



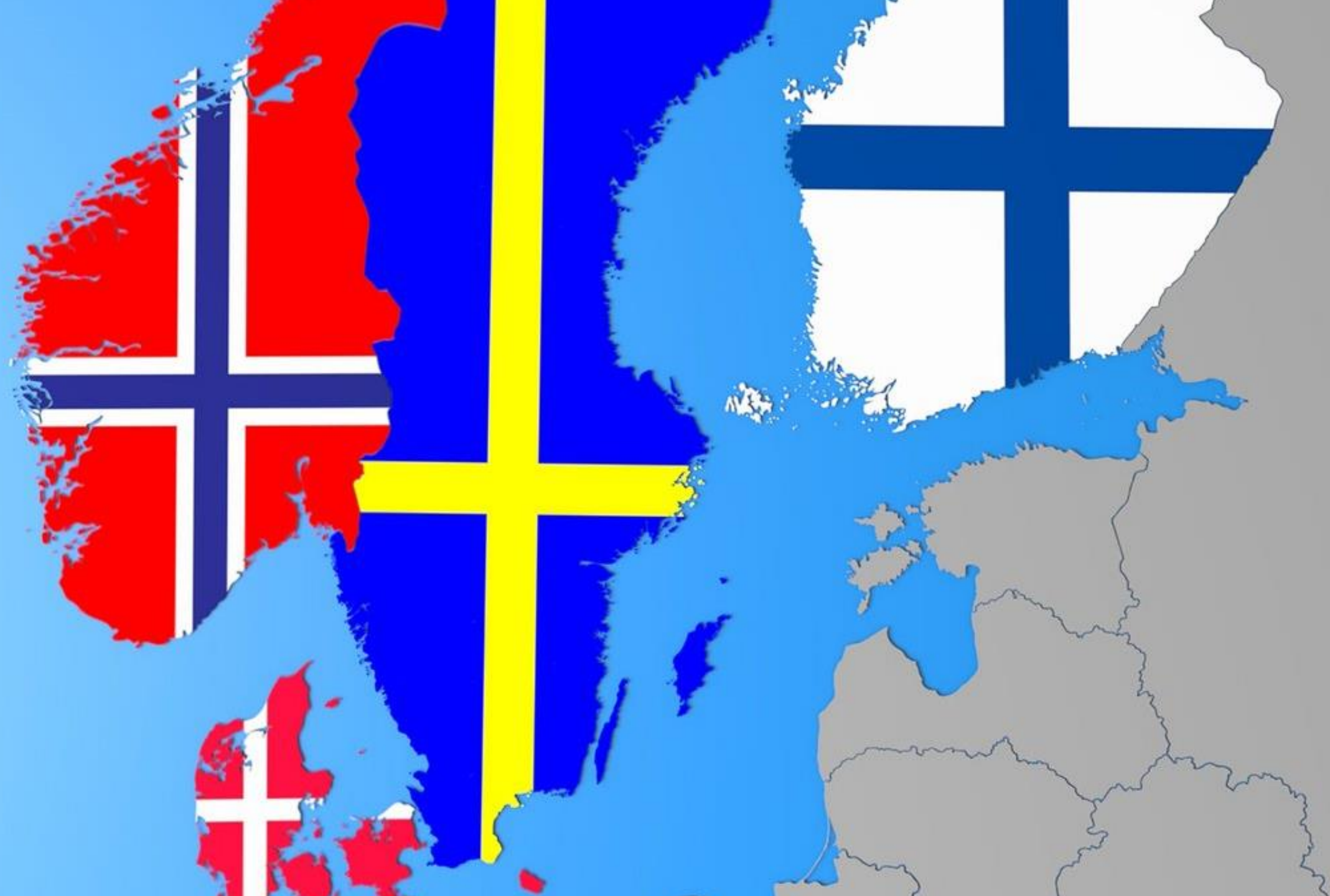
# We built a GKE platform

With only 2 engineers and lots of coffee ☕



Eline Henriksen  
Lead Product Lead  
Telenor - Cloud Platforms



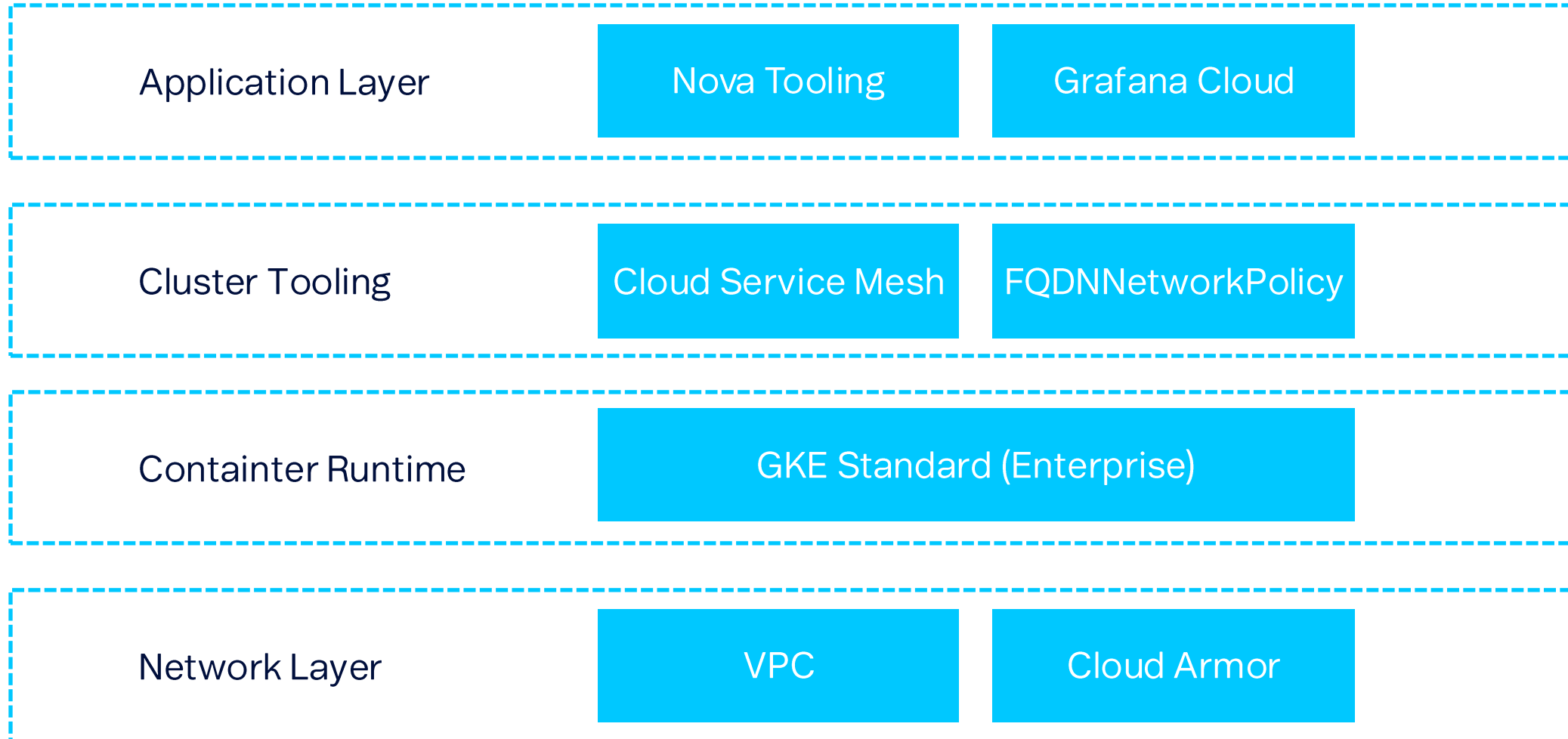






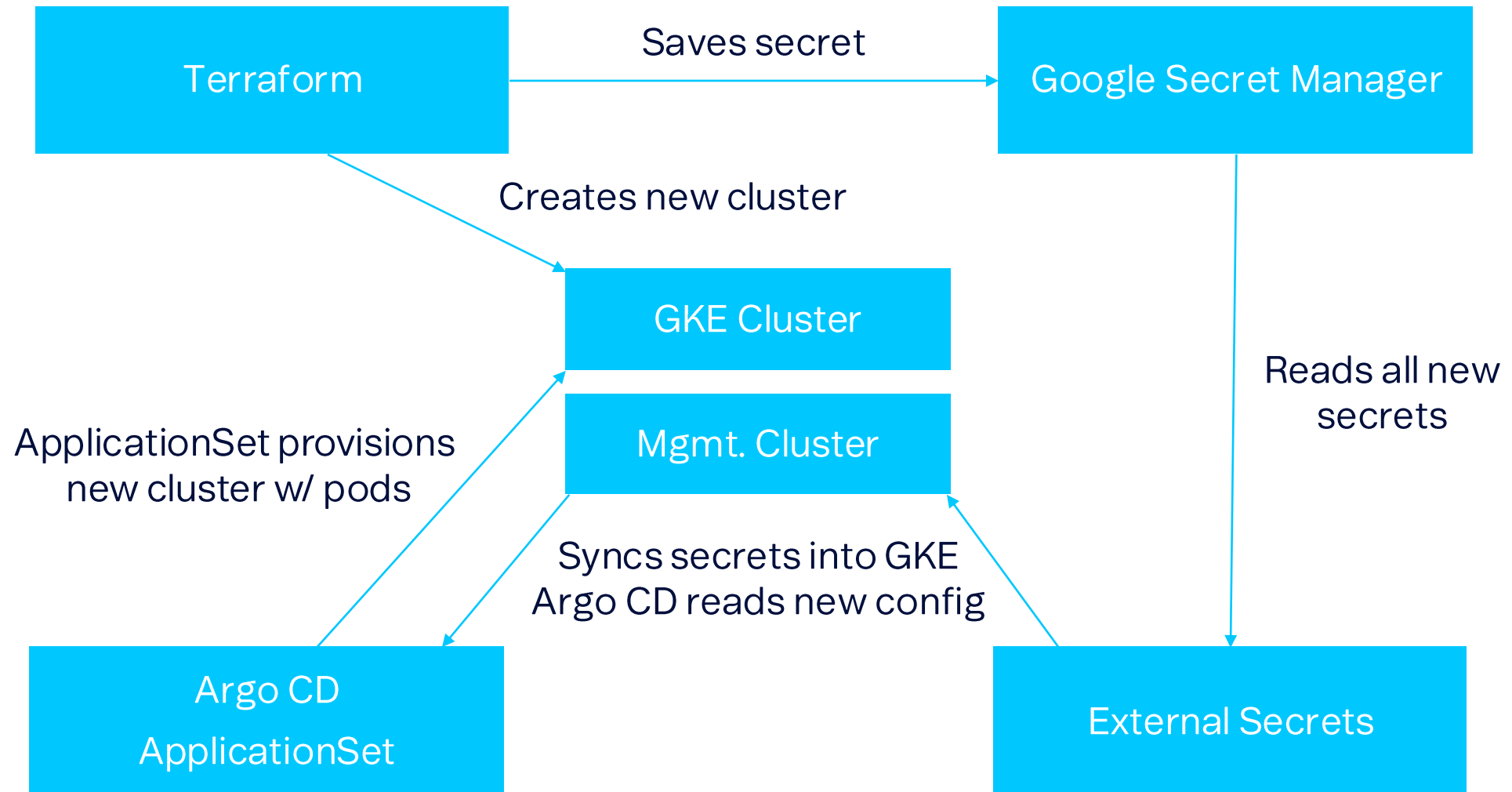
# We're a small team

Can we still deliver world-class developer experience on GKE?





Automation is key







# Managed offerings

# Cloud Service Mesh

- DA mandates mTLS
- We have (not great) experience with Istio
- We wanted as managed an offering as possible - Cloud Service Mesh!
- CSM has two modes, we use Traffic Director
- Largely one-"click" install
