MODERN APPLICATION DELIVERY WITH

KUBERNETES

kubernetes

etcd

CoreDNS

CNI

gRPC

Open Policy Agent

Istio

envoy

HELM

container d

SECURITY

APP PACKAGING + DEPLOYMENT

fluentd

elastic

Prometheus

Grafana

MONITORING

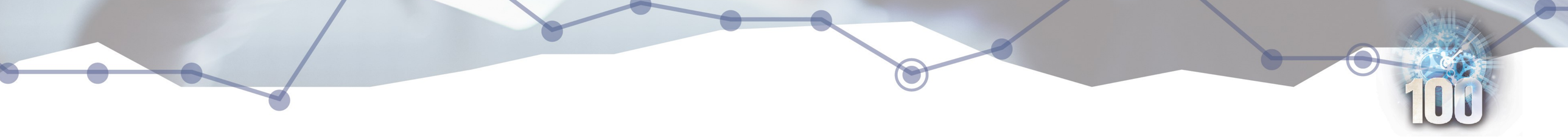
OPENTRACING

JAEGER

TRACING

Virtual Kubelet

SERVERLESS



THE BASE

PLATFORM

WHAT IS KUBERNETES?

- Orchestrates computing, networking and storage infrastructure (and more)
- Portable, extensible open-source platform for managing containerized workloads
- Uses declarative configuration, facilitating automation
- Huge and rapidly growing community

WHAT IS KUBERNETES?

- Supports Linux and Windows containers
- Support different container runtimes
  - Docker
  - Containerd
  - and anything that implements the Container Runtime Interface (CRI)
- Many supported network plugins (cloud network, overlay networks, etc.)
- And other plugins for storage, secret management, policy enforcement, etc.

WHAT IS KUBERNETES?

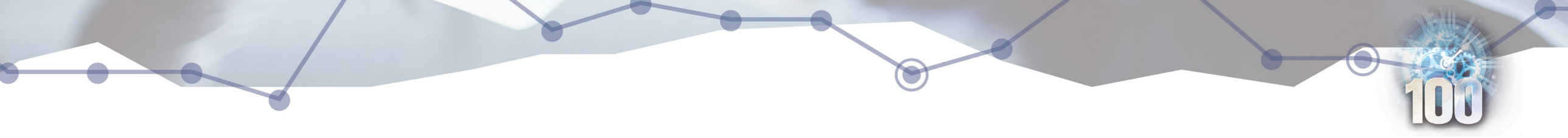
- All major cloud providers offer a managed service
  - Google, Microsoft, Amazon, Digital Ocean, IBM, Oracle, and more!
- Platform as a Service (PaaS) offerings
  - RedHat Openshift, VMWare Cloud PKS, Pivotal PKS, and more!
- Self-hosted (on-premise or on IaaS)
  - Kubeadm, kops, Kubespray

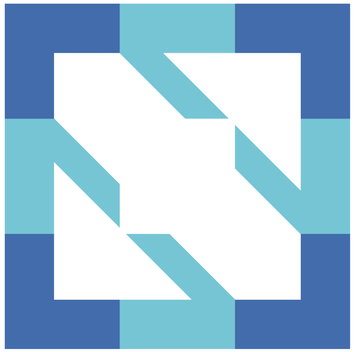
WHAT IS KUBERNETES?

- In use by many large organizations:
  - Google
  - GitHub
  - Reddit
  - Shopify
  - CERN
  - IBM
  - OpenAI
  - Pinterest
  - Tinder
  - and many more!

WHAT IS KUBERNETES?

- In use by many Government departments:
  - STATCAN
  - CDS / TBS
  - SSC
  - CSE / CSIS
  - ISED
  - DFO
  - ESDC
  - House of Commons
  - City of Ottawa
  - and many more!

