Using source code management patterns to configure and secure your Kubernetes clusters

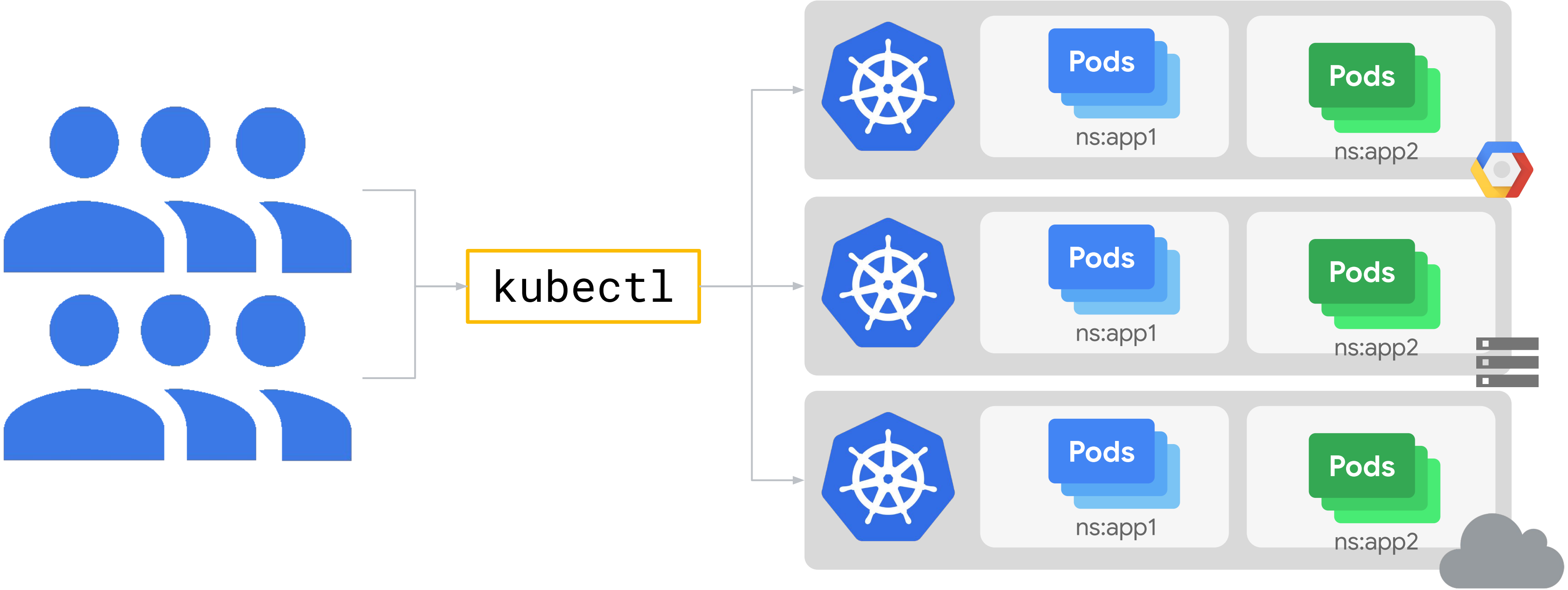
Giovanni Galloro - Customer Engineer, Google Cloud

