
Cilium +
eBPF Day
NORTH AMERICA

Hubble beyond Cilium

Anubhab Majumdar and Mathew Merrick

Speakers

Cilium + eBPF Day NORTH AMERICA

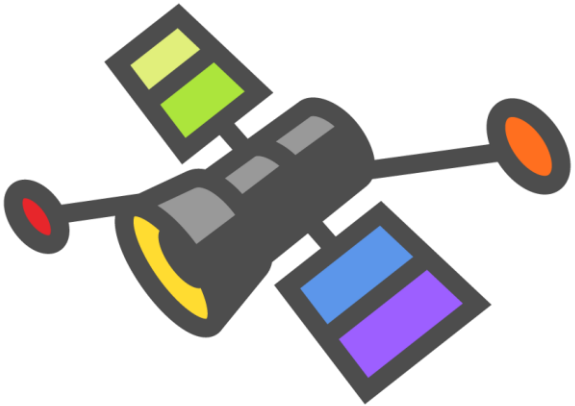
November 12, 2024
Salt Lake City

Anubhab Majumdar
Senior Software Engineer
Microsoft

Mathew Merrick
Software Engineer II
Microsoft

What is Hubble

- Hubble is a fully distributed networking and security observability platform for cloud native workloads.
- Built with eBPF
- Tightly coupled with Cilium
- Brings network level insights to fundamental Kubernetes resources



Problem

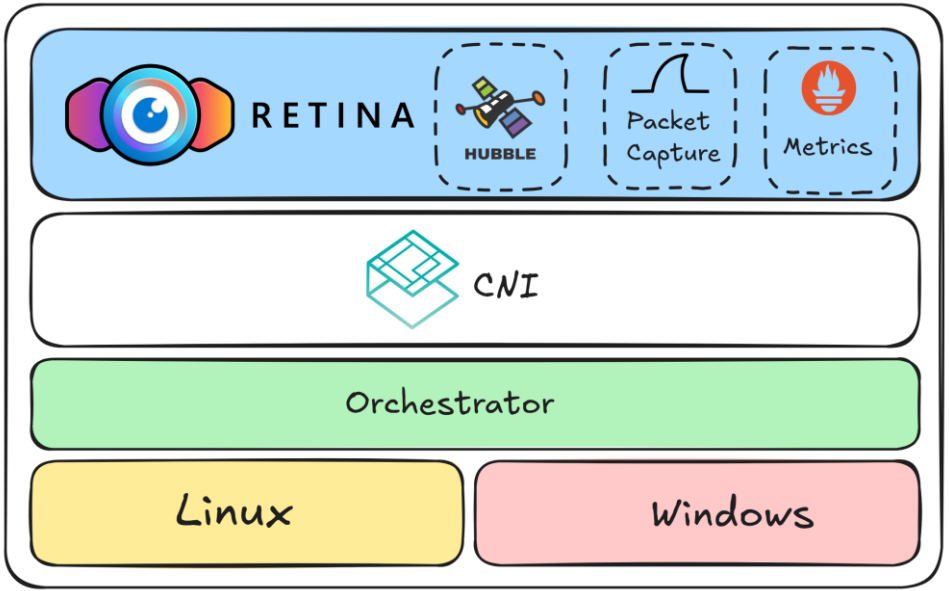
- In some cases, people want the Hubble network observability tooling without changing their underlying CNI, which brought us to two main questions:
- Can the Hubble experience live beyond Cilium?
- Can we take the Hubble experience beyond Linux?

Retina

Retina is a cloud-native container networking observability and security platform developed by Microsoft. It helps Kubernetes users visualise, observe, debug, and analyse workload traffic.

Characteristics:

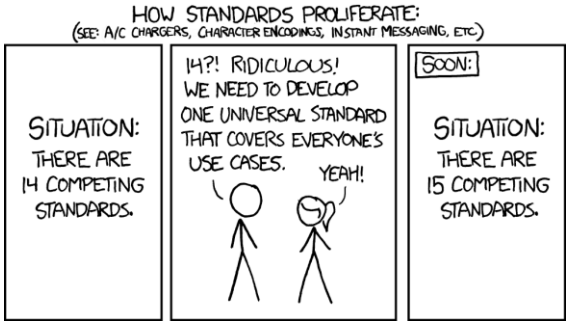
- Platform agnostic
- CNI Agnostic
- eBPF based
- Offers industry standard metrics



