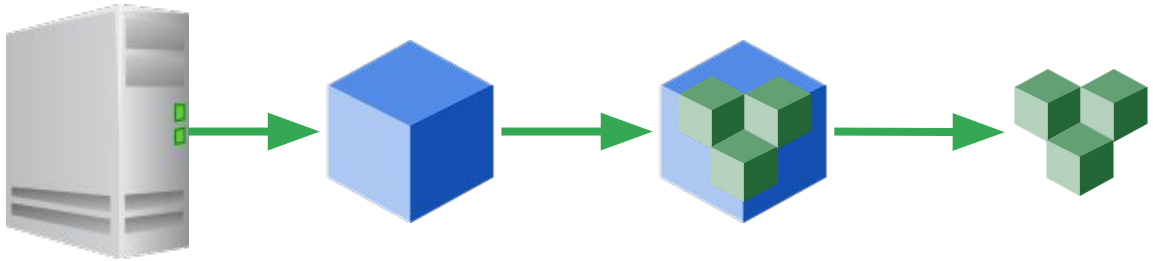
Mathieu Benoit
Cloud Customer Engineer

Google Cloud

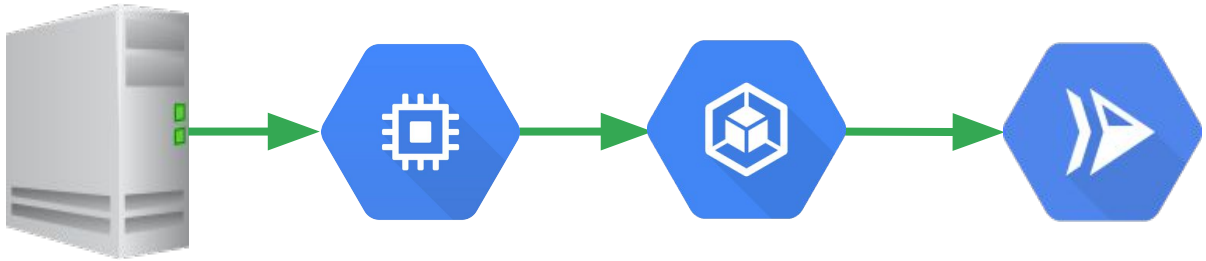
Objectives in 45 min :)

- Containers and Kubernetes
- GKE + demo
- Developer productivity
- Service Mesh and Istio
- Anthos
- Q&A