{CODEMOTION}

Online Tech Conference

- Italian edition -

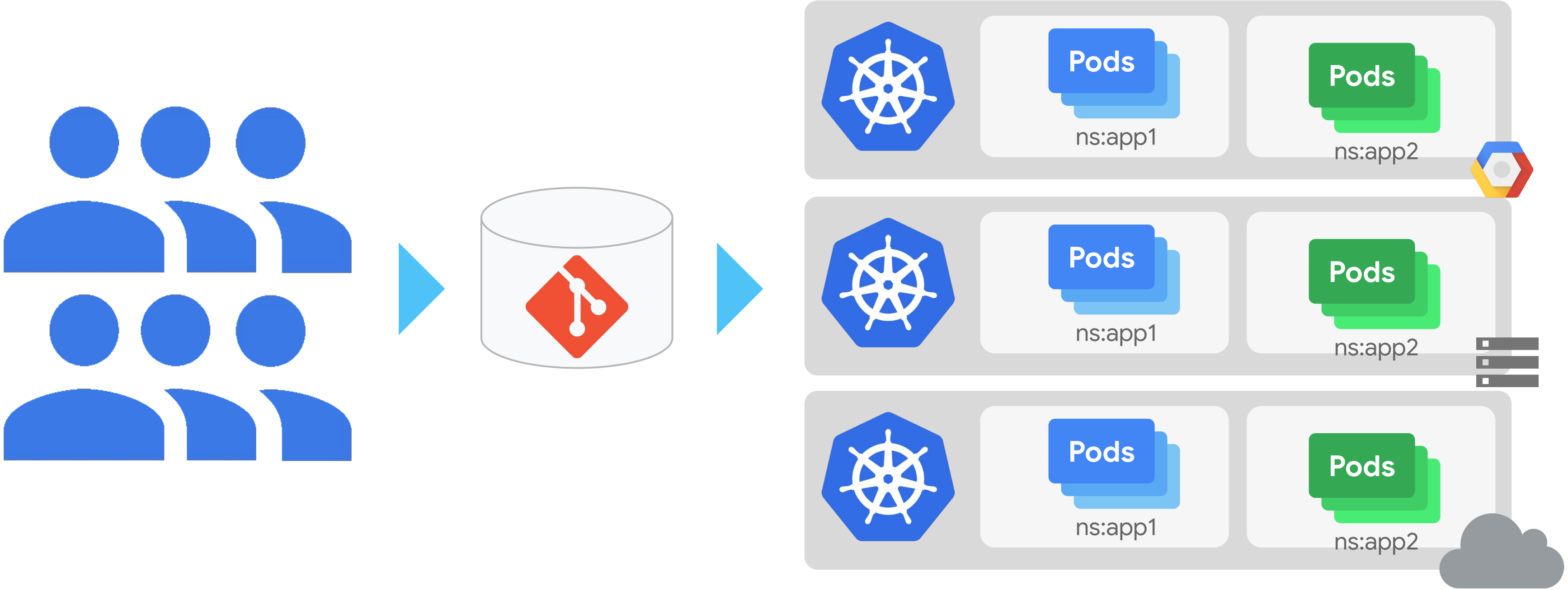
23-24-25 Marzo, 2021



Operator team

Imperative ops

Multi-Platform environment

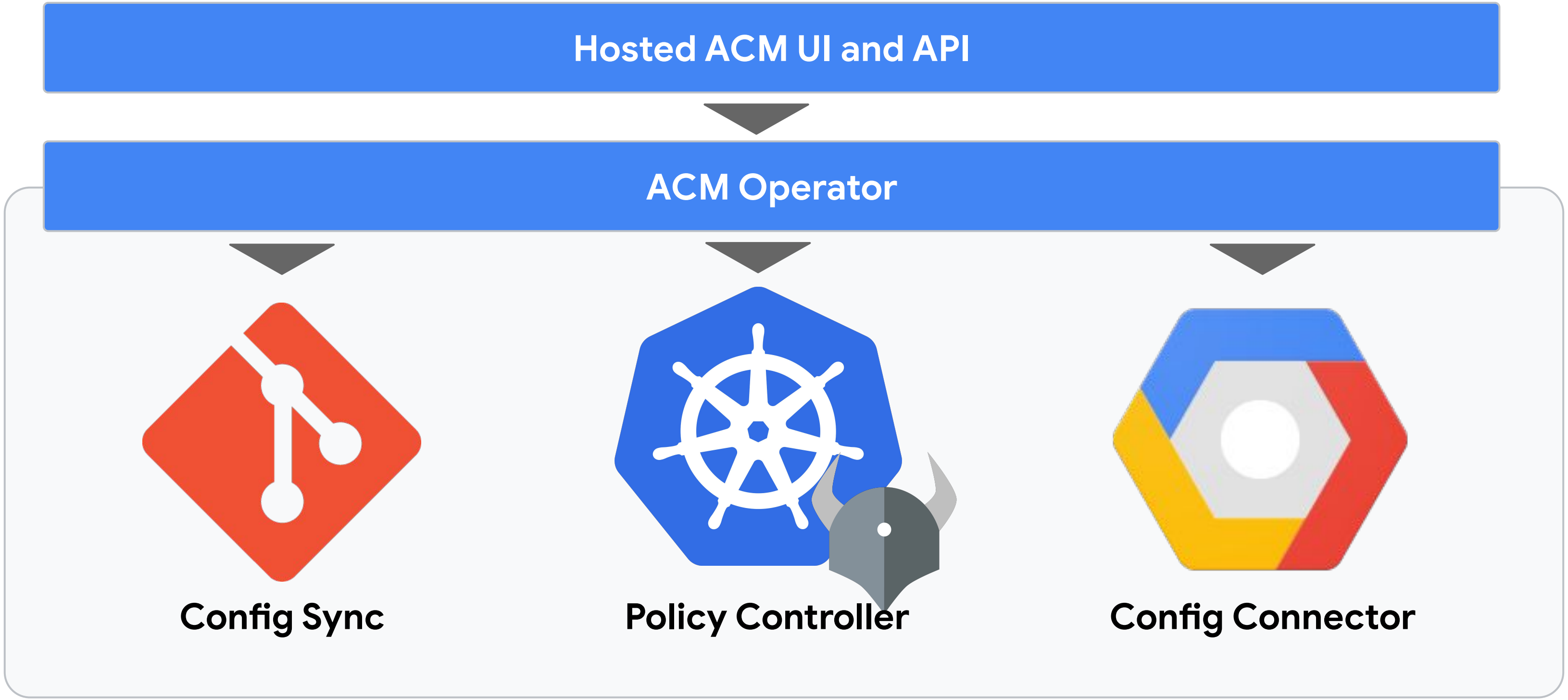


Operator team

Config repo

Multi-Platform environment

Anthos Config Management (ACM) Components