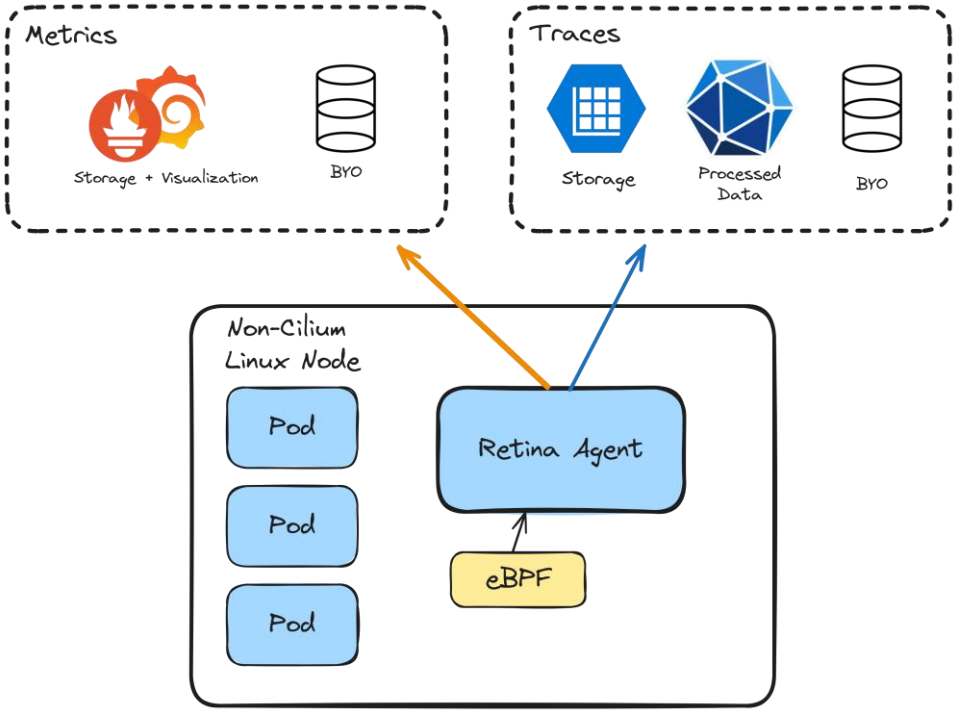
Overview

Retina's fundamental goal from the start was to just get metrics off the machine, to be visualized and processed elsewhere.

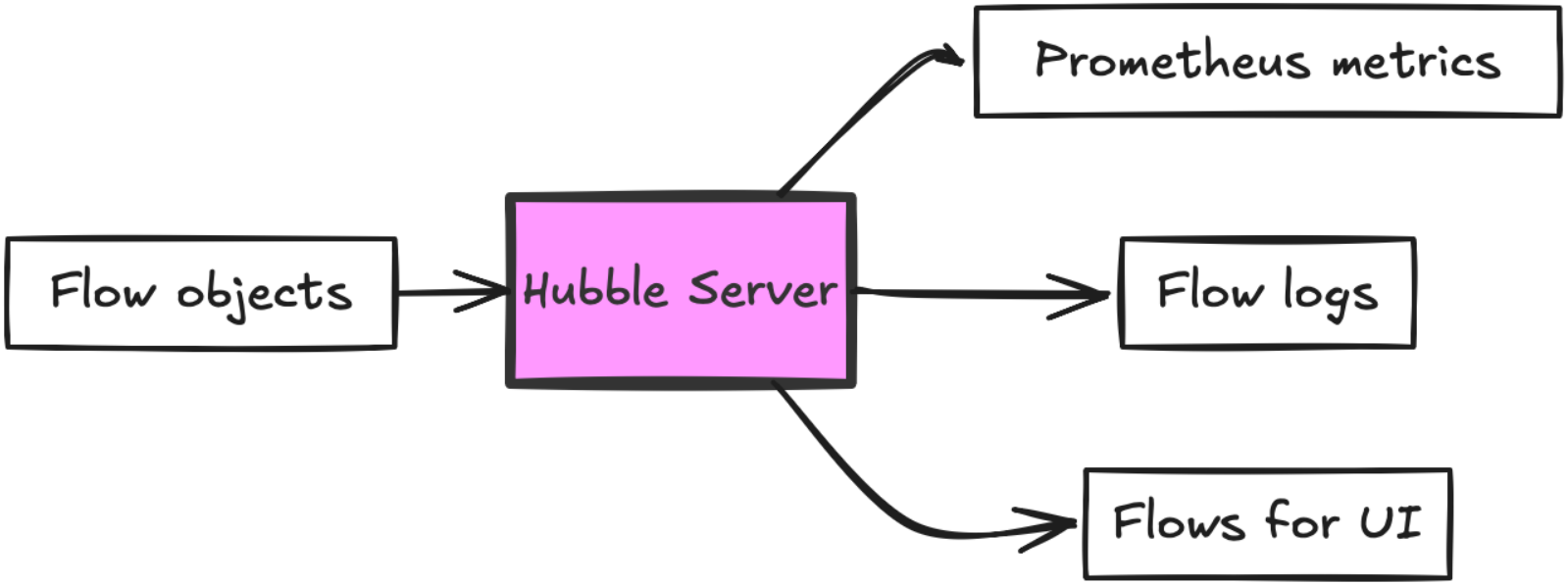
Plenty of other tooling can do great processing and visualizations, like Grafana and Hubble UI.