- In theory should make multi-cluster mesh easy too (not tested)
- GKE Sandbox is not friends with CSM TD

Google Cloud X Shared - T Search (/) for resources, docs, products and more Search

Service mesh / Services / Service view: frontend / Overview

ENTERPRISE

All fleets

Fleet tdk-tx-x-shared

Overview

Health

Metrics

Connected Services

Diagnostics

Infrastructure

Traffic

Security

Resources

Marketplace

Release notes

<1

t-s1-nova-example/frontend

Alerts timeline No service alerts Time selection is 12:02 pm to 1:02 pm GMT+1 Reset Time Span 1 hour Show timeline

Service status: none

There are no SLOs set for this service.

Create an SLO

Topology metric Requests/sec (avg)

0 services frontend

Details

Namespace t-s1-nova-example Name frontend

Description -- Clusters [t-x-shared-01](#)

Type Service

Traffic 1.1 0% Server error rate 58.7% 0%

Client error rate 0.0% 0% P50 latency 1ms 0%

P95 latency 4ms 0% CPU utilisation 0.3% 0%

Memory utilisation 6.1% +2%

```
resource "google_gke_hub_feature" "servicemesh" {
  name      = "servicemesh"
  location  = "global"
  project   = var.project_id
  fleet_default_member_config {
    mesh {
      management = "MANAGEMENT_AUTOMATIC"
    }
  }
}
```

Recommendations

The server error rate is elevated and has averaged 60.00% over the past 24 hours.