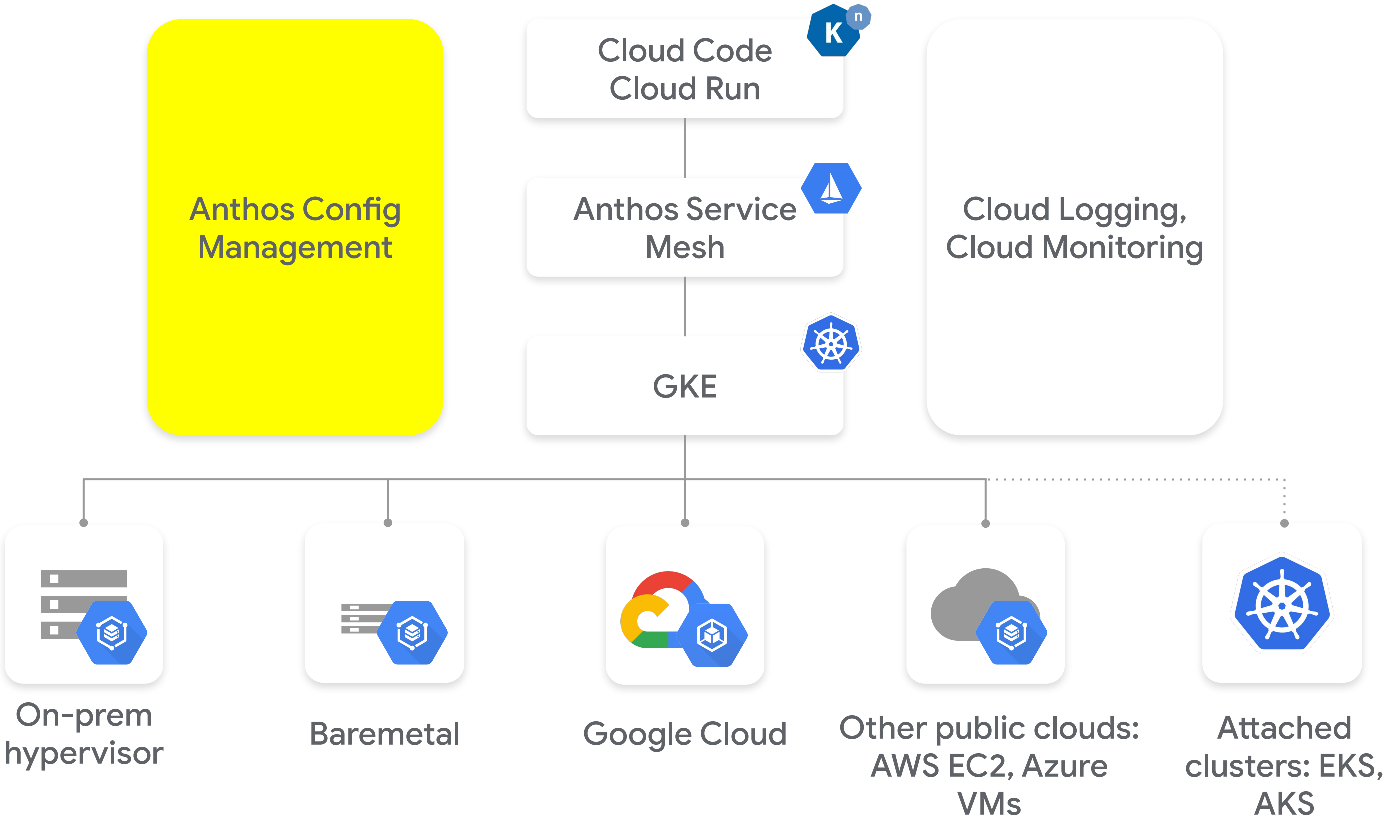
Hosted ACM UI and API

ACM Operator

Config Sync

Policy Controller

Config Connector



Anthos Config Management

Cloud Code
Cloud Run

Anthos Service Mesh

GKE

Cloud Logging, Cloud Monitoring

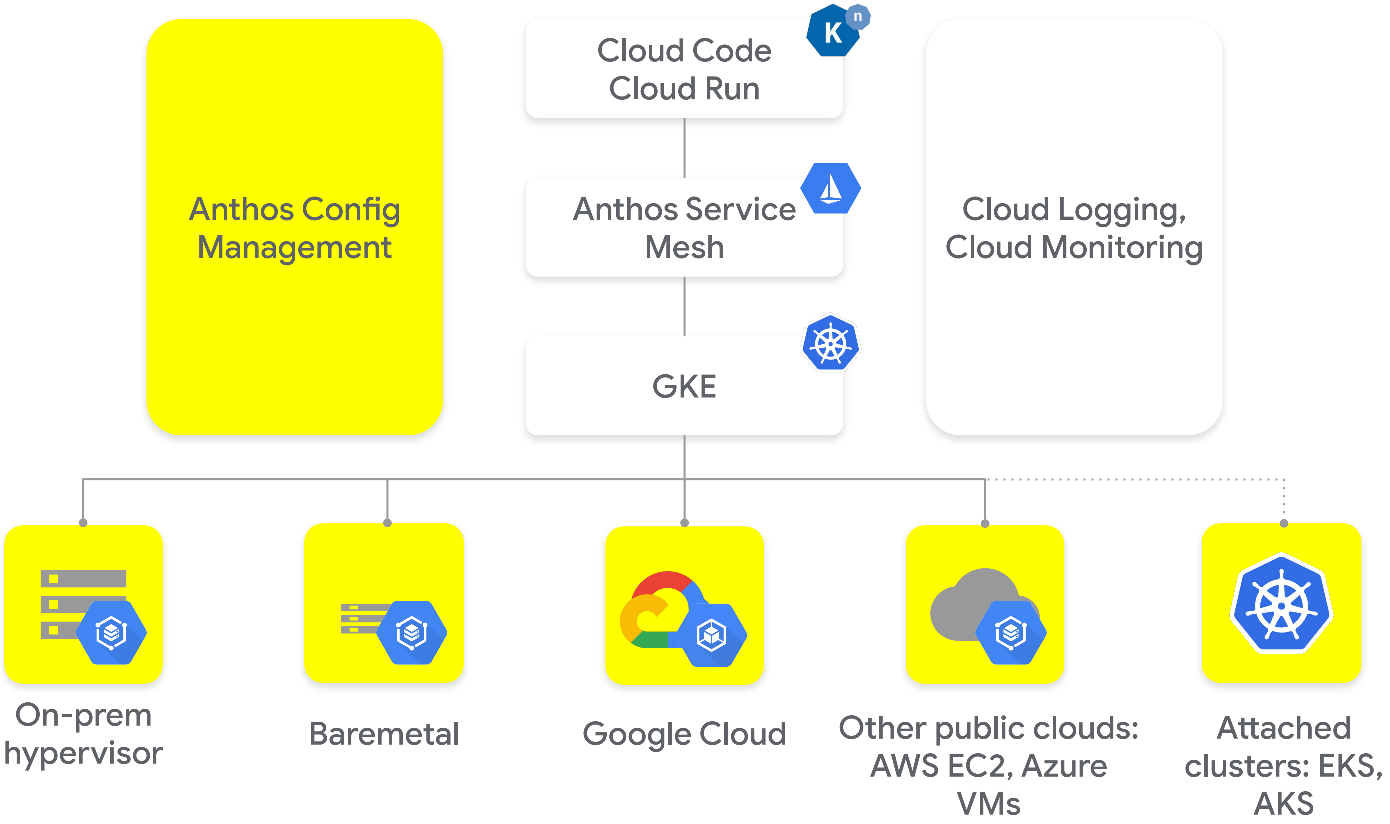
On-prem hypervisor

Baremetal