source: xkcd

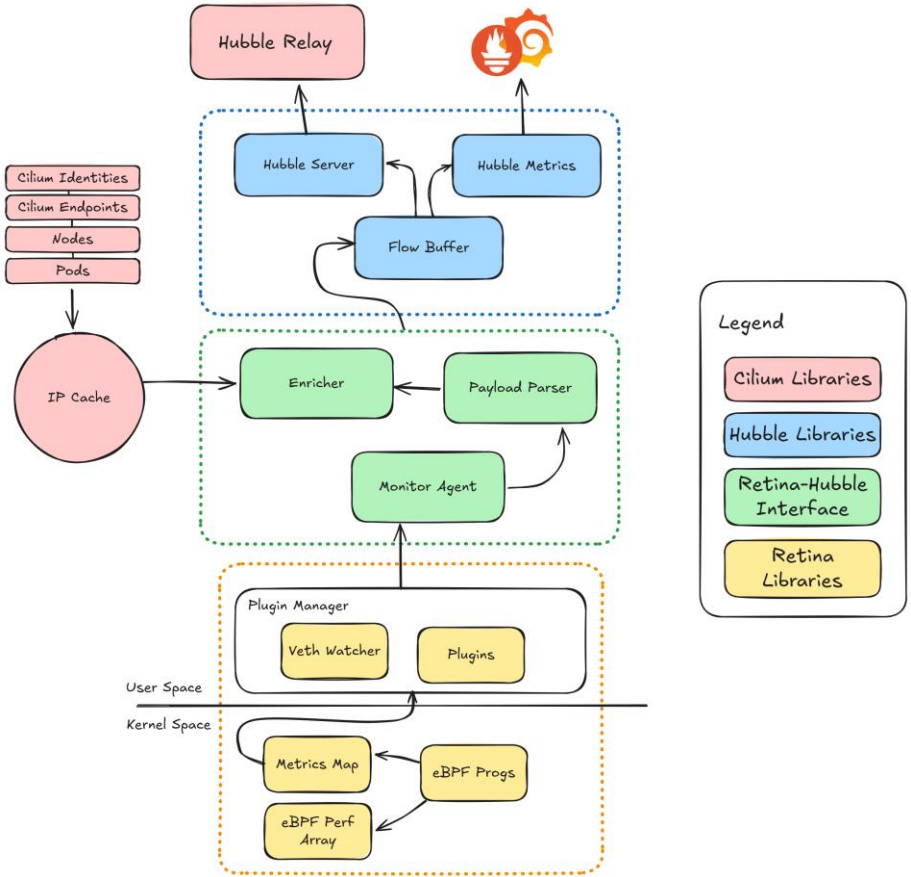


Hubble API contract

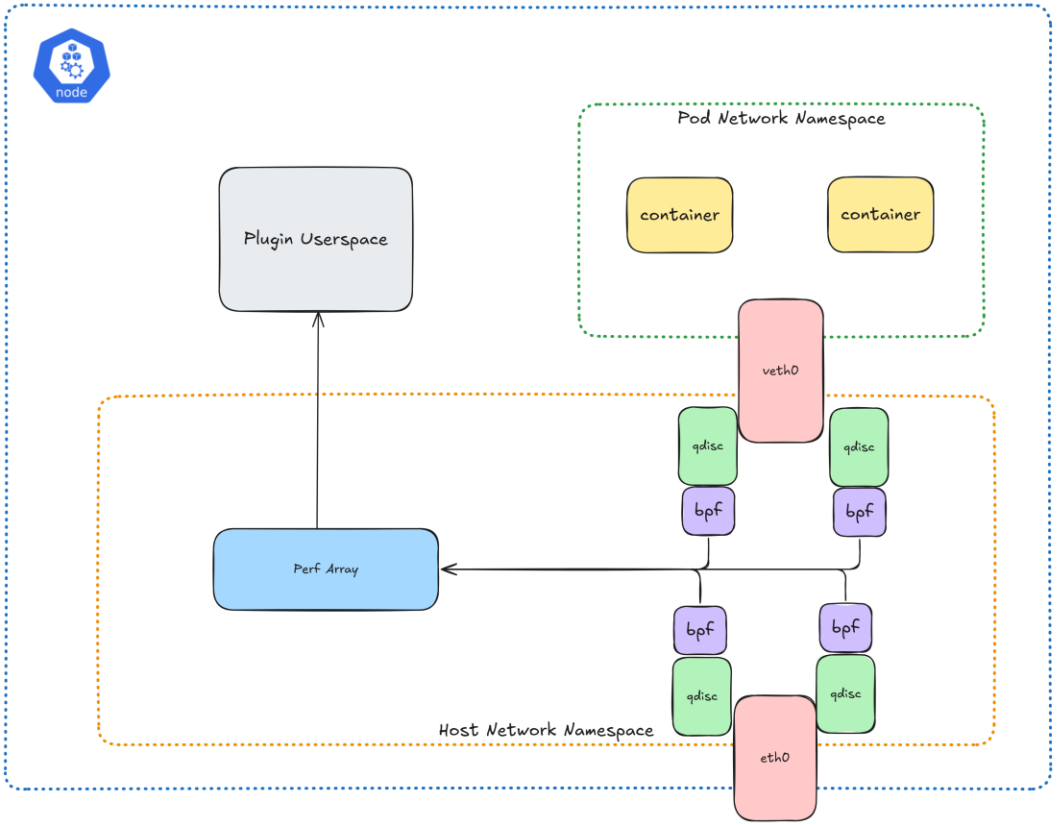


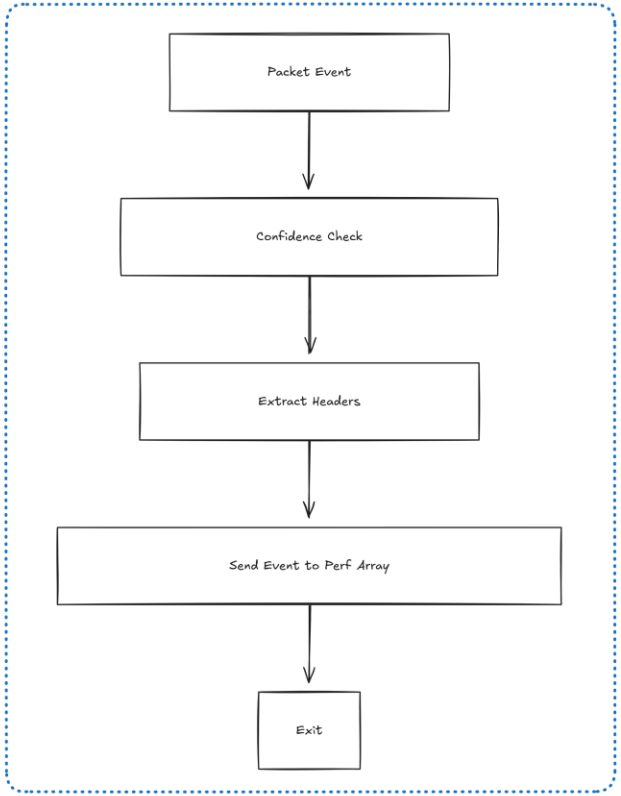
Agent

- Divided into Data plane and Control plane
- Loads eBPF program into kernel
- Reads and converts kernel events into Flow object
