Cilium project

Welcome, Vision & Updates

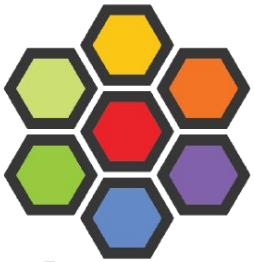
Thomas Graf
Isovalent

Laurent Bernaille
Datadog

Purvi Desai
Google

Liz Rice
Isovalent

cilium



cilium

Created by ISOVALENT

eBPF-based:

- Networking
- Security
- Observability
- Service Mesh & Ingress

Foundation

CLOUD NATIVE COMPUTING FOUNDATION

Technology

eBPF envoy

Wild Life

Building a Global Multi Cluster Gaming Infrastructure with Cilium

Adobe

What Makes a Good Multi-tenant Kubernetes Solution

Capital One

Building a Secure and Maintainable PaaS

Alibaba Cloud

Building High-Performance Cloud-Native Pod Networks

MÁSMÓVIL

Scaling a Multi-Tenant k8s Cluster in a Telco

Trip.com

First step towards cloud native networking

CENGN

Cloud Native Networking with eBPF

DigitalOcean

Managed Kubernetes: 1.5 Years of Cilium Usage at DigitalOcean

Google

Google chooses Cilium for Google Kubernetes Engine (GKE) networking

Bell

Why eBPF is changing the Telco networking space?

GitLab

Kubernetes Network Policies in Action with Cilium

aws

AWS picks Cilium for Networking & Security on EKS Anywhere

Scaleway

Scaleway uses Cilium as the default CNI for Kubernetes Kapsule

sportradar

Sportradar is using Cilium as their main CNI plugin in AWS (using kops)

Utmost

Utmost is using Cilium in all tiers of its Kubernetes ecosystem to implement zero trust

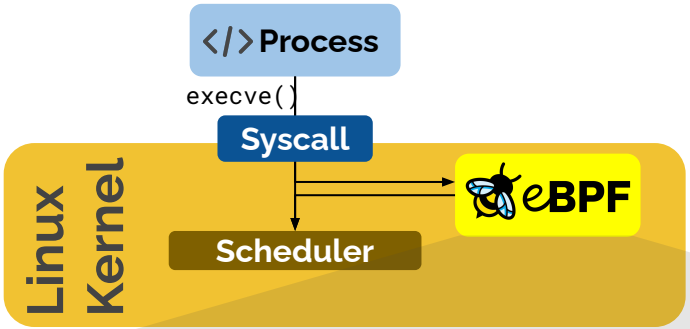
yahoo!

Yahoo is using Cilium for L4 North-South Load Balancing for Kubernetes Services

eBPF

Makes the Linux kernel programmable in a secure and efficient way.

“What JavaScript is to the browser, eBPF is to the Linux Kernel”




```c
int syscall__ret_execve(struct pt_regs *ctx)
{
        struct comm_event event = {
                .pid = bpf_get_current_pid_tgid() >> 32,
                .type = TYPE_RETURN,
        };

        bpf_get_current_comm(&event.comm, sizeof(event.comm));
        comm_events.perf_submit(ctx, &event, sizeof(event));

        return 0;
}
```