Evolution of Dev-Compute



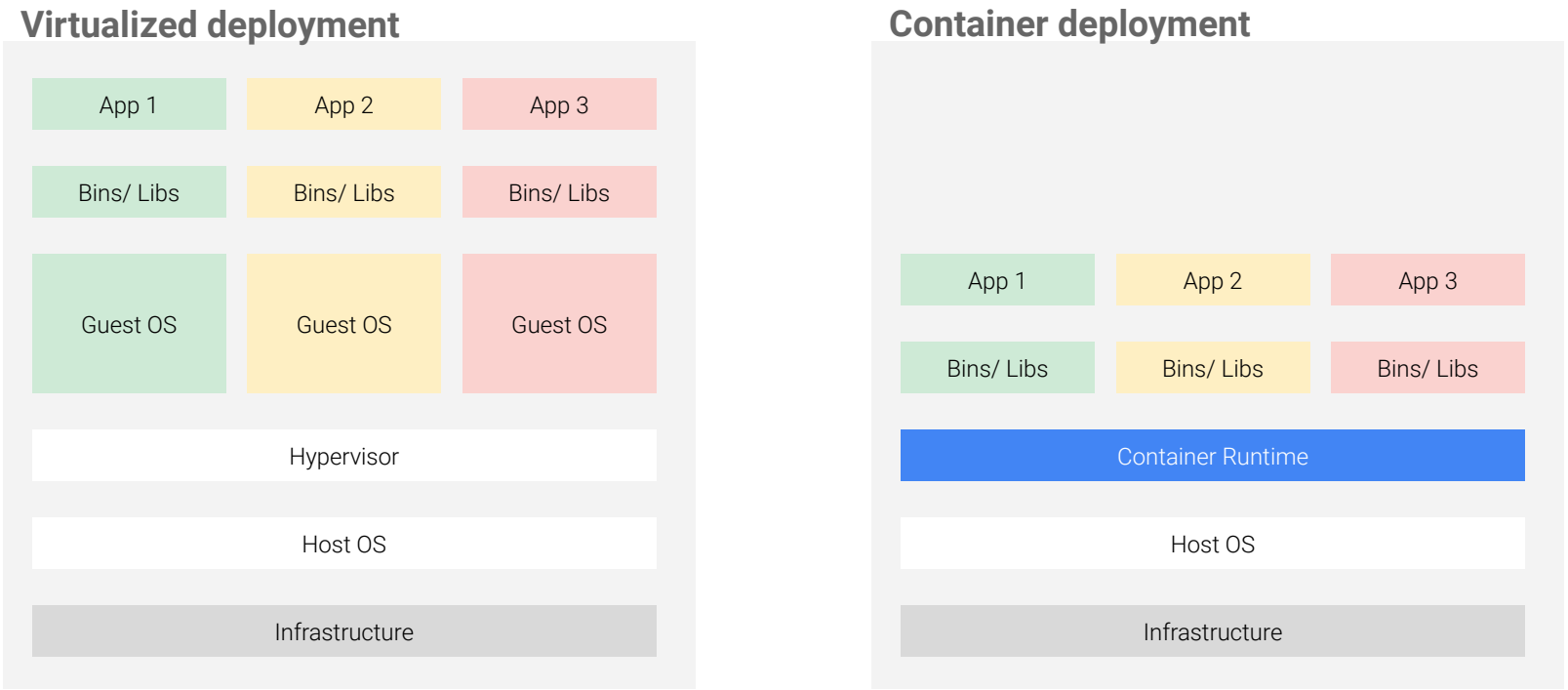
Evolution of Dev-Compute



VM

Container

Containers: A lightweight unit for applications



Google Cloud

Containers

A better way to develop and deploy applications

Immutable infrastructure

Isolation

Faster deployments

Portability

Reusability

Introspection

Versioning

Ease of sharing

What is Kubernetes?

- A portable, open-source, **container-centric** management platform
- Built-in primitives for **deployments, rolling upgrades, scaling, monitoring, and more**
- Inspired by **Google's internal systems**
- Get true **workload portability** and increased **infrastructure efficiency**

Kubernetes Handles:

Scheduling:
Decide where my containers should run

Lifecycle and health:
Keep my containers running despite failures

Scaling:
Make sets of containers bigger or smaller

Naming and discovery:
Find where my containers are now

Load balancing:
Distribute traffic across a set of containers

Storage volumes:
Provide data to containers

Logging and monitoring:
Track what's happening with my containers

Debugging and introspection:
Enter or attach to containers

Identity and authorization:
Control who can do things to my containers

But getting started can be challenging

Kubernetes The Hard Way

This tutorial walks you through setting up Kubernetes the hard way. This guide is not for people looking for a fully-automated command to bring up a Kubernetes cluster. If that's you then check out Google Kubernetes Engine or the Getting Started Guides.

- Prerequisites
- Installing the Client Tools
- Provisioning Compute Resources
- Provisioning the CA and Generating TLS Certificates
- Generating Kubernetes Configuration Files for Authentication
- Generating the Data Encryption Config and Key
- Bootstrapping the etcd Cluster
- Bootstrapping the Kubernetes Control Plane
- Bootstrapping the Kubernetes Worker notes
- Configuring kubectl for Remote Access
- Provisioning Pod Network Rules
- Deploying the DNS Cluster Add-On
- Smoke Test
- Cleaning Up