- Flows are enriched using cache
- Hubble converts Flows into metrics and logs



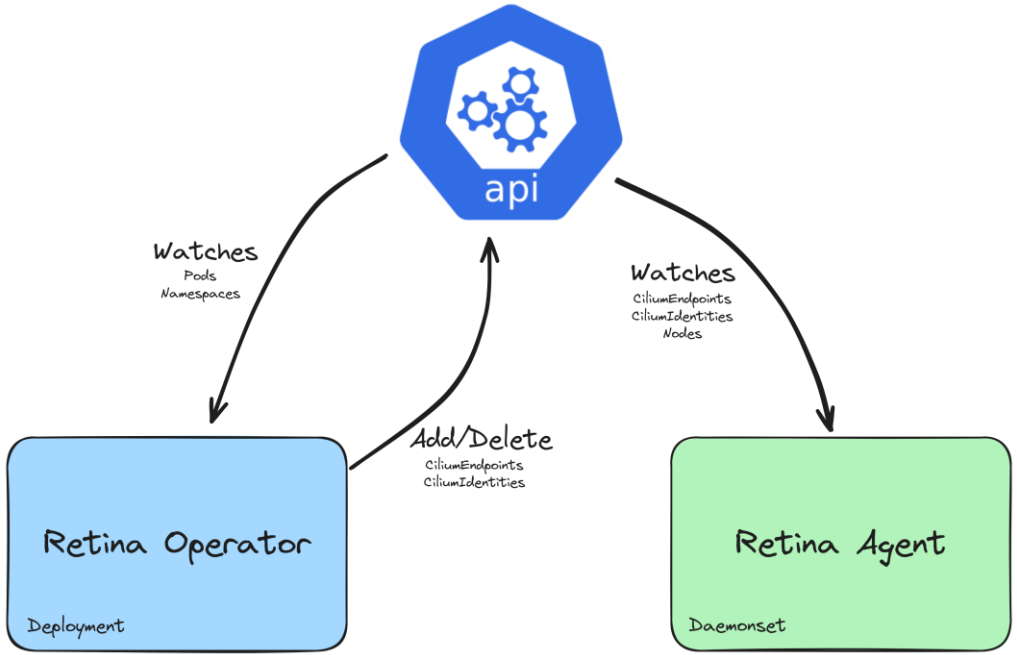
Plugin


node
Pod Network Namespace
container
container
Plugin Userspace
veth0
qdisc
qdisc
bpf
bpf
Perf Array
bpf
bpf
qdisc
qdisc
Host Network Namespace
eth0