Cilium
CNI

Scalable, Secure,
High Performance
CNI Plugin

Cilium CNI

Scalable, Secure, High Performance CNI Plugin

Cilium Service Mesh

Sidecar-free Mesh & Ingress

Cilium
CNI

Scalable, Secure,
High Performance
CNI Plugin

Cilium
Service Mesh

Sidecar-free Mesh &
Ingress

Hubble

Network
Observability

Cilium CNI

Scalable, Secure, High Performance CNI Plugin

Cilium Service Mesh

Sidecar-free Mesh & Ingress

Hubble

Network Observability

Tetragon

Security Observability & Runtime Enforcement

Cilium CNI Overview

Efficient and Scalable Kubernetes CNI

- IPv4, IPv6, NAT46, SRv6, ...
- Overlays, BGP, Cloud Provider SDNs

High-performance Load-Balancing

- Kubernetes Services
- North-South load-balancer
- Kubernetes Ingress

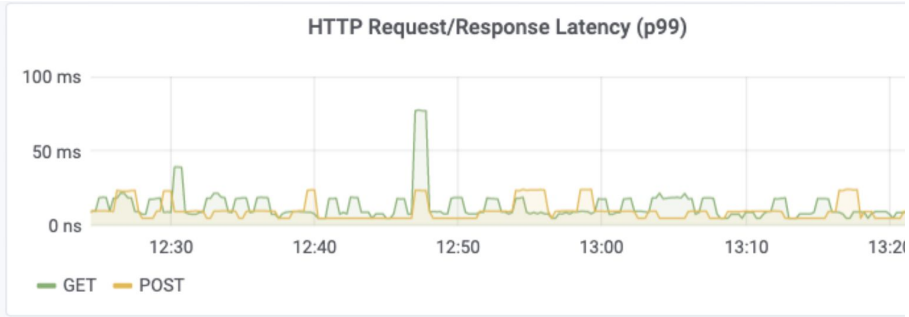
Network Policies & Encryption

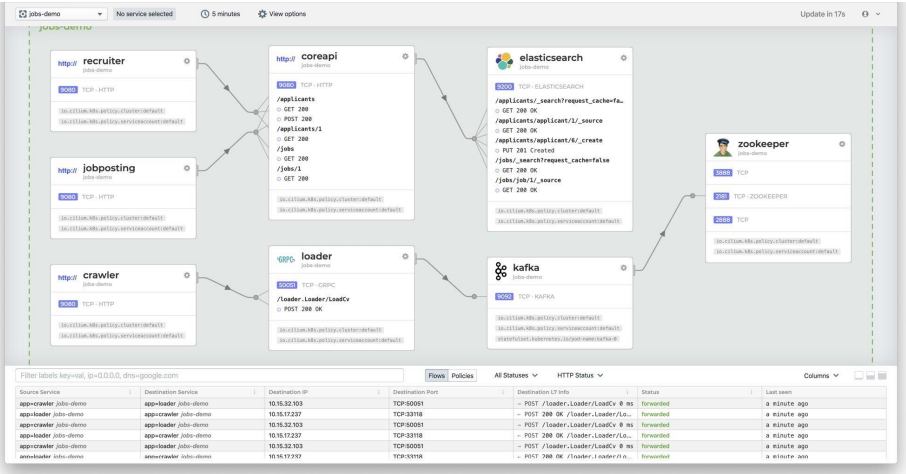
- Kubernetes Network Policy
- Cilium Network Policy (FQDN, L7, ...)
- Transparent Encryption

Multi-Cluster & External Workloads

- Global Services, Service Discovery, Network Policy
- Integration of Metal & VMs
- Egress Gateway

Hubble Observability





Metrics, Logs, & Service Map

- L3/L4
- L7 (HTTP, DNS, Kafka, ...)
- Network Policy
- ...

Cilium Service Mesh

Option 1:
Sidecar-free

eBPF + envoy

Option 2:
Istio Integration

eBPF + Istio

Control plane of your choice

SMI · Istio · Ingress / Services · Gateway API · SPIFFE · Linkerd(?)