Google Cloud

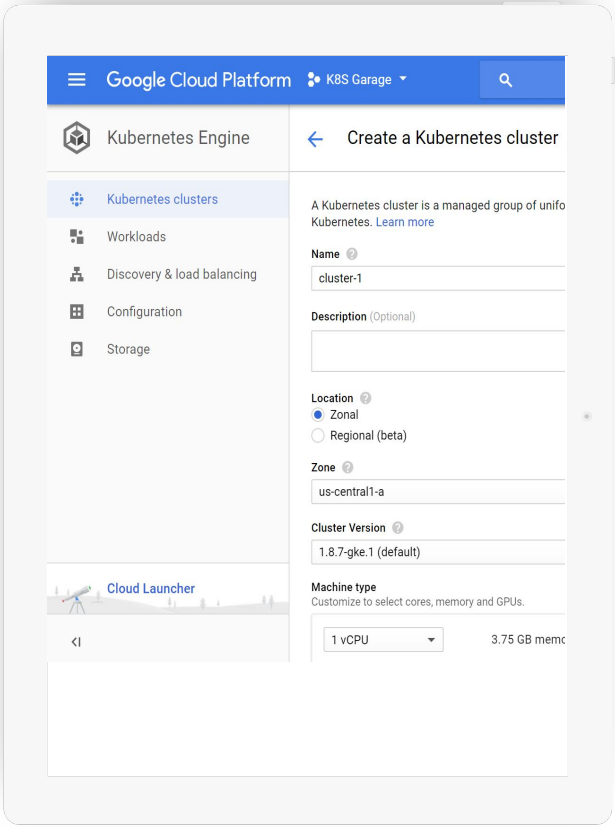
And don't forget "Day 2" ops

- Managing components
- Encrypting and securing etcd
- Configuring HA
- Rolling out security patches
- Backups and disaster recovery
- Bootstrapping TLS
- Managing users and policies

GKE

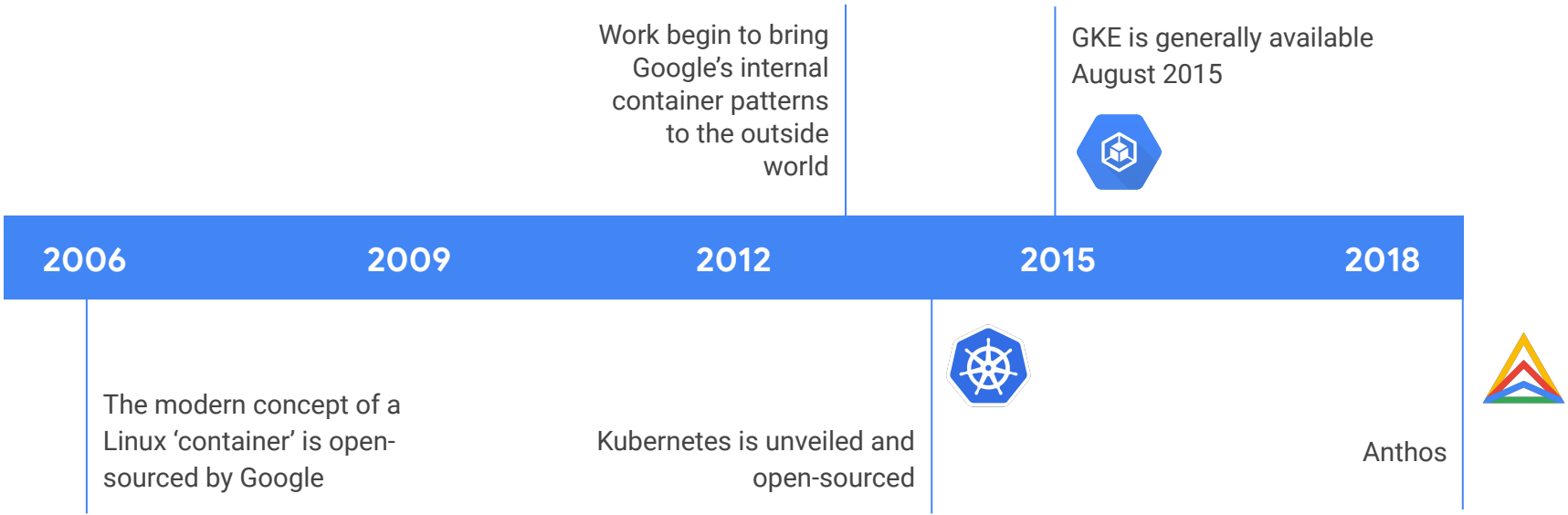
Kubernetes the Easy Way

- Enterprise container management from Google
- Start a cluster with one-click
- View your clusters and workloads in a single pane of glass
- Google keeps your cluster up and running