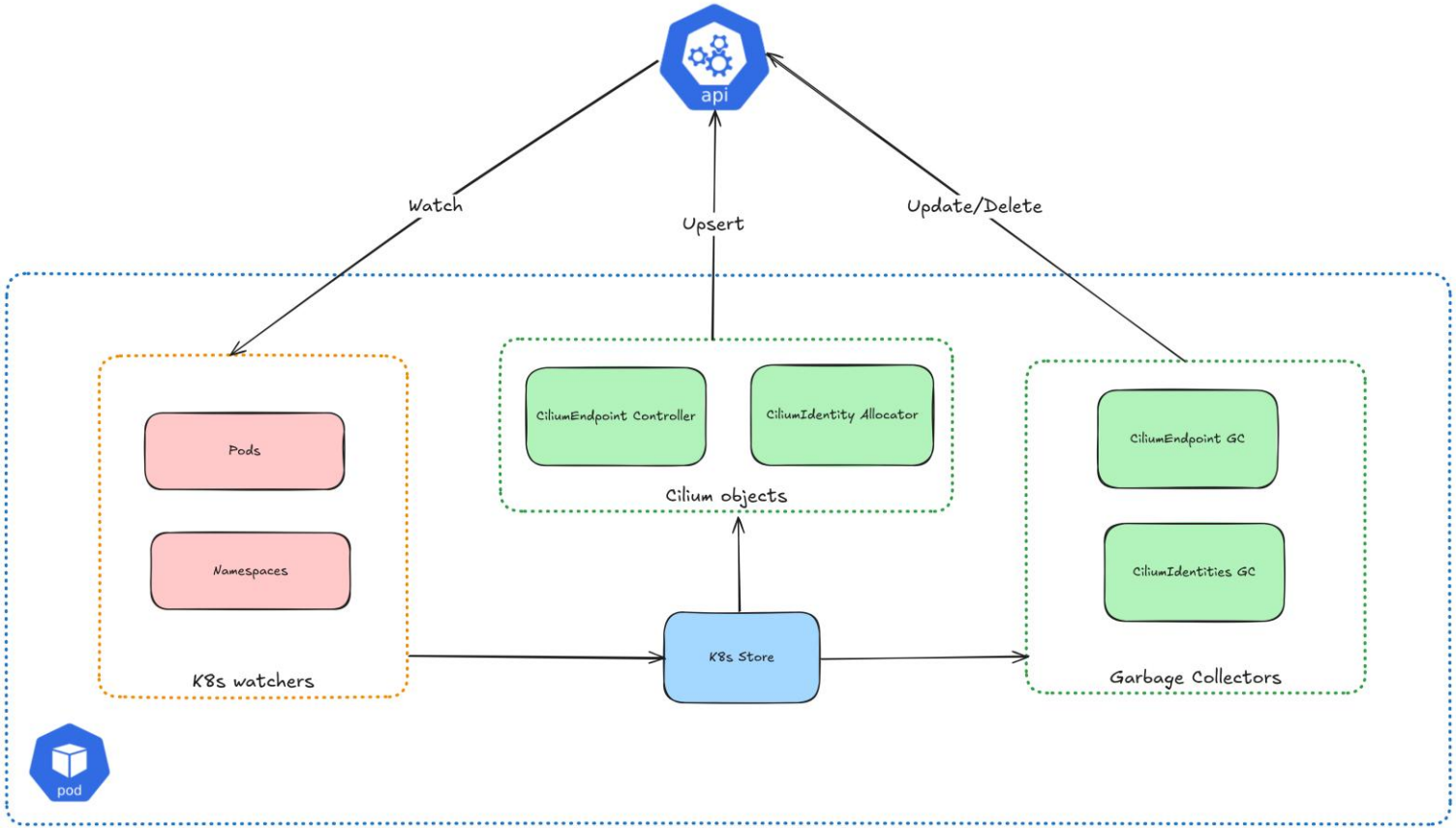

Packet Event
Confidence Check
Extract Headers
Send Event to Perf Array
Exit

Operator Overview

- Operator oversees generating Cilium endpoint and identities
- Watches for Pods and namespaces
- Add/delete/update Cilium endpoints, including labels

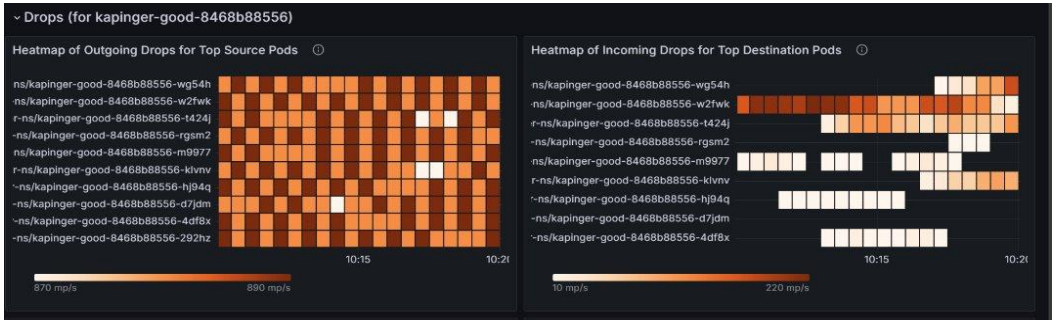


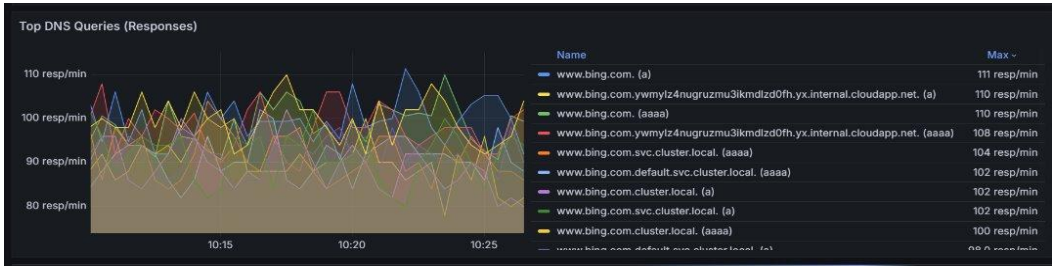
Operator Architecture



Pod Level Metrics

- L4 metrics at various points in Linux kernel
- Drop metrics with reason at Pod level
- L7 (DNS) metrics at Pod level