Observability Integrations

fluentd · JSON · Grafana · OpenTelemetry

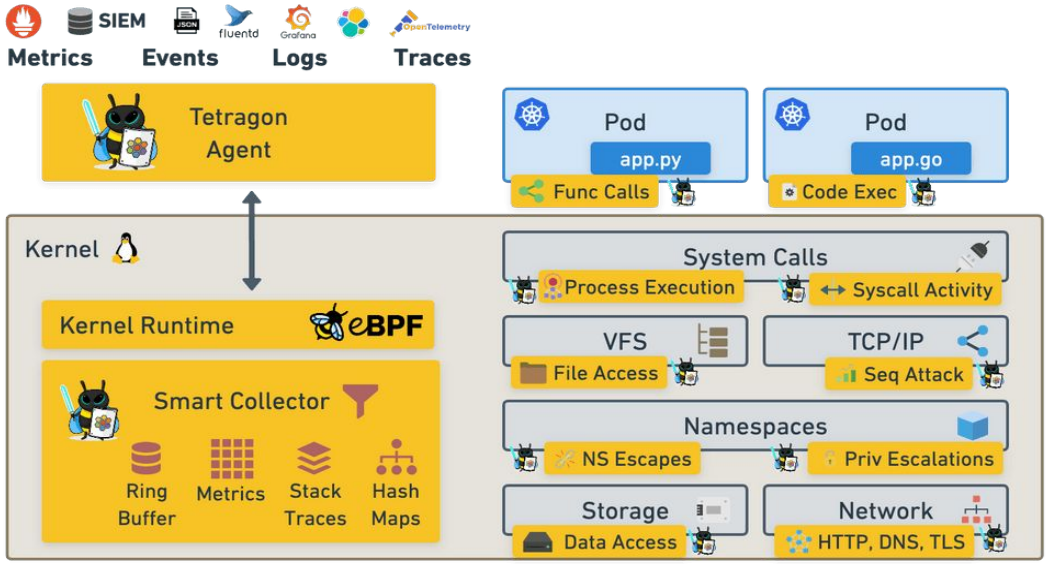
Tetragon

Security Observability & Runtime Enforcement

CLOUD NATIVE COMPUTING FOUNDATION

```
root@ubuntu2:/# /root/cve-2021-22555
[+] Linux Privilege Escalation by theflow@ - 2021

[+] STAGE 0: Initialization
[*] Setting up namespace sandbox...
[...]
[+] STAGE 5: Post-exploitation
[*] Escaping container...
[*] Cleaning up...
[*] Popping root shell...
Killed
```



Cilium 1.13 Roadmap

- Service Mesh Control Plane Integrations
- Gateway API Support
- SPIFFE Integration
- Next-Gen mTLS Authentication
- ...

Tell us what else you need!