Google Cloud

GKE is *the* battle-tested managed Kubernetes service



CLOUD NATIVE COMPUTING FOUNDATION

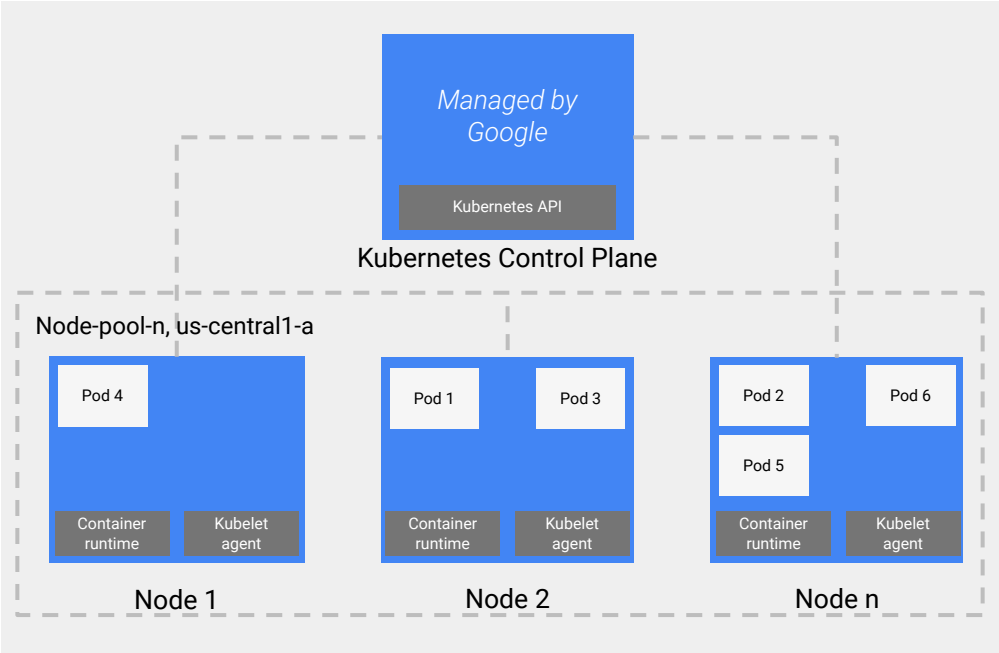
Google Cloud

32 000+ pull requests the latest year

60,000+ commits the latest year

~23 PRs merges/day in the core repo

GKE Architecture



Google Cloud

Auto Kubernetes

Auto-repair

Automatically initiate repair process for nodes that fail a health check.

Auto-upgrade

Keep the control plane and nodes in the cluster up-to-date with the latest stable version

Auto-scale

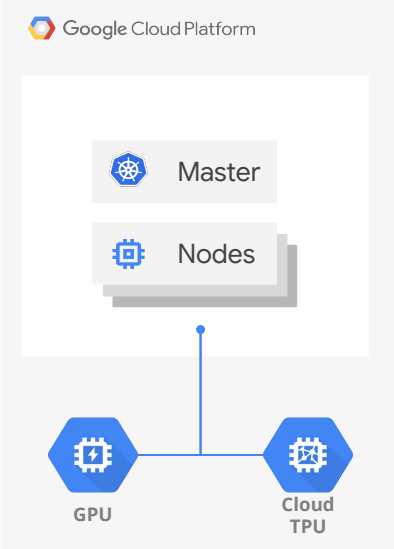
Cluster autoscaling handles increased demand and scales back as needed

Auto-provision

Automatically create new node pools to accommodate workloads

Google Cloud

Application Accelerators



- **Local SSD**
  - Standardized node pools for high throughput/low latency processing apps
- **Cloud GPU**
  - Use GPUs to accelerate special workload instances such as advanced data processing
- **Cloud TPU**
  - Hardware accelerated clusters for advanced apps like machine learning