Network Flow Logs

- Hubble CLI to query for all or filtered network flows across all nodes.
- Single pane of glass for identifying dropped, forwarded and DNS flows.
- Rich support filters

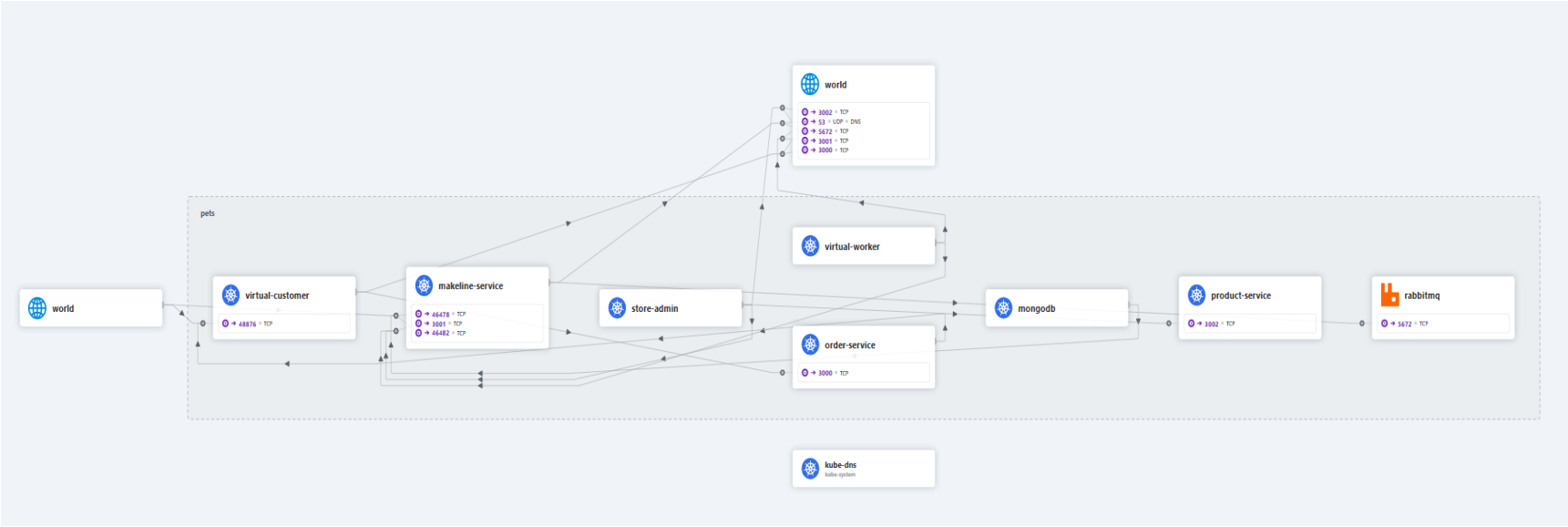
```
~/github/retina main *4 ?1 hubble observe flows --server localhost:4245 -t l7 --last 3
Oct 30 21:20:34.112: default/kapinger-good-5cdd557bb9-vvz5b (ID:52097) <- 10.0.0.10 (world) dns-response  FORWARDED (DNS Answer RCode: Non-Existent Domain (Query WRzrgBFeqq.sh. AAAA))
Oct 30 21:20:34.201: default/kapinger-good-5cdd557bb9-h42wh (ID:52097) <- kube-system/coredns-597bb9d4db-r7fx2 (ID:46373) dns-response  FORWARDED (DNS Answer RCode: Non-Existent Domain
Oct 30 21:20:34.201: default/kapinger-good-5cdd557bb9-h42wh (ID:52097) <- 10.0.0.10 (world) dns-response  FORWARDED (DNS Answer RCode: Non-Existent Domain (Query zsNvuogIty.sh. AAAA))
Oct 30 21:20:34.339: default/kapinger-good-5cdd557bb9-cffxb (ID:52097) <- 10.0.0.10 (world) dns-response  FORWARDED (DNS Answer RCode: Non-Existent Domain (Query bcEpXsSsDT.sh. AAAA))
Oct 30 21:20:34.437: default/kapinger-good-5cdd557bb9-cffxb (ID:52097) <- kube-system/coredns-597bb9d4db-224nh (ID:46373) dns-response  FORWARDED (DNS Answer RCode: Non-Existent Domain
Oct 30 21:20:34.437: default/kapinger-good-5cdd557bb9-cffxb (ID:52097) <- 10.0.0.10 (world) dns-response  FORWARDED (DNS Answer RCode: Non-Existent Domain (Query bcEpXsSsDT.sh. A))
Oct 30 21:20:34.639: default/kapinger-good-5cdd557bb9-jwk7b (ID:52097) <- 10.0.0.10 (world) dns-response  FORWARDED (DNS Answer  (Query kapinger-service.default.svc.cluster.local. AAAA)
Oct 30 21:20:34.639: default/kapinger-good-5cdd557bb9-jwk7b (ID:52097) <- kube-system/coredns-597bb9d4db-r7fx2 (ID:46373) dns-response  FORWARDED (DNS Answer "10.0.48.215" (Query kapinge
Oct 30 21:20:34.639: default/kapinger-good-5cdd557bb9-jwk7b (ID:52097) <- 10.0.0.10 (world) dns-response  FORWARDED (DNS Answer "10.0.48.215" (Query kapinger-service.default.svc.cluster
~/github/retina main *4 ?1
```

```
~/github/retina main *4 ?1 hubble observe flows --server localhost:4245 -t trace --last 3 -n kube-system
Oct 30 21:25:24.052: 10.224.0.4:39638 (host) -> kube-system/azure-policy-56679cc957-mvjkf:9090 (ID:9243) to-endpoint FORWARDED (TCP Flags: ACK:true)
Oct 30 21:25:24.137: 10.224.0.6:40630 (host) -> kube-system/azure-policy-webhook-5df9bd9ff8-ws7nw:9090 (ID:18375) to-endpoint FORWARDED (TCP Flags: ACK:true)
Oct 30 21:25:24.775: kube-system/metrics-server-677fd8c788-tp99c:4443 (ID:28352) <- kube-system/konnectivity-agent-5dc85756b5-84pbc:38812 (ID:18148) to-endpoint FORWARDED (TCP Flags: PSH:true ACK:true)
Oct 30 21:25:24.777: kube-system/metrics-server-677fd8c788-tp99c:4443 (ID:28352) -> kube-system/konnectivity-agent-5dc85756b5-84pbc:38812 (ID:18148) to-stack FORWARDED (TCP Flags: PSH:true ACK:true)
Oct 30 21:25:24.783: kube-system/metrics-server-677fd8c788-l8rl2:4443 (ID:28352) <- kube-system/konnectivity-agent-5dc85756b5-r7p8n:47968 (ID:18148) to-endpoint FORWARDED (TCP Flags: PSH:true ACK:true)
Oct 30 21:25:24.783: kube-system/metrics-server-677fd8c788-l8rl2:4443 (ID:28352) -> kube-system/konnectivity-agent-5dc85756b5-r7p8n:47968 (ID:18148) to-stack FORWARDED (TCP Flags: ACK:true)
Oct 30 21:25:25.449: kube-system/konnectivity-agent-5dc85756b5-84pbc:51176 (ID:18148) -> 10.224.0.5:10250 (host) to-stack FORWARDED (TCP Flags: PSH:true ACK:true)
Oct 30 21:25:25.451: kube-system/hubble-relay-8477c98f44-t7j4v:57592 (ID:53458) -> 10.224.0.6:4244 (remote-node) to-stack FORWARDED (TCP Flags: PSH:true ACK:true)
Oct 30 21:25:25.451: kube-system/hubble-relay-8477c98f44-t7j4v:33350 (ID:53458) -> 10.224.0.4:4244 (remote-node) to-stack FORWARDED (TCP Flags: PSH:true ACK:true)
```