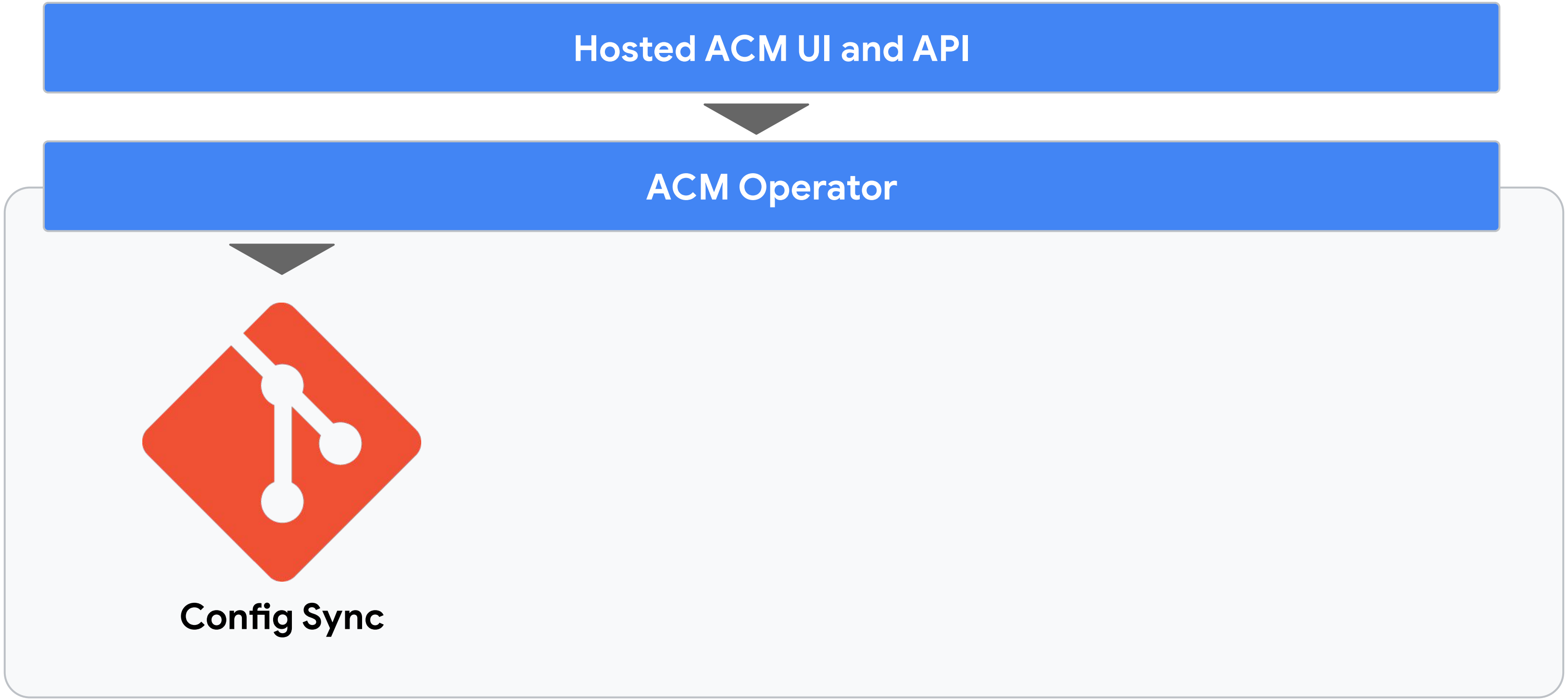
Google Cloud

Other public clouds: AWS EC2, Azure VMs

Attached clusters: EKS, AKS


Anthos Config Management
Cloud Code
Cloud Run
Anthos Service Mesh
GKE
Cloud Logging, Cloud Monitoring
On-prem hypervisor
Baremetal
Google Cloud
Other public clouds: AWS EC2, Azure VMs
Attached clusters: EKS, AKS