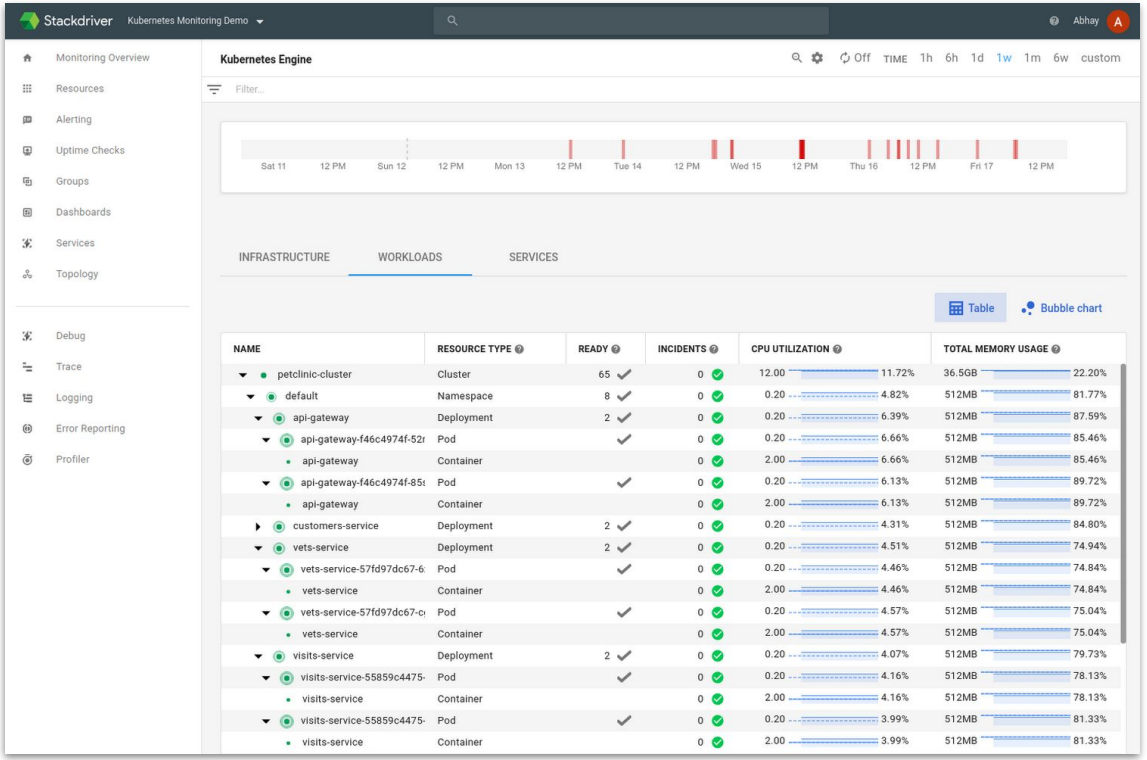
At a glance
Security

- All GKE components are **encrypted at rest**. This includes etcd where secrets are stored.
- **TLS** for master-to-master and node-to-master communication
- **Container-Optimised OS (COS)** hardened, google tested images on all nodes
- **Network policies** to control pod-to-pod (**Istio** to encrypt), ingress and egress communication
- **Private clusters** makes your master inaccessible from the public internet
- **Metadata concealment** isolates workloads from node metadata