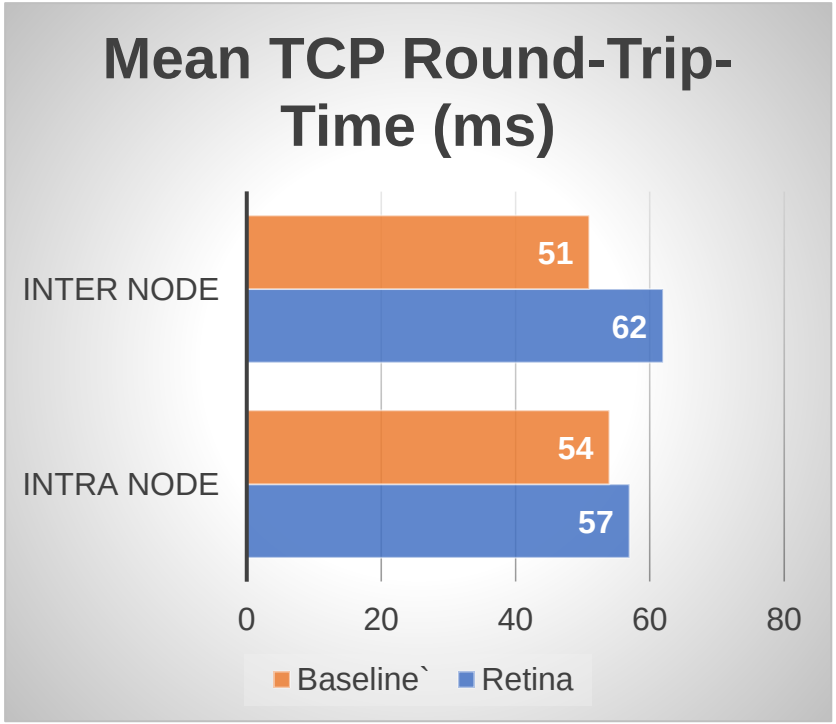
```
~/github/retina main *4 ?1 hubble observe flows --server localhost:4245 -t drop --last 3
Oct 30 21:30:51.762: kapinger-ns/kapinger-good-8468b88556-g6xfs:4810 (ID:25618) <> kapinger-ns/kapinger-bad-7778f55bf8-2h668:36895 (ID:49196) Policy denied DROPPED (Drop Reason: IPTABLE_RULE_DROP
Note: This reason is most accurate. Prefer over others while using Hubble CLI.)
Oct 30 21:30:52.780: kapinger-ns/kapinger-good-8468b88556-g6xfs:4810 (ID:25618) <> kapinger-ns/kapinger-bad-7778f55bf8-2h668:36895 (ID:49196) Policy denied DROPPED (Drop Reason: IPTABLE_RULE_DROP
Note: This reason is most accurate. Prefer over others while using Hubble CLI.)
Oct 30 21:30:54.796: kapinger-ns/kapinger-good-8468b88556-g6xfs:4810 (ID:25618) <> kapinger-ns/kapinger-bad-7778f55bf8-2h668:36895 (ID:49196) Policy denied DROPPED (Drop Reason: IPTABLE_RULE_DROP
Note: This reason is most accurate. Prefer over others while using Hubble CLI.)
```