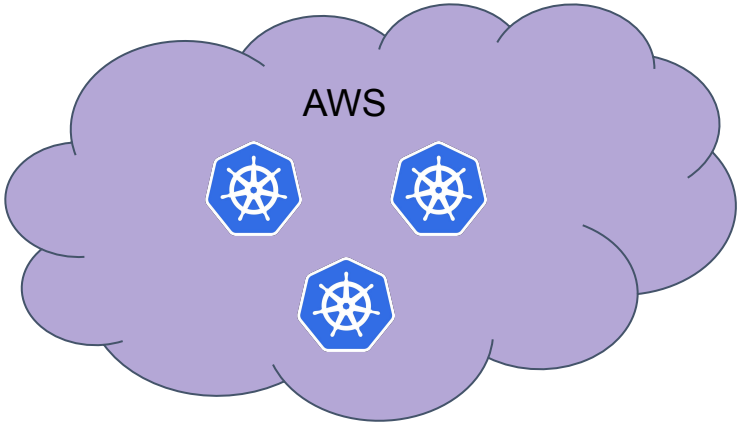
Cilium at Datadog

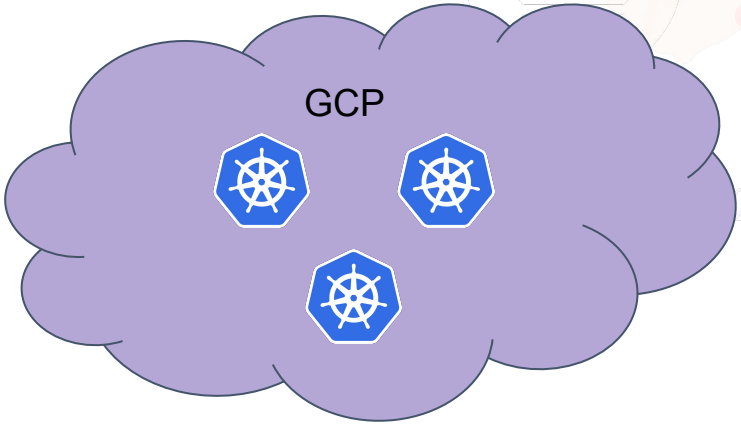
Datadog

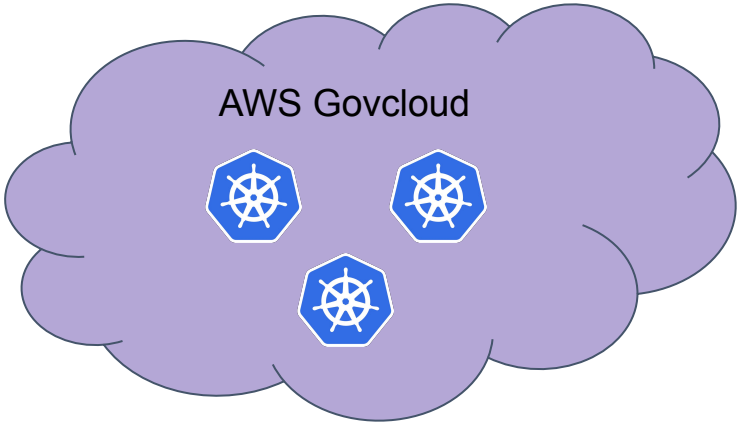
Over 500 integrations
Over 3,000 employees
Over 18,500 customers
Runs on millions of hosts
Tens of trillions of events per day

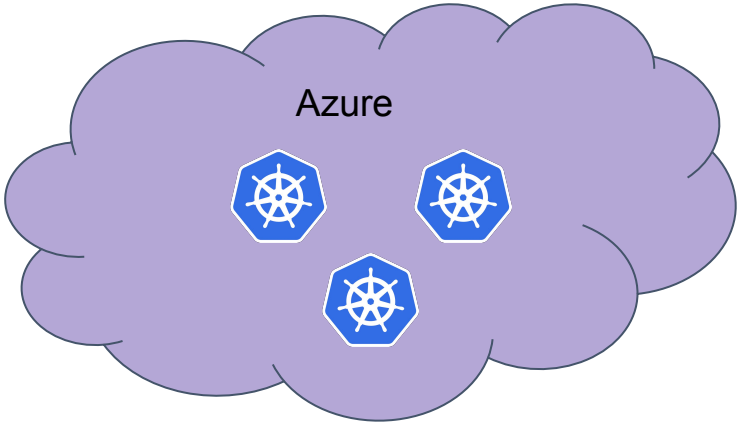
Tens of thousands of nodes
Hundreds of thousands of pods
10s of k8s clusters with 100-4000 nodes
Multi-cloud
Very fast growth