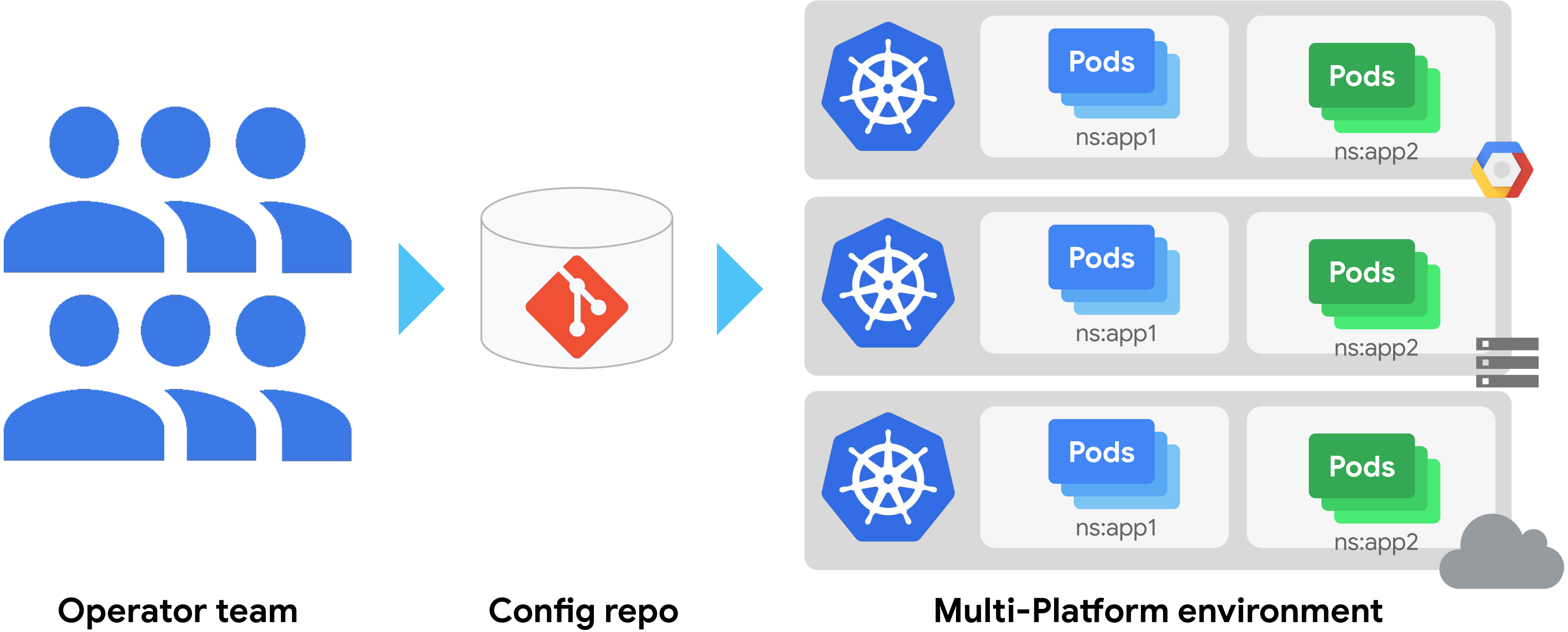
Anthos Config Management (ACM) Components