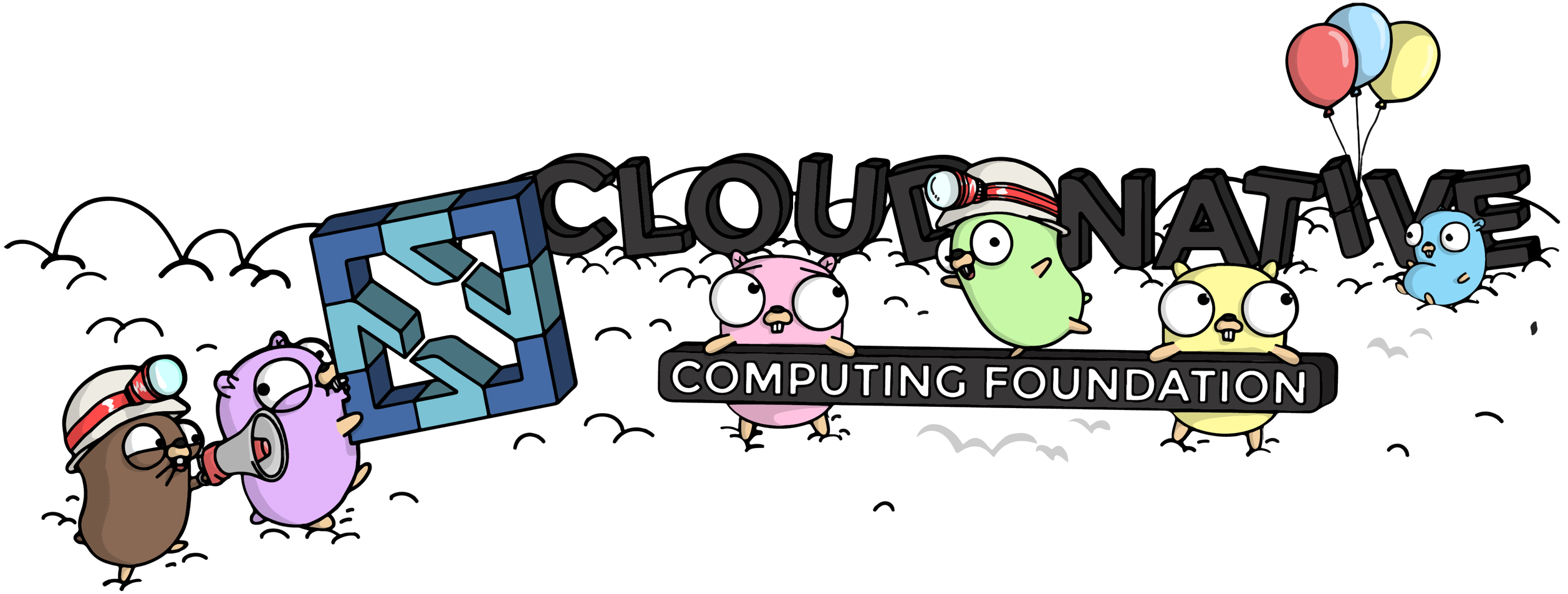




ENHANCE YOUR CLUSTER

PLATFORM TOOLS

CNCF: CLOUD NATIVE COMPUTING FOUNDATION



PROMETHEUS / GRAFANA

- Real-time cluster and application metrics
  - Broken down to different levels, including per-application, per-service, per-namespace, per-node
- Alerting rules
  - Custom defined rules, and various alerting mechanisms

ELASTICSEARCH

- Centralized application and cluster logging
- Indexed and can be searched
- Can be visualized

HELM

- Official Kubernetes package manager
- Helm Charts help define, install and upgrade complex applications with ease
- Templating of your applications cluster resources
  - Easily deploy multiple instances of your application
- Provides application lifecycle management
- Many official charts: https://github.com/helm/charts

VELERO (FORMERLY ARK)

- A utility for managing disaster recovery of cluster resources and data volumes
- Takes snapshots of your cluster (and its data)
- Restore across clusters (and soon, cloud providers)