The Datadog infrastructure

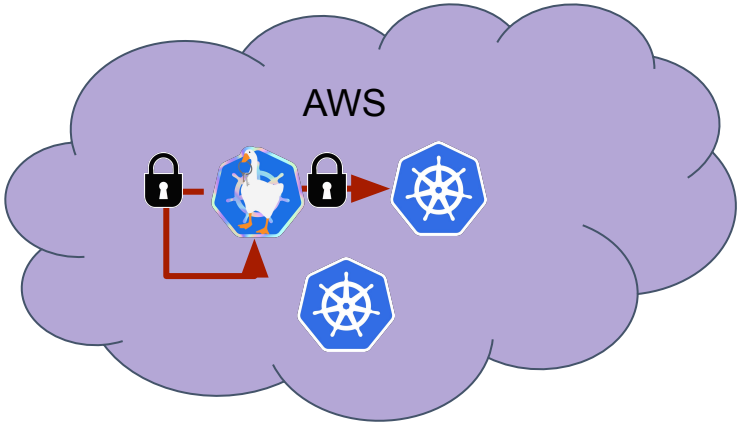


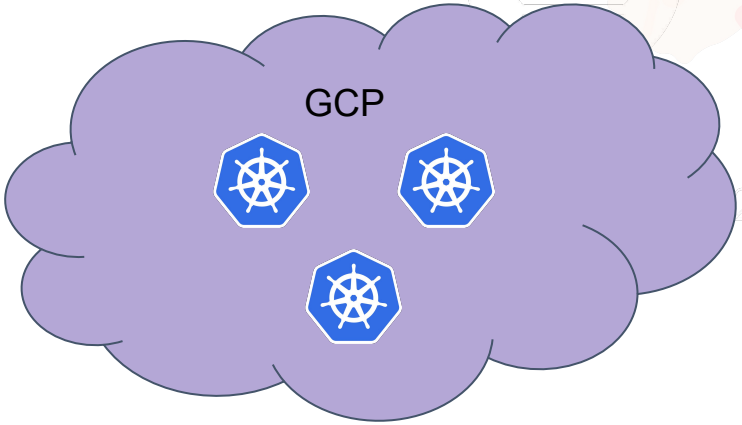


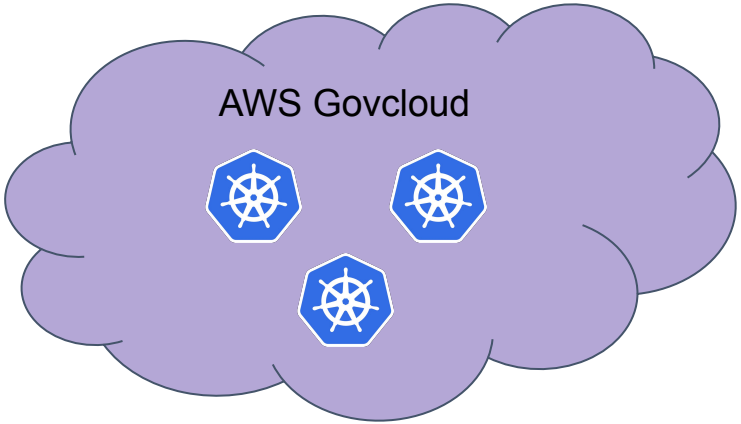


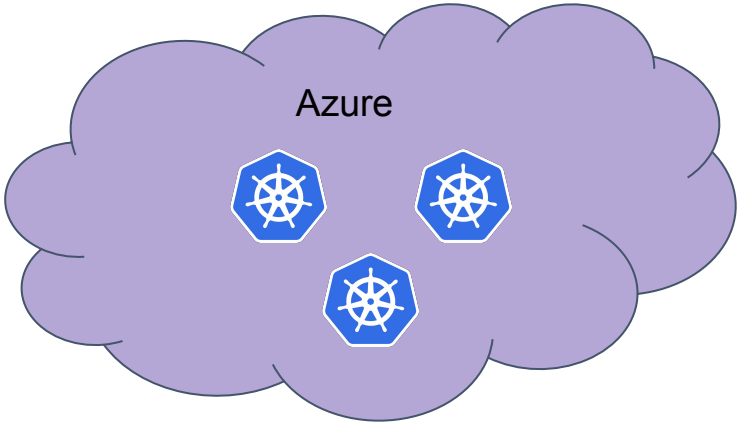


Challenges









Routable pod IPs

Advantages