Logging and Monitoring

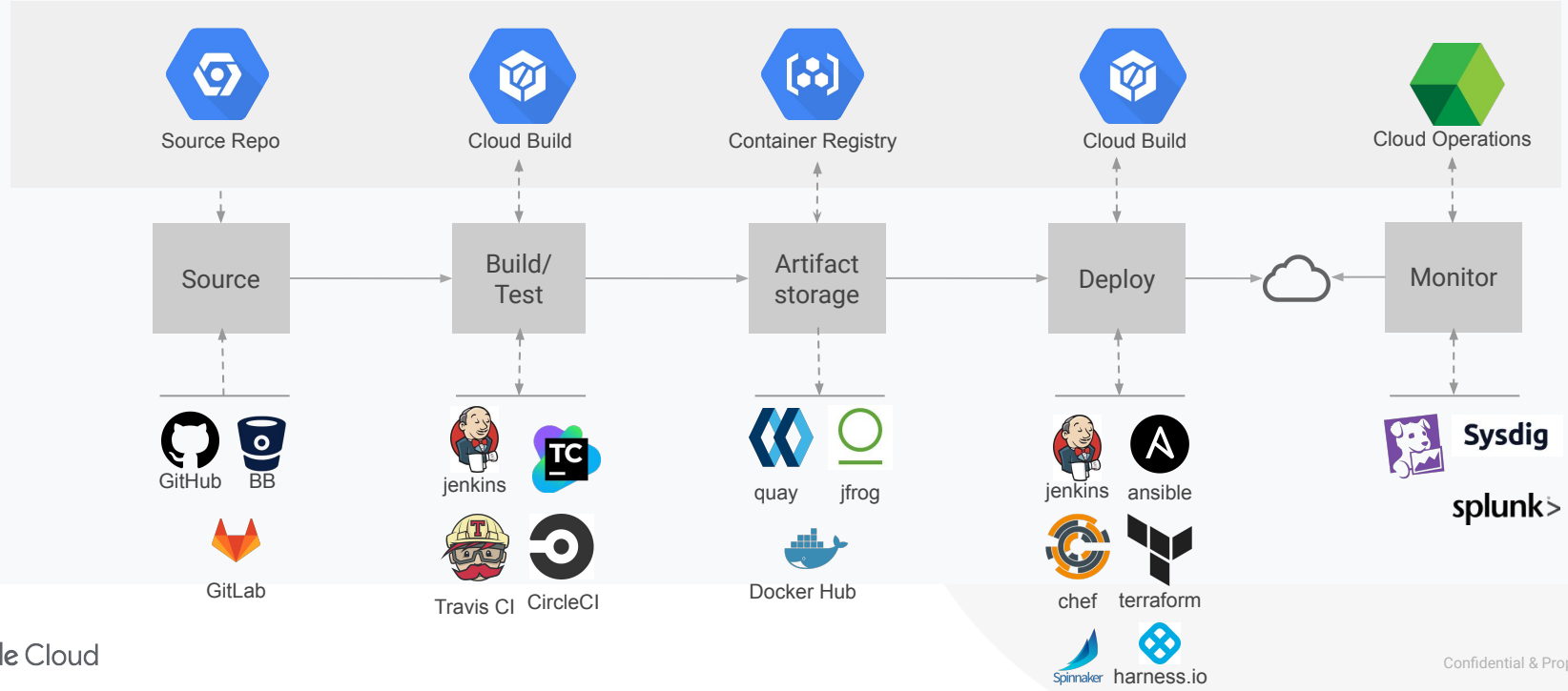
- Use Cloud Logging to automatically collect, process, and store your container and system logs
- Integrated with Audit Logging
- Cloud Monitoring will monitor your cluster's CPU and memory as well as custom metrics for your application