VIRTUAL KUBELET

- Masquerades as a cluster node but interfaces with external runtimes
  - Azure Container Instances
  - Amazon AWS Fargate
  - and more!
- Hybrid workflow between dedicated machines and serverless infrastructure
  - Cost-benefit: use dedicated machines for base loads, and cloud container runtimes for burst load

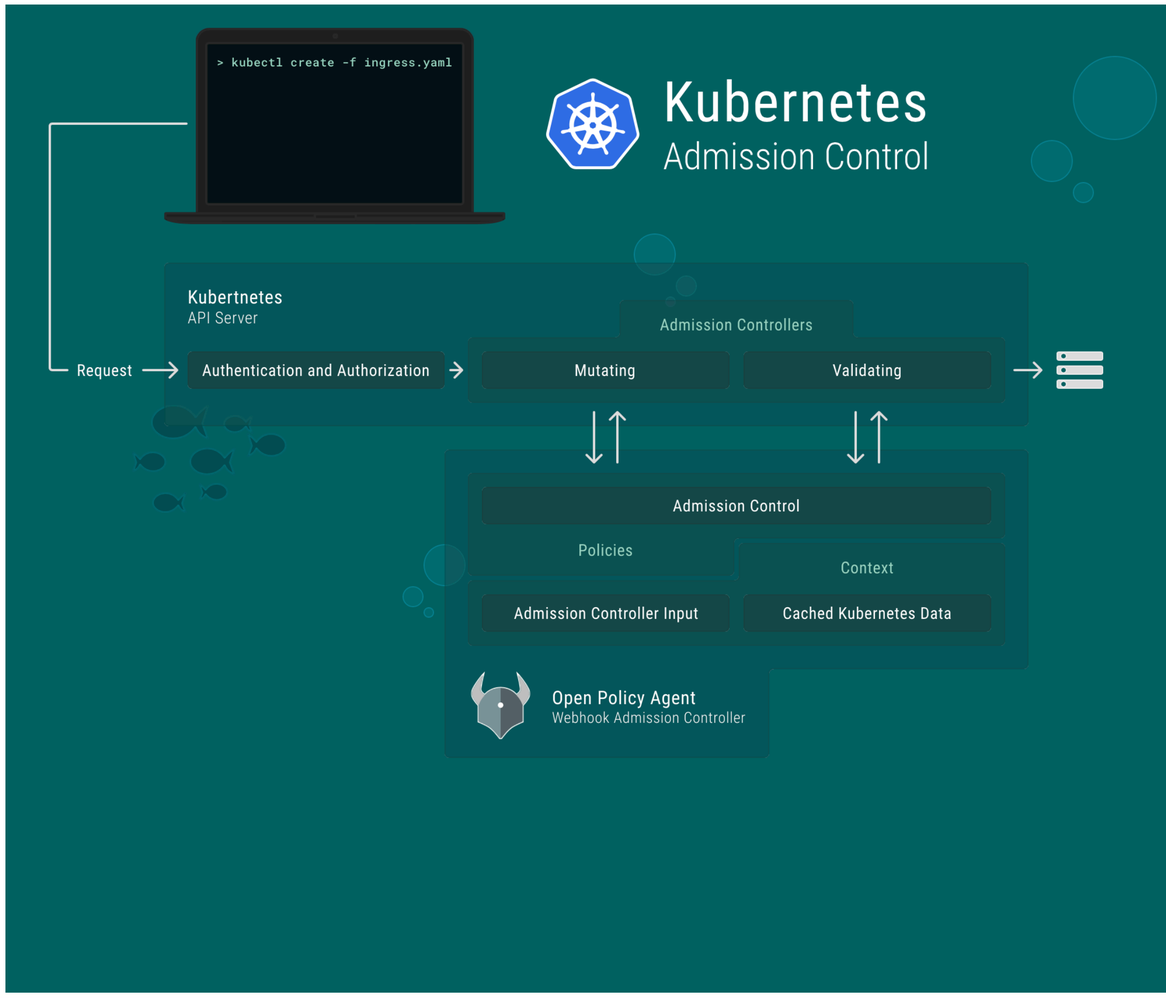
OPEN POLICY AGENT (GATEKEEPER)