- Performance
- Direct cross-cluster

Challenges

- Managing IP space
- Cross-cluster Discovery

Initial solution

AWS

- Lyft CNI plugin

GCP

- IP alias ranges
- PTP plugin

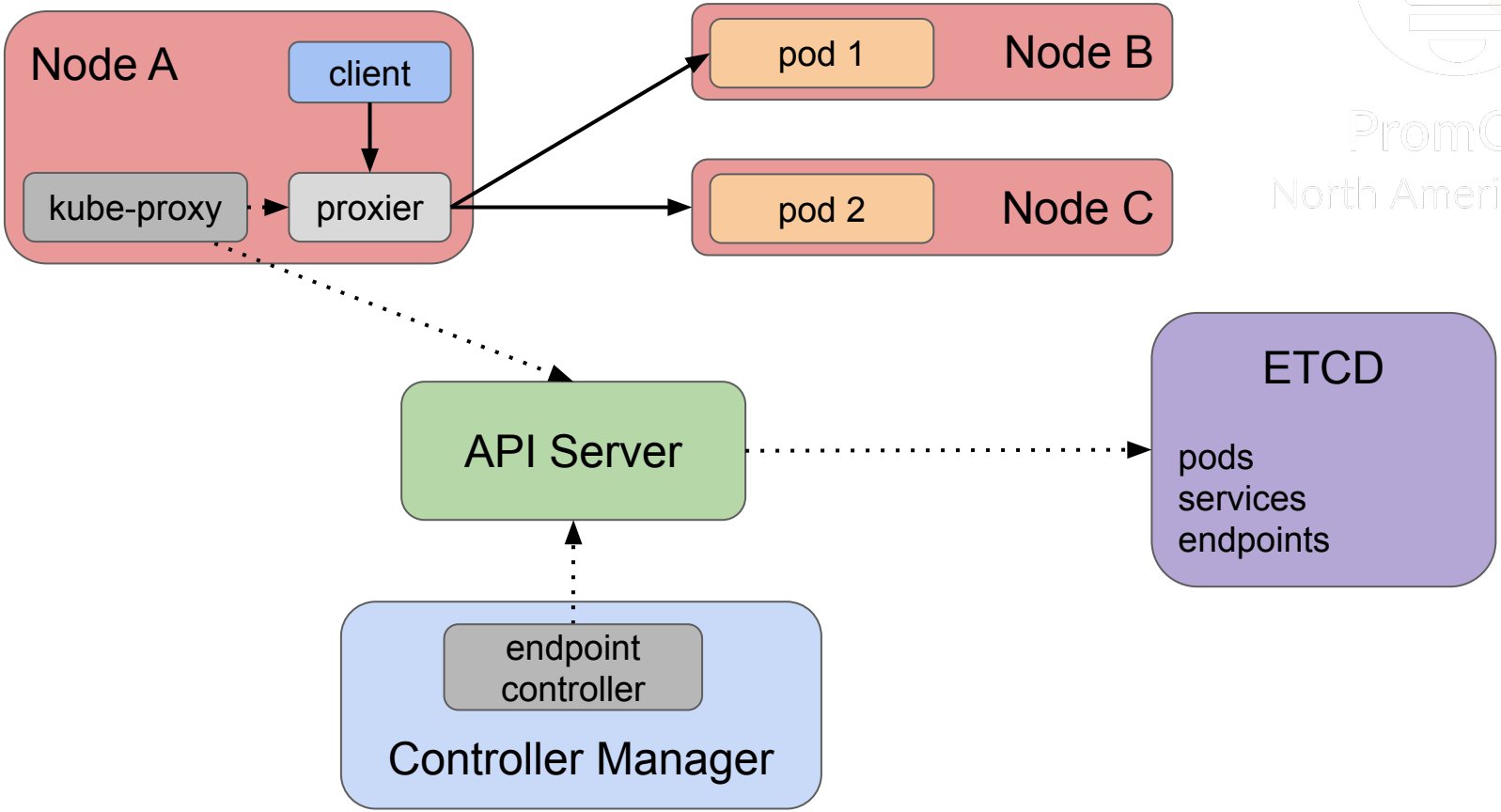
Other cloud providers: ?