View on metrics page

Was this helpful? 👍 👎





# Use built-in features

# FQDNNetworkPolicy

- GKE Dataplane v2 is based on Cilium
- Cilium has L7 NetworkPolicy
- GKE made their own, FQDNNetworkPolicy
- Works well
- GKE also provides CiliumClusterwideNetworkPolicy

```
apiVersion: networking.gke.io/v1alpha1
kind: FQDNNetworkPolicy
metadata:
  name: allow-out-fqdnnp
spec:
  podSelector:
    matchLabels:
      app: curl-client
  egress:
    - matches:
      - pattern: "*.yourdomain.com"
      - name: "www.google.com"
    ports:
      - protocol: "TCP"
        port: 443
```





Don't write code when you don't have to

# controller-runtime & operator pattern

```
// Setup a new controller to reconcile ReplicaSets
entryLog.Info(msg: "Setting up controller")
c, err := controller.New(name: "foo-controller", mgr, controller.Options{
    Reconciler: &reconcileReplicaSet{client: mgr.GetClient(), log: log.WithName(name: "reconciler")},
})
if err != nil {
    entryLog.Error(err, msg: "unable to set up individual controller")
    os.Exit(code: 1)
}

// Watch ReplicaSets and enqueue ReplicaSet object key
if err := c.Watch(&source.Kind{Type: &apps1.ReplicaSet{}}, &handler.EnqueueRequestForObject{}); err != nil {
    entryLog.Error(err, msg: "unable to watch ReplicaSets")
    os.Exit(code: 1)
}

// Watch Pods and enqueue Pod object key
if err := c.Watch(&source.Kind{Type: &core1.Pod{}}, &handler.EnqueueRequestForObject{}); err != nil {
    entryLog.Error(err, msg: "unable to watch Pods")
    os.Exit(code: 1)
}
```

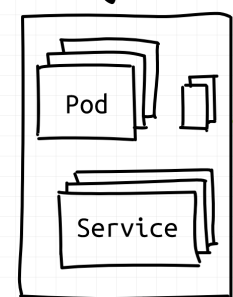
## kubernetes-sigs/ controller-runtime

Repo for the controller-runtime subproject of  
kubebuilder (sig-apimachinery)

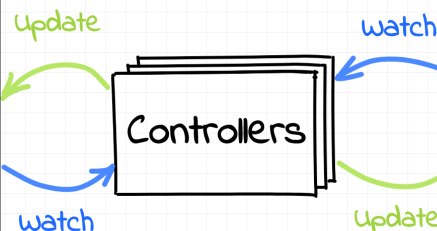
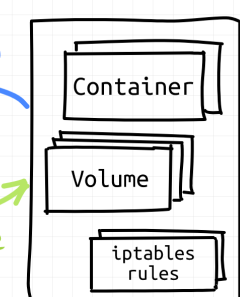