Hosted ACM UI and API

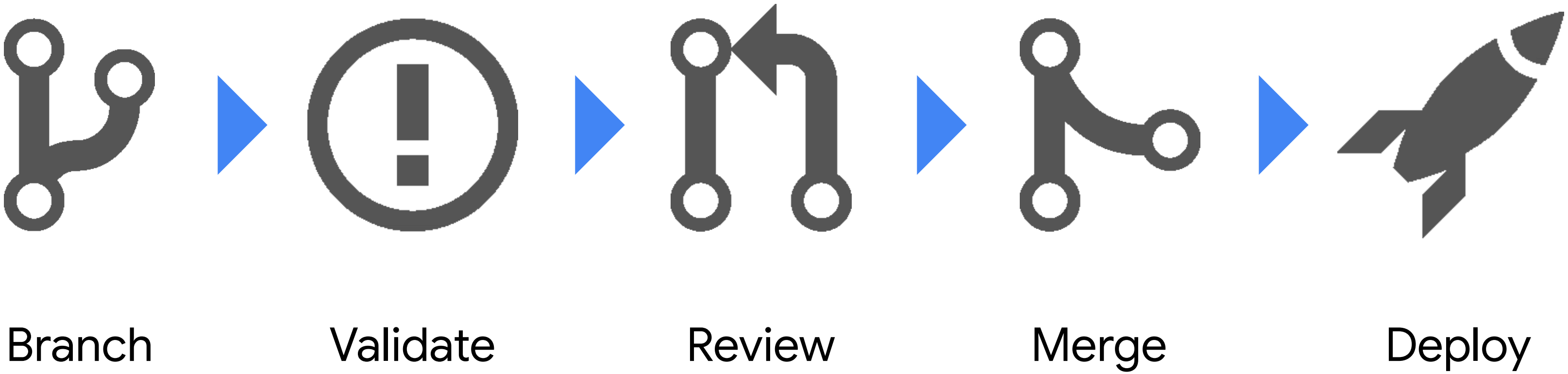
ACM Operator

Config Sync



Google Cloud

Source Code Management approach to Config Management



Branch

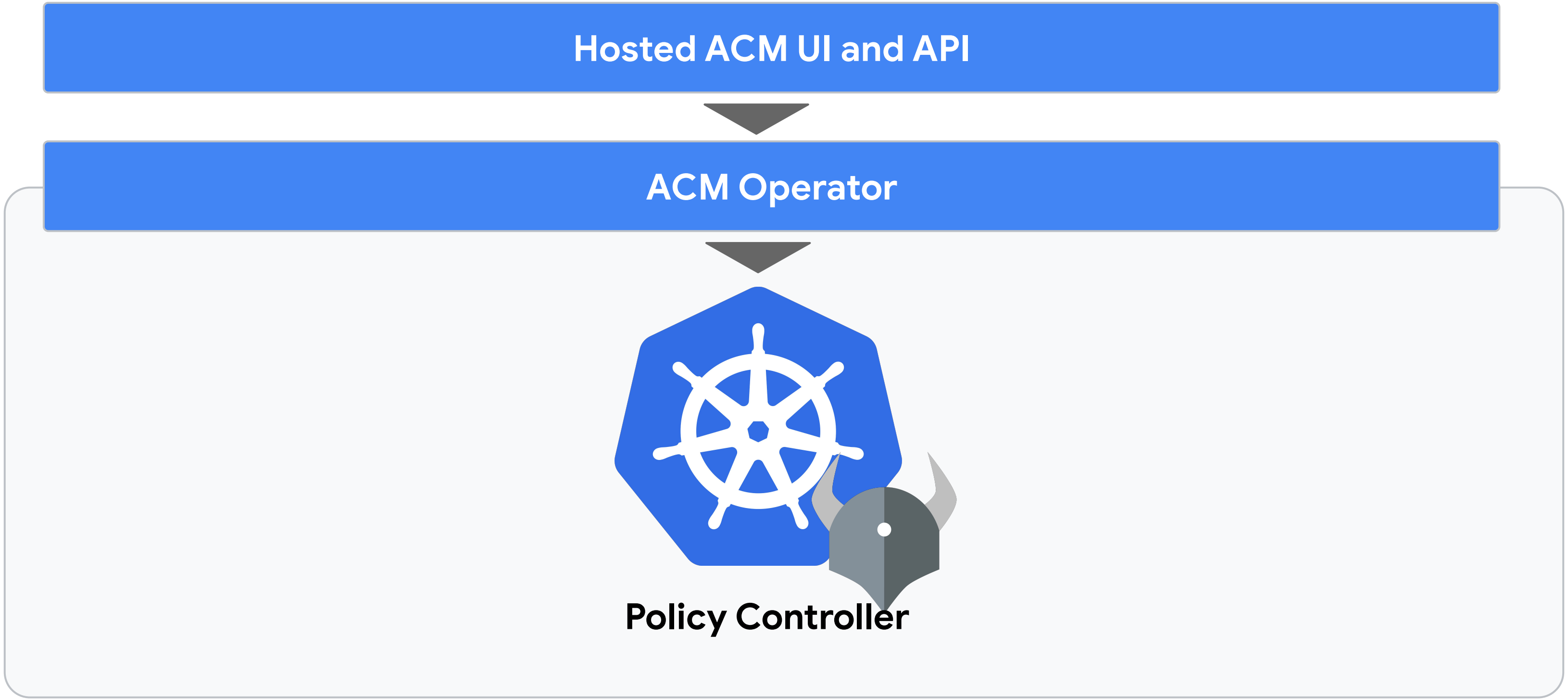
Validate

Review

Merge

Deploy

Anthos Config Management (ACM) Components



Hosted ACM UI and API

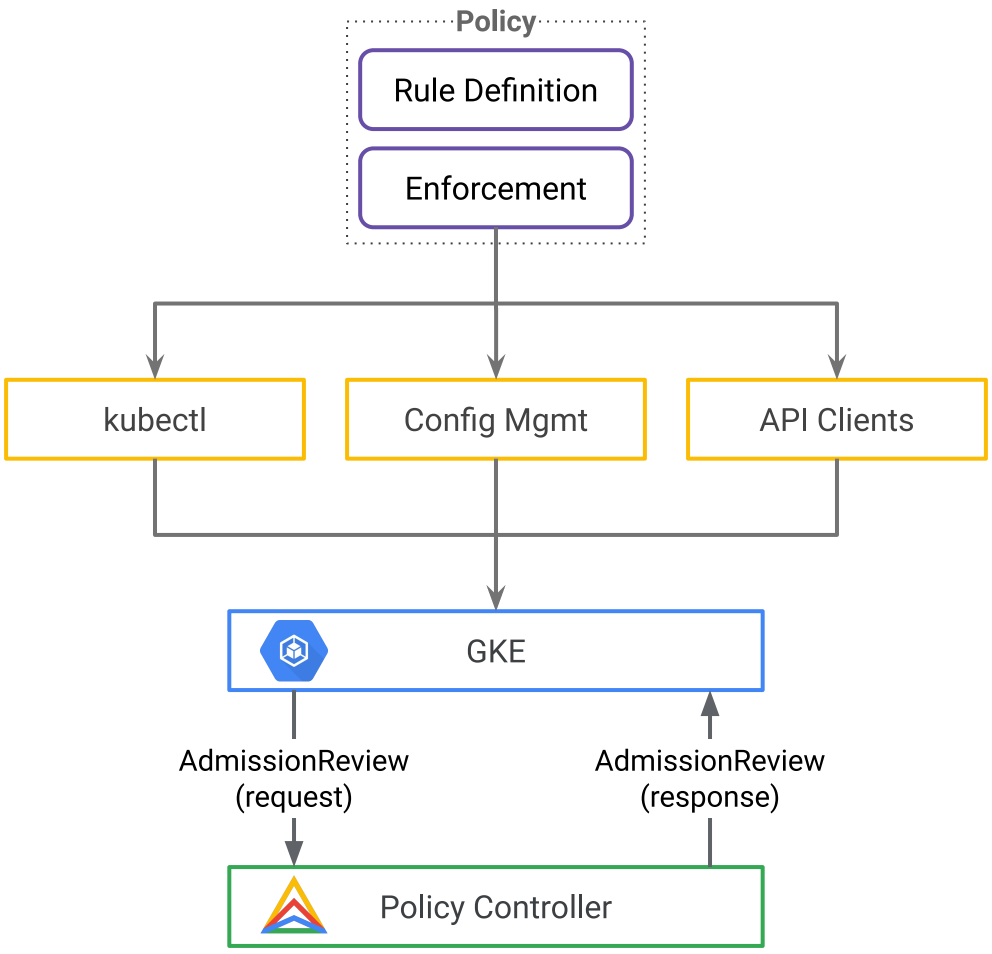
ACM Operator

Policy Controller

Policy controller

Based on Open Policy Agent’s Gatekeeper, **ACM Policy Controller** provides first-class integration between OPA and Kubernetes via a custom controller.