Challenges

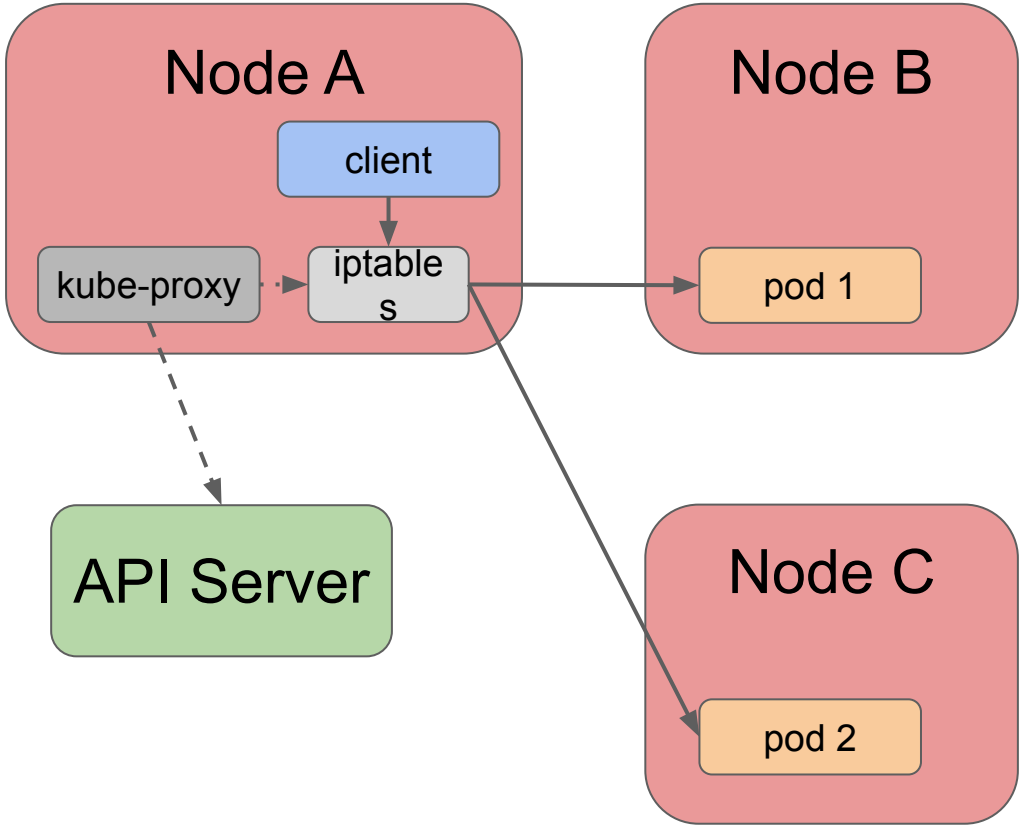
- Provider differences
- Network policy lacking
- No encryption option