- Enforce a baseline suite of policies for all cluster resources
- Policy examples (validating):
  - Only allowed images to be pulled from specified sources
  - Deny external load balancers
  - Ensure container limits are specified and reasonable
  - Only allow ingresses in a specific domain and ensure unique ingresses
- Can also add information to new resources (mutating):
  - Automatically add necessary taints/tolerations to containers (Windows, special pools, etc.)
  - Copy financing codes from the namespace object to the sub-resources

OPEN POLICY AGENT (GATEKEEPER)

- Policies are written in a language called Rego
- Policies can refer to many data sources, including:
  - The object being created and/or updated
  - Other objects in the cluster
  - External data sources fed into OPA (e.g., users/group membership, etc.)

OPEN POLICY AGENT (GATEKEEPER)

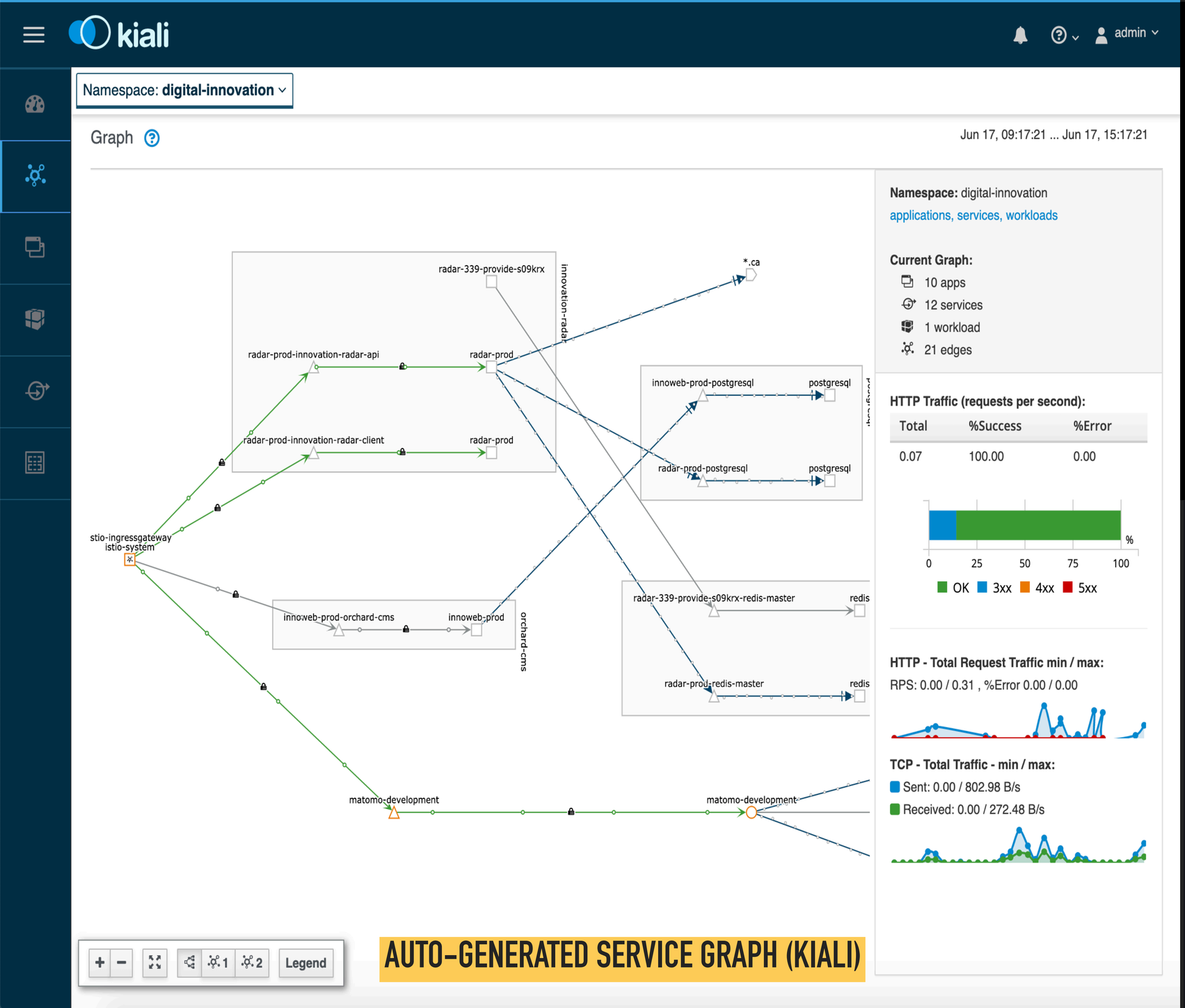


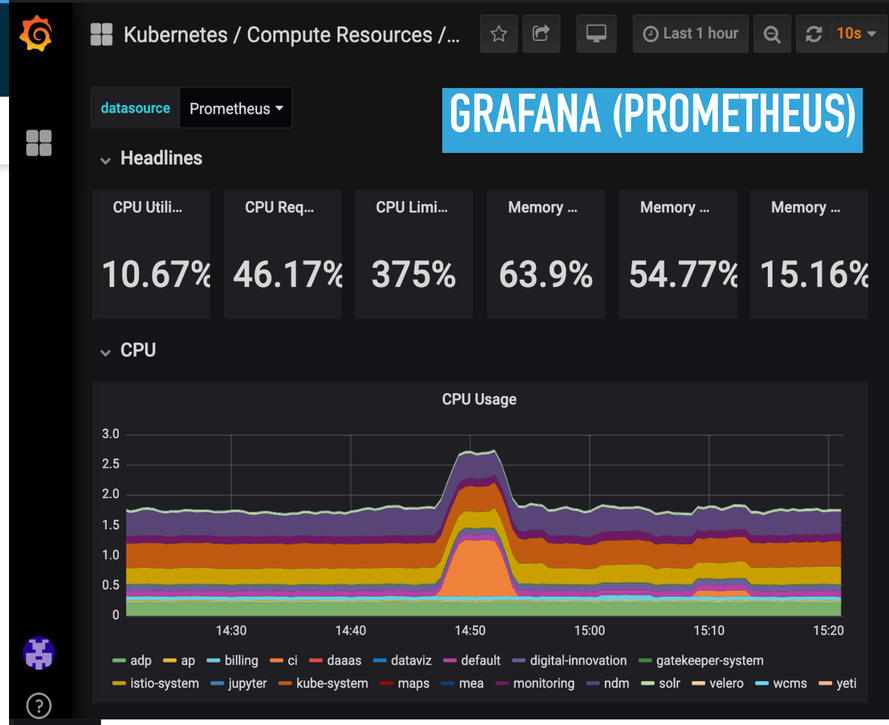
invariants.rego — ~/src/policies/admission-control/kubernetes