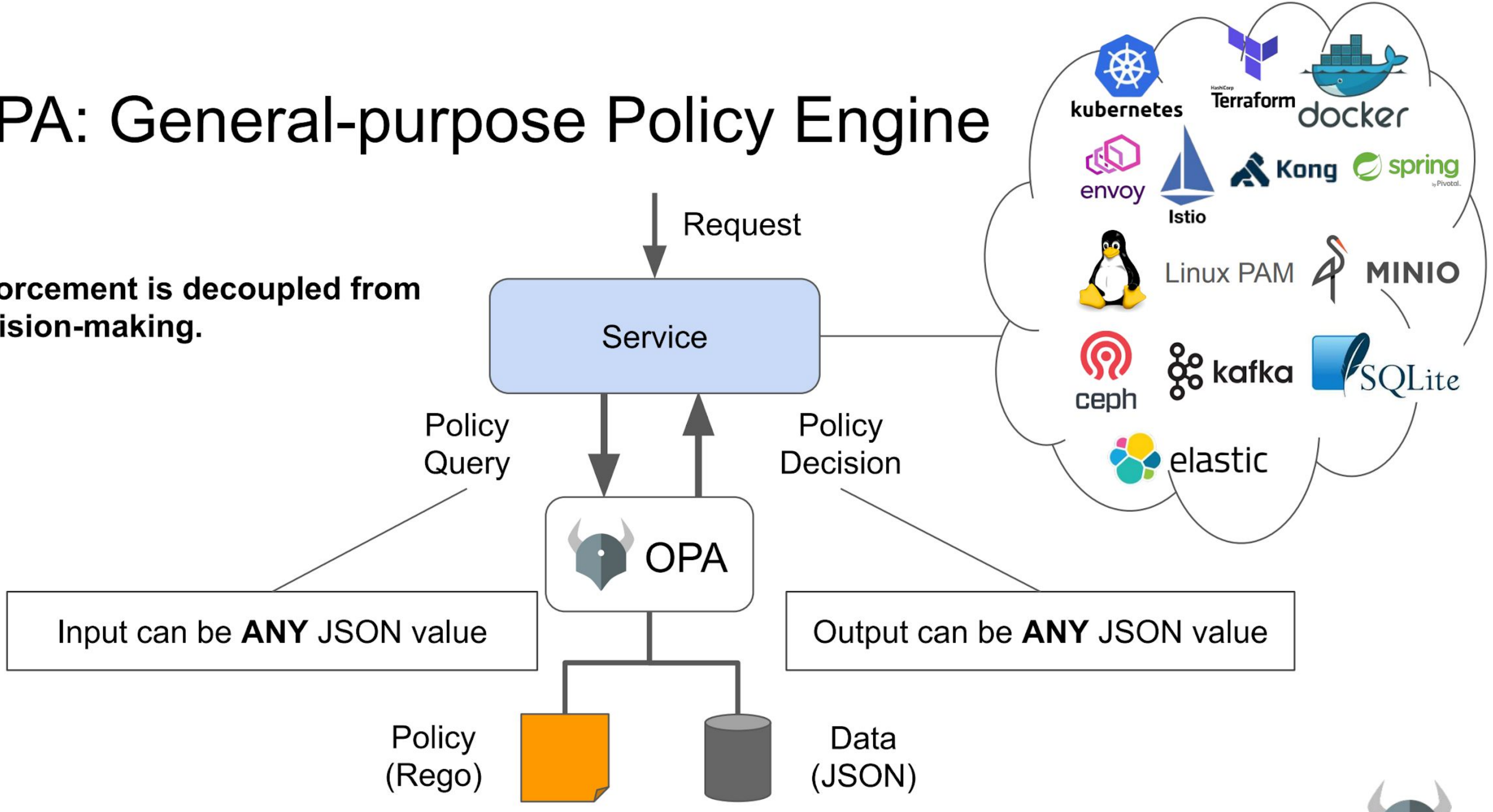
It turns Rego policies into Kubernetes objects, allowing them to be customized and deployed using standard workflows.



Google Cloud

OPA: General-purpose Policy Engine

Enforcement is decoupled from decision-making.