Stackdriver

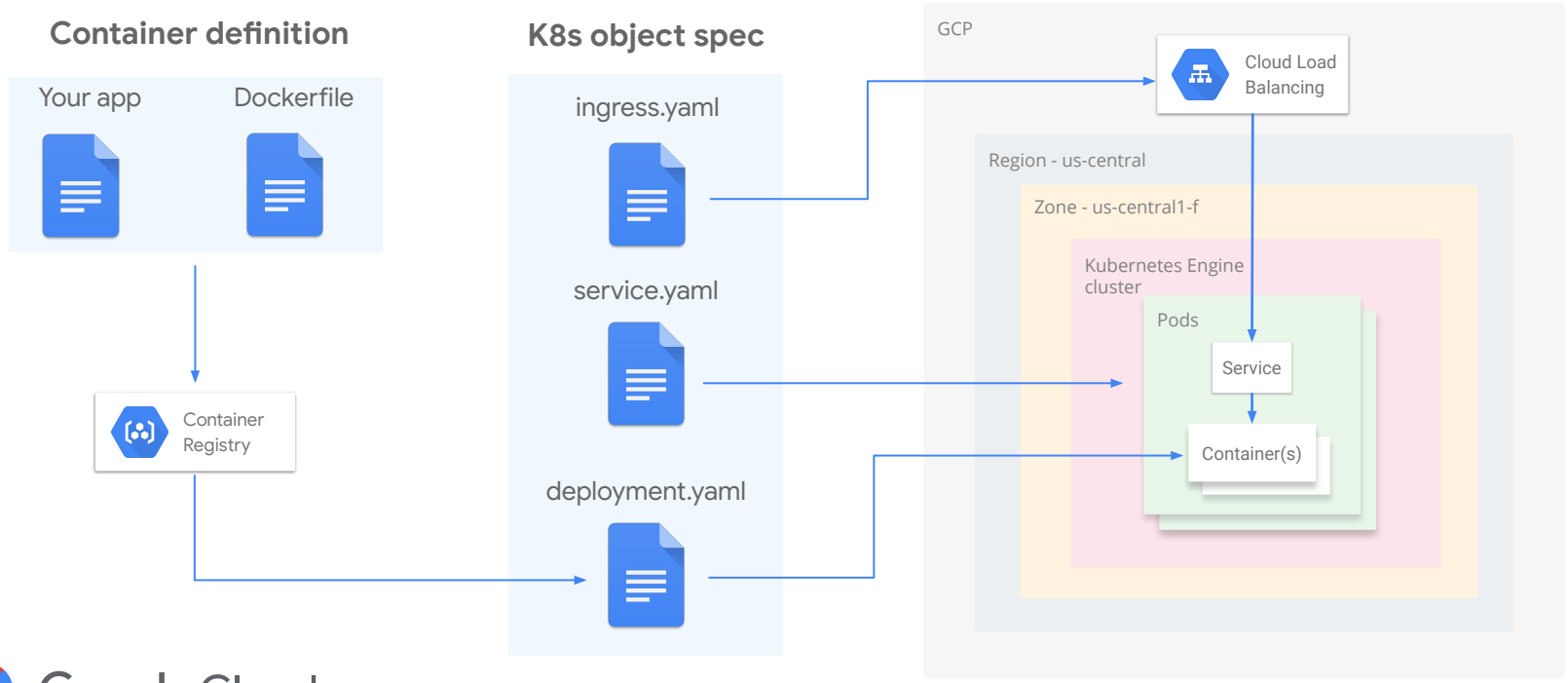


Google Cloud

CI/CD with Containers



Demo: deploying containers in GKE



Google Cloud

Tools can help...

minikube

docker

Cloud Code

flux

SKAFFOLD

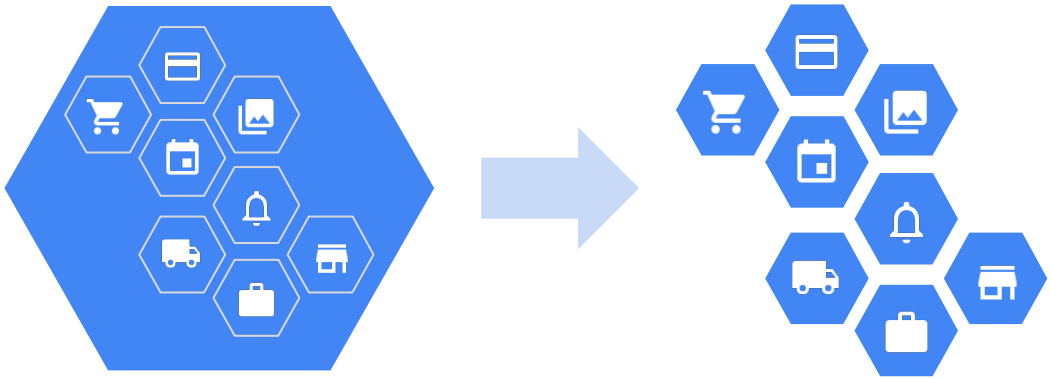
Jib

Containerize your Java application.

HELM

Google Cloud

Microservices create API management challenges

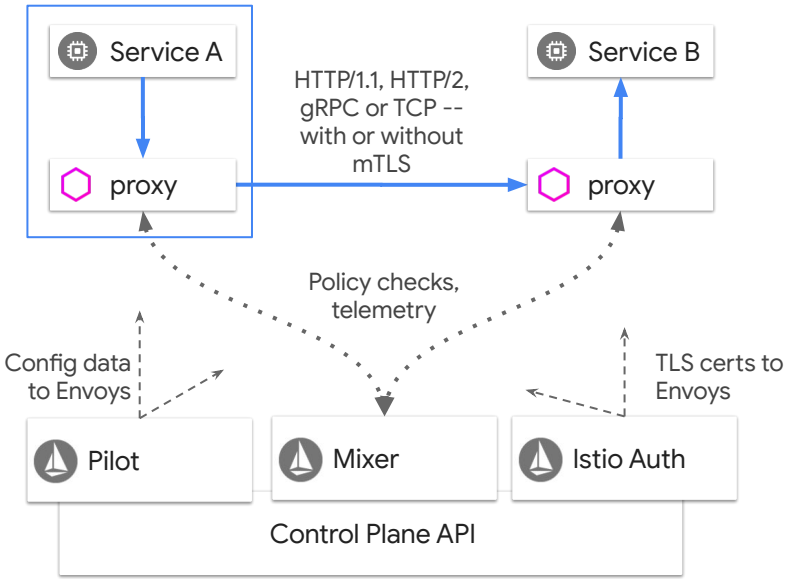


- Maintaining resilience, discovery, and routing logic in code for independent services written in different languages becomes incredibly complex and expensive to operate
- The role of a service mesh is to overlay your services with a management framework