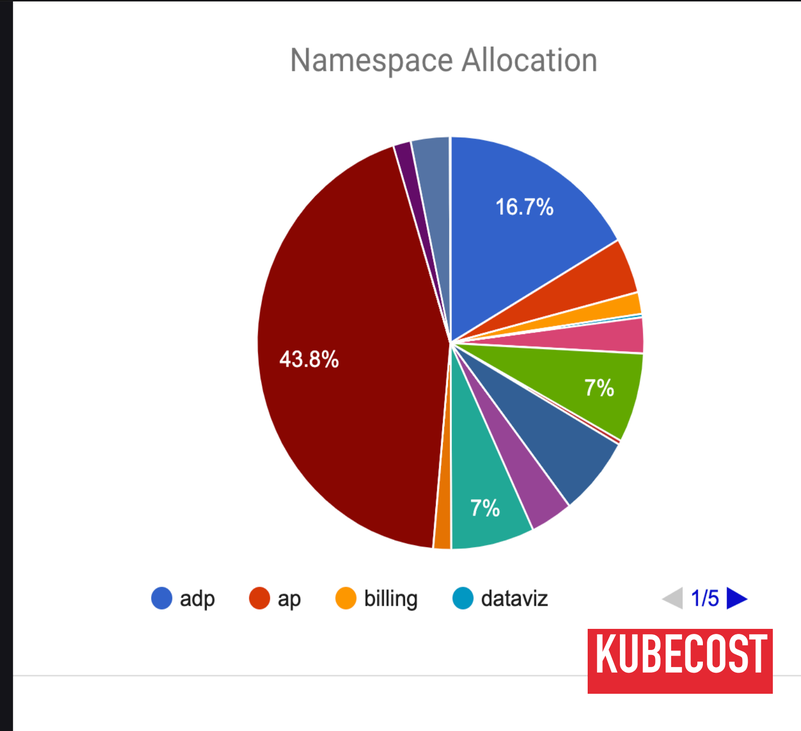
```rego
# Kubernetes Admission Control Invariants

package kubernetes.invariants

import data.kubernetes.ingresses
import data.kubernetes.namespaces

# ------------------------------------------------------------------------
# Ingress Invariants

# Generates a list of non-compliant ingresses identified by `namespace`
# and ingress specification `name`.
violations[{
    "namespace": namespace,
    "name": name,
    "message": "ingress hostname must match whitelist"
}] {
    ingress := ingresses[namespace][name]
    host := ingress.spec.rules[_].host
    not contains(whitelist[namespace], host)
}

# Generates a list of allowed hostnames per namespace.
whitelist[namespace] = hosts {
    obj := namespaces[namespace]
    annotations := obj.metadata.annotations
    annotation := annotations["acmecorp.com/hostname-whitelist"]
    hosts := json.unmarshal(annotation)
}

# ------------------------------------------------------------------------
# Helpers

# Checks if `list` includes an element matching `item`.
contains(list, item) {
    list[_] = item
}
```

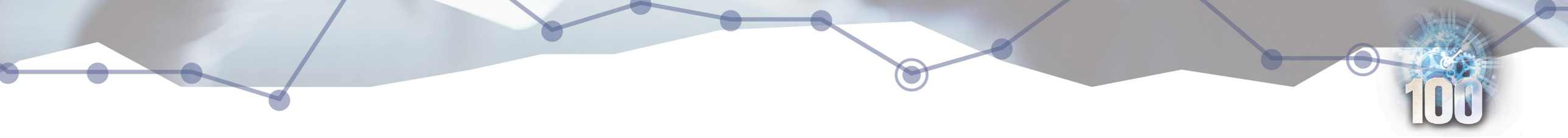
ISTIO (SERVICE MESH)

- Automatic mutual TLS between services in the cluster
  - Handled by proxy sidecar, which intercepts all network traffic. **No changes to the app.**
- Observability: tracing, monitoring and logging of all network communication
- Enhanced routing rules, including:
  - Timeouts and retries
  - Per-instance routing (e.g, 90% of traffic to v1, 10% to v2)
  - Load balancing between instances
  - Circuit breaking


kiali
admin
Namespace: digital-innovation
Graph
Jun 17, 09:17:21 ... Jun 17, 15:17:21
radar-339-provide-s09krx
innovation-radar
*.ca
radar-prod-innovation-radar-api
radar-prod
radar-prod-innovation-radar-client
radar-prod
innoweb-prod-postgresql
postgresql
radar-prod-postgresql
postgresql
stio-ingressgateway
istio-system
innoweb-prod-orchard-cms
innoweb-prod
orchard-cms
radar-339-provide-s09krx-redis-master
redis
radar-prod-redis-master
redis
matomo-development
matomo-development
Namespace: digital-innovation
applications, services, workloads
Current Graph:
10 apps
12 services
1 workload
21 edges
HTTP Traffic (requests per second):
Total
%Success
%Error
0.07
100.00
0.00
0
25
50
75
100
%
OK
3xx
4xx
5xx
HTTP - Total Request Traffic min / max:
RPS: 0.00 / 0.31 , %Error 0.00 / 0.00
TCP - Total Traffic - min / max:
Sent: 0.00 / 802.98 B/s
Received: 0.00 / 272.48 B/s
Legend
AUTO-GENERATED SERVICE GRAPH (KIALI)