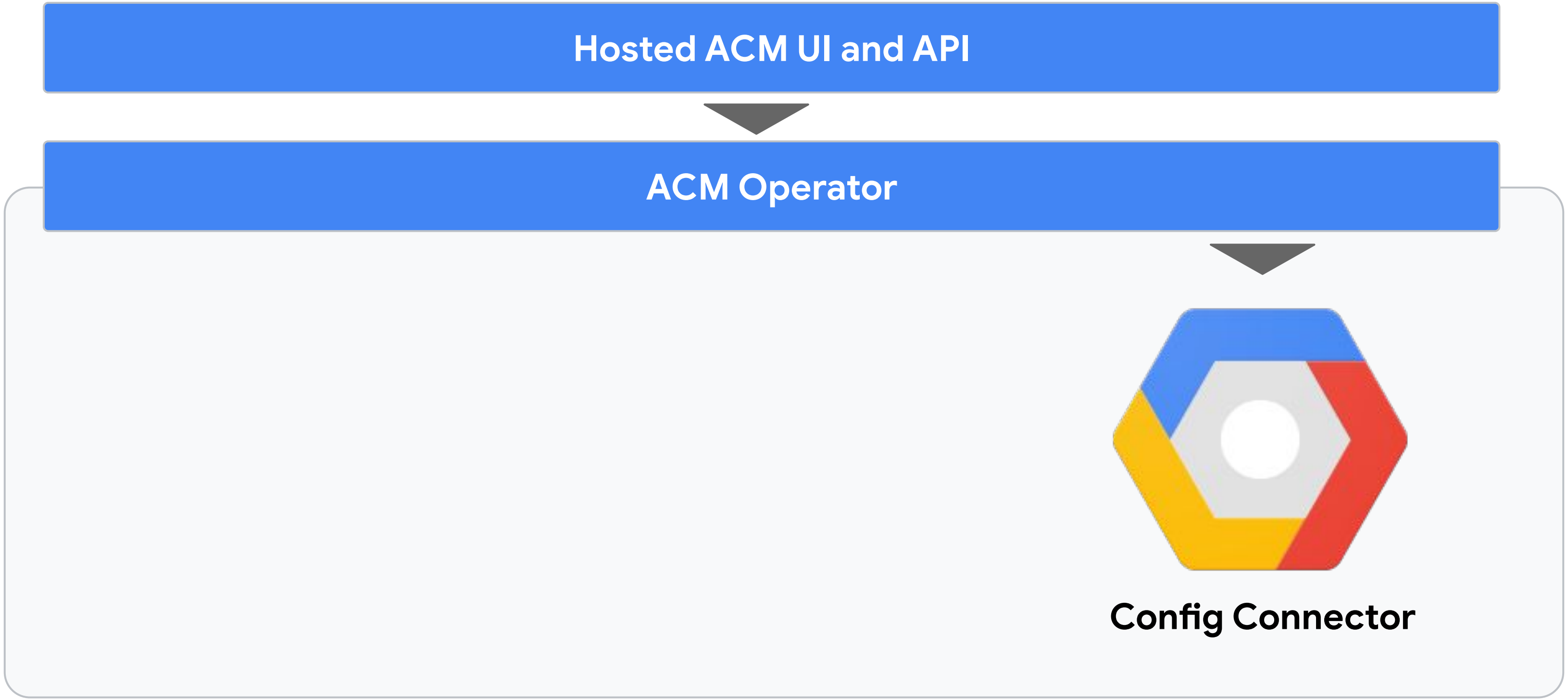


openpolicyagent.org

Pod Security Policies → Gatekeeper Constraints

PSP Field Name	OPA GK Constraint Template
privileged	privileged-containers
hostPID, hostIPC	host-namespaces
hostNetwork, hostPorts	host-network-ports
volumes	volumes
allowedHostPaths	host-filesystem
allowedFlexVolumes	flexvolume-drivers
runAsUser, runAsGroup, supplementalGroups	users*
fsGroup	users*
readOnlyRootFilesystem	read-only-root-filesystem
allowPrivilegeEscalation	allow-privilege-escalation
defaultAddCapabilities, requiredDropCapabilities, allowedCapabilities	capabilities
seLinux	seLinux
allowedProcMountTypes	proc-mount
Annotations for AppArmor profile	apparmor
Annotations for seccomp profile	seccomp
forbiddenSysctls,allowedUnsafeSysctls	forbidden-sysctls

Anthos Config Management (ACM) Components



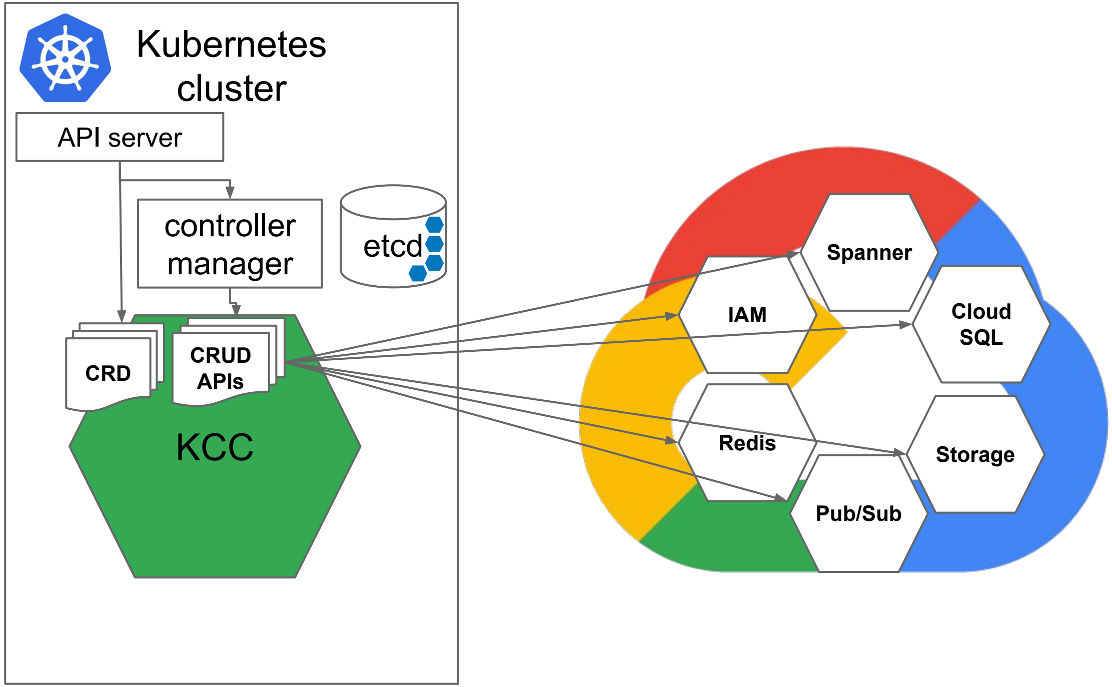
Hosted ACM UI and API

ACM Operator

Config Connector

How does KCC work?

KCC resources are registered via Custom Resource Definitions watched by the KCC controller



Q & A