352 Contributors  
15 Used by  
3k Stars  
1k Forks

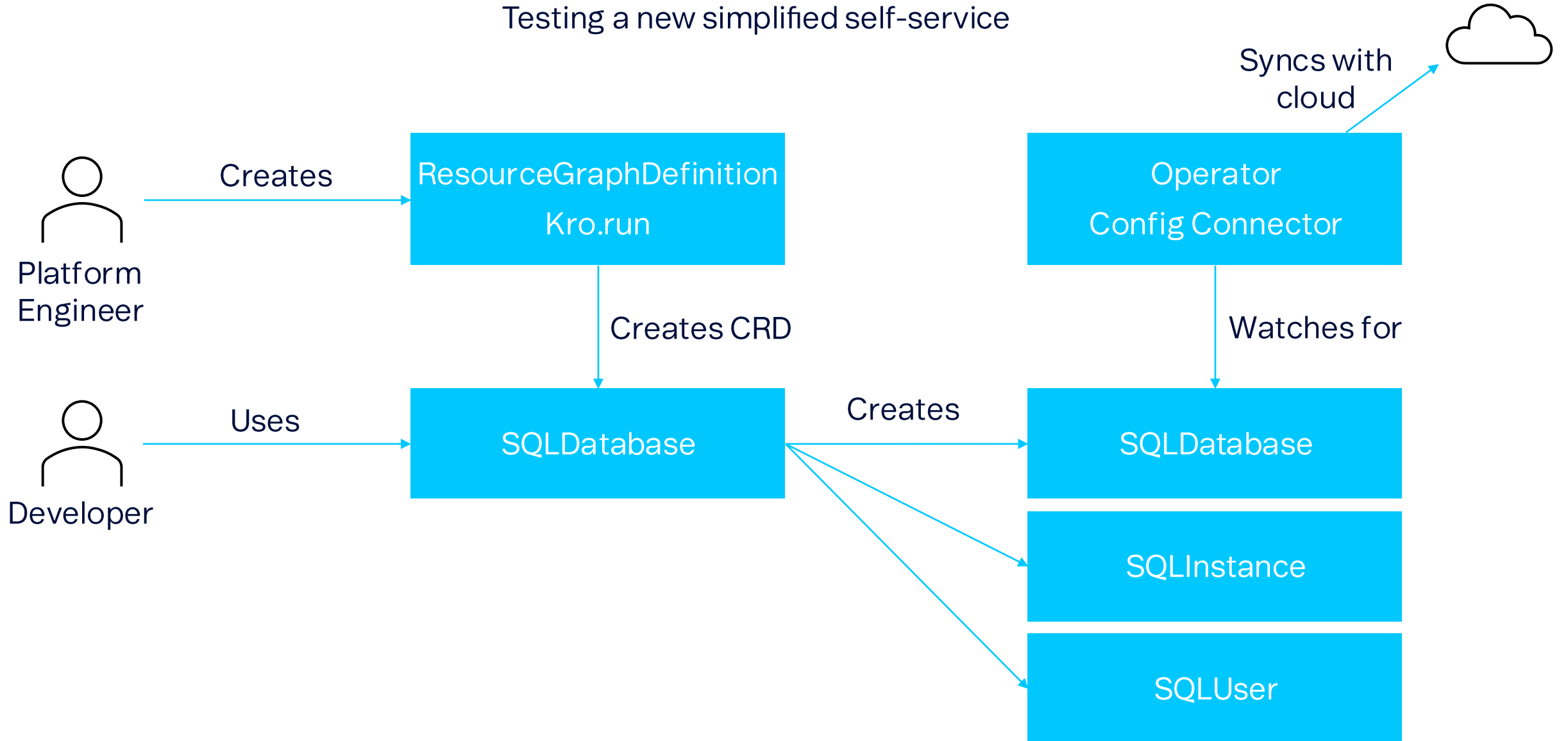
## Kubernetes objects



## System Resources



# Testing a new simplified self-service





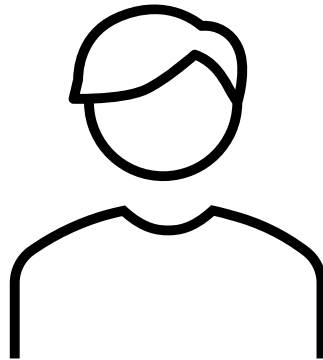
# Lessons learned



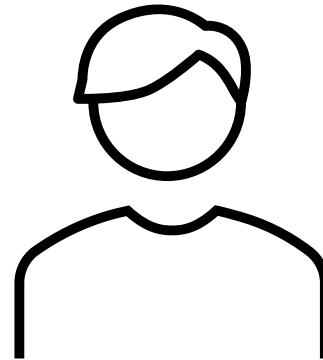
# Biggest challenge – Attrition risk



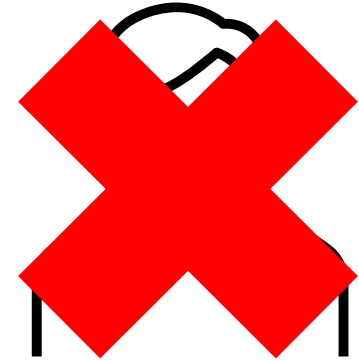
Promoted



Transferred



Hired



Quit



# Lessons learned

- Attrition risk manageable if you keep complexity low and use industry standard tools
- Build as little as possible yourself
- Use managed services
- Use built-in Kubernetes stuff (VAP, PSS)
- Automation is key
- Consider Autopilot

And finally:

It's possible to run a serious GKE operation with a handful of people if you play your cards right!





Thanks!