Kubernetes / Compute Resources /...
Last 1 hour
10s
datasource
Prometheus
GRAFANA (PROMETHEUS)
Headlines
CPU Utili...
10.67%
CPU Req...
46.17%
CPU Limi...
375%
Memory ...
63.9%
Memory ...
54.77%
Memory ...
15.16%
CPU
CPU Usage
3.0
2.5
2.0
1.5
1.0
0.5
0
14:30
14:40
14:50
15:00
15:10
15:20
adp
ap
billing
ci
daaas
dataviz
default
digital-innovation
gatekeeper-system
istio-system
jupyter
kube-system
maps
mea
monitoring
ndm
solr
velero
wcms
yeti


Namespace Allocation
16.7%
43.8%
7%
7%
adp
ap
billing
dataviz
1/5
KUBECOST



“SERVERLESS”

KNATIVE

Event-driven, sometimes also called serverless or functions as a service, is a computing execution model in which the infrastructure/provider dynamically manages the allocation of machine resources.

Brendan Burns (Kubernetes Founder)

OVERVIEW OF KNATIVE

- Not a complete server less solution on its own. It’s a platform to build serverless.
- “The future will be containerized and those containers will run on serverless infrastructure” (Brendan Burns)
- Collaborative approach of vendors
  - Defines vendor-agnostic standards for serverless computing
- “Portability not just at the container level, but at the serverless platform level” (Jason Polites)

SERVING: HOW YOUR CODE RECEIVES REQUESTS AND SCALES WITH THEM

- Request-driven compute runtime
- Scale-to-zero / scale out per load
- Multiple revisions of the same app
- Route traffic across revisions (powered by Istio)

BUILDING: HOW YOUR CODE IS BUILT AND PACKAGED AS A CONTAINER

- Pluggable model to automatically build containers from source
- Build in-cloud or on-cluster
- Templates available (buildpacks, kaniko, etc)
  - Don’t need to create a Dockerfile for your app
  - Don’t need domain-specific knowledge

EVENTING: HOW YOUR CODE IS TRIGGERED BY EVENTS AND EXECUTED

- Apps and functions consume and publish to event streams
- Multiple event sources available, examples:
  - Kafka
  - Cloud events
  - Webhooks
  - And more!
- Encourages asynchronous, loosely coupled architecture

WHY KNATIVE?

- Provider agnostic: your code runs inside of your Kubernetes cluster
  - Current solutions like AWS Lambda, Google Cloud Functions, Azure Functions have little interoperability between each other
- Knative, rather than developers, manages cluster resources:
  - Deployments, services, ingresses, routing rules, etc.
- Knative manages application scaling based on load (scale up and down)

IN CLOSING

WRAPPING IT UP

WHAT ARE WE DOING?

- On-boarded 10+ developer teams to a unified workflow
  - Hybrid workloads: Linux and Windows
- Use Kubernetes to run our platform services
  - Source code management system, artifact repository, build and deployment tools
- We’re currently working with our IT security team to complete our security control profile
  - Isolation of workloads
  - Policies: Role Based Access Control, Network, Pod Security Policies
- Automation via Terraform

USEFUL LINKS

- The following are some useful links that should help you get started:
  - Kubernetes Learning Path
  - CNCF Landscape
  - CNCF Trail Map
  - CNCF KubeCon 2019
  - Awesome Kubernetes
  - Awesome Operators
  - GoC Cloud Native
  - Digital Academy
  - KataCoda
  - StatCan

VIDEO

https://www.youtube.com/watch?v=-Pa9KodBnGo

William Hearn

william.hearn@canada.ca

sylus

william_hearn

Questions?

Zachary Seguin

zachary.seguin@canada.ca

zachomedia

zachomedia