Istio is an open framework (from Google, IBM and Lyft) for connecting, securing, managing and monitoring services

Google Cloud

Istio architecture overview



Pilot

Control plane to configure and push service communication policies

Envoy

Network proxy to intercept communication and apply policies

Mixer

Policy enforcement with a flexible plugin model for providers for a policy

Istio Auth

Service-to-service auth[n,z] using mutual TLS, with built-in identity and credential management

Google Cloud

Consumption or Subscription-based, patched via automation

Based on Kubernetes, Istio, Knative, Tekton

Tools to perform no-touch migration & automation

Anthos is a **managed** **application platform** for **enterprises** that want faster **modernization** and greater **consistency** in a **hybrid and multi-cloud** world.

Built for large companies with complex needs

Define declarative policies to enforce secure standards everywhere

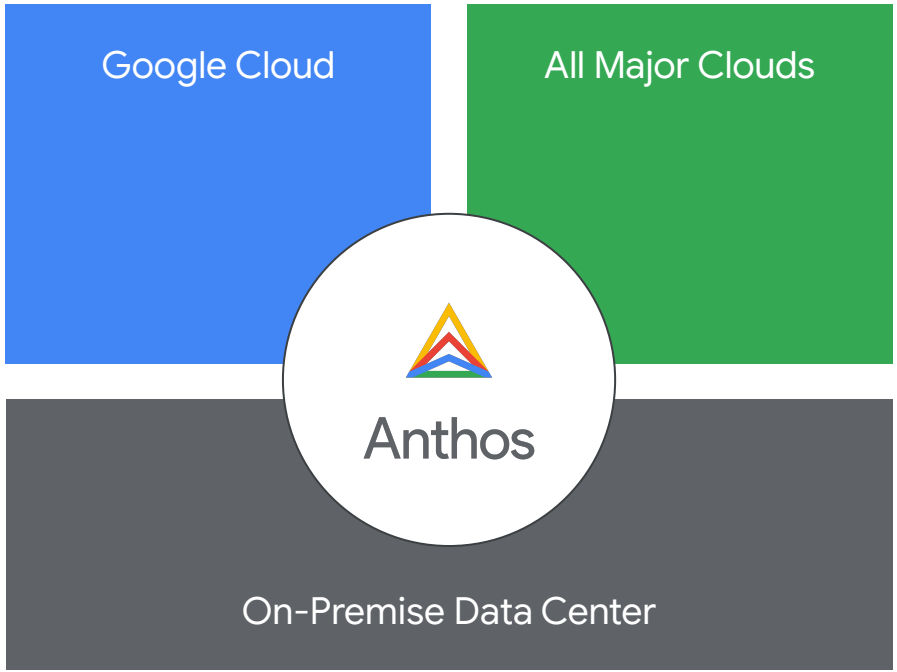
Run on-premises (bare metal), in GCP, and other public clouds

Introducing Google Cloud's Anthos

Anthos lets you build and manage modern **hybrid and multi-cloud** applications without lock-in

Build once, to run anywhere, across your existing on-premise infrastructure and all major public cloud providers

Built on open-source **kubernetes, Istio and Knative**



Google Cloud

Core Components of Anthos

Extras: Anthos Ingress, Binary Authorization, Hybrid AI, Marketplace

gitops

Config & Policy management

Anthos Config Management

Open Policy Agent

Application Development & Deployment

Cloud Run for Anthos

Cloud Build for Anthos

Service Management

Anthos Service Mesh

kubernetes

Container Management

Anthos GKE

Operations Management

Cloud Logging & Monitoring, ASM ServiceOps

Google Cloud

Resources

- **Looking ahead as GKE**, the original managed Kubernetes, turns 5
- gVisor: **Protecting GKE and serverless** users in the real world
- Bayer Crop Science seeds the future with **15000-node GKE clusters**
- Exposing GKE applications through Ingress and Services

- Start your K8s learning journey with hands-on training at no cost
- Introduction to **Kubeflow on Google Kubernetes Engine**
- App Modernization for CIO ebook
- Anthos ebook

- Cloud Native Computing Foundation

That’s a wrap!
Q&A

Google Cloud