Another Challenge: Service Load Balancing

Internal service load balancing



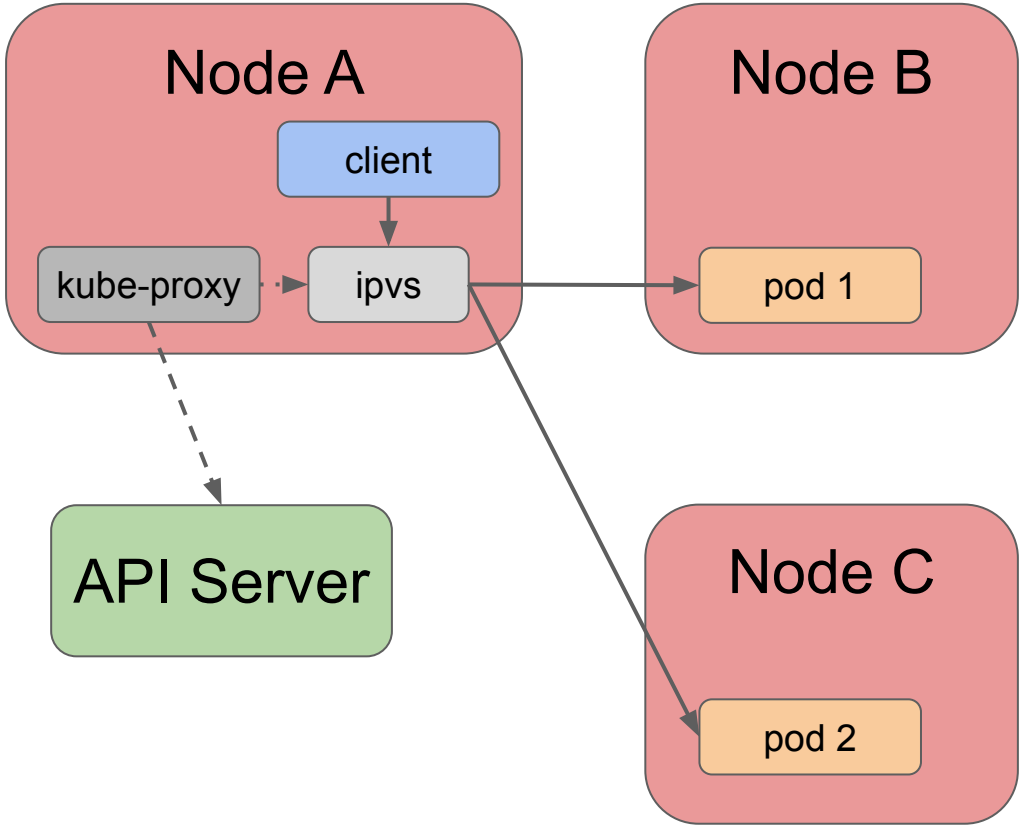
kube-proxy: iptables mode



Challenges

- Rule count
- Update time
- Matching time

kube-proxy: IPVS mode



Challenges

- Connection tracking
- Lacks feature parity

Summary: Growing pains...

- IPVS / iptables
  - not designed for client-side load balancing
- Kernel fixes/improvements slow (veth bug)
- Network policies: iptables?

What if we could dynamically program these features?

From users to contributors

From users to contributors

- We use Cilium at significant scale
- We have a few specific use cases
- We really felt welcome
- A few recent contributions
  - Prefix delegation on AWS (Hemanth Malla)
  - Make stale IPs unroutable on pod deletion

GKE Dataplane V2 and Cilium

Purvi Desai
Director of Engineering, Kubernetes Networking, Google Cloud

GKE DPv2 - Launched in 2020

Kubernetes superpower : developer-first networking model

Opinionated dataplane that harnesses the power of eBPF and Cilium for managed Kubernetes service

Strong customer adoption and feedback

Continued commitment to Cilium Open Source

Journey Ahead

Magnify commitment to Cilium Open Source

- Upstream new innovations
- Coordination between Cilium and Kubernetes

Power of AND not OR

Modular, Pluggable, Composable in manner of Kubernetes

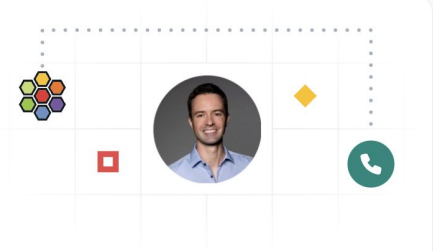
Northstar - GKE as vibrant and open ecosystem of innovative networking features

Getting started with Cilium

cilium.io/get-started

docs.cilium.io

cilium.io/slack



Weekly Interactive Cilium Introduction and Live Q&A

With Thomas Graf, Cilium Co-Creator

Book your seat

Documentation & Tutorials

Quickly get started with Cilium. Read the documentation or use our interactive tutorial in a live environment.

Documentation

Tutorials

Getting help - and giving it

cilium.io/slack

- Community assistance
- Feature-specific channels e.g. #service-mesh, #tetragon…

github.com/cilium

- Issues

Feature ideas

 cilium.io/slack

 github.com/cilium

- New Issue: Feature requests
- CFP template

 docs.cilium.io/en/latest/community/roadmap

Code contributions

Developer documentation

cilium.io/slack

github.com/cilium good-first-issue

Weekly developer call & SIGs

- github.com/cilium/cilium#community

Cilium in your community

cilium.io/get-help

- Blog posts
- Slides
- Swag
- Speakers

Feedback and ideas

cilium.io

github.com/cilium

See you on Slack!