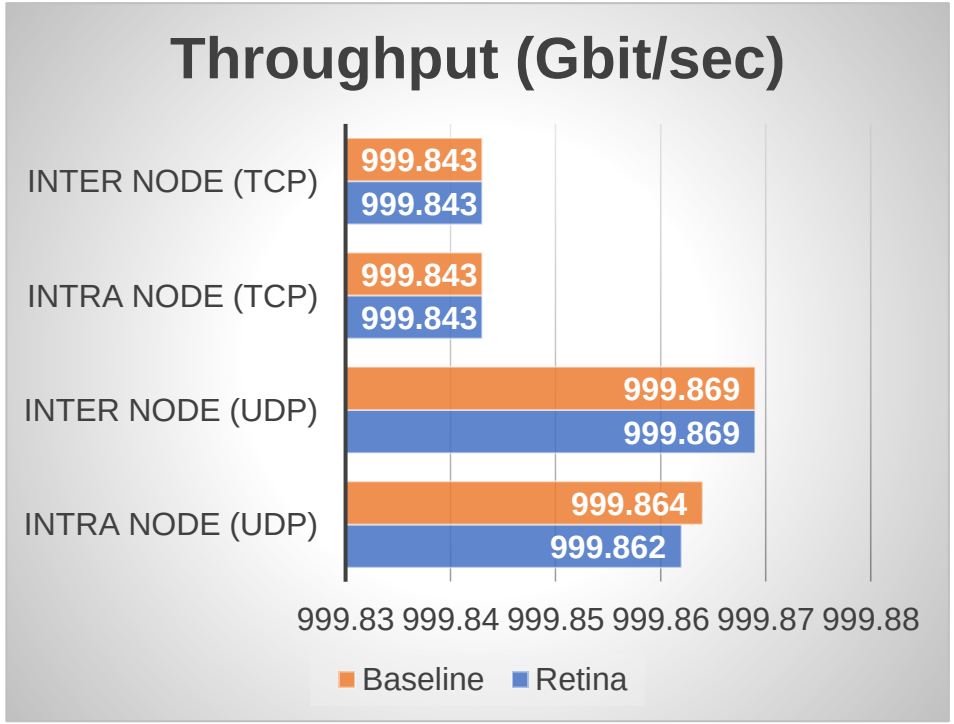
Network Flow Graph

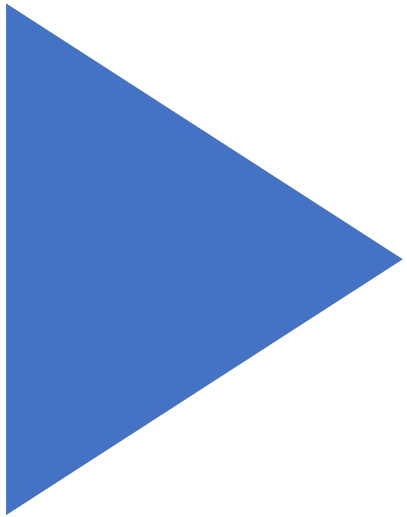
- Hubble UI to visualize filtered network flows across all nodes.
- Single pane of glass for easy visualization of application traffic.



Performance





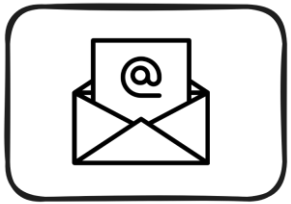


Demo

Future Work

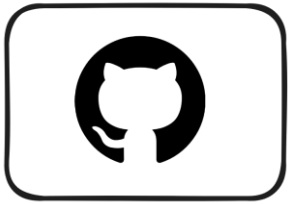
- Run Hubble on Windows node (issue/471)
- Enrich flows with K8s service name (issue/915)
- L7 observability support – HTTP/HTTPS/mTLS (issue/452, issue/85)
- Multi NIC support in a single pod (issue/577)
- AI based network troubleshooting (issue/439)

Contribute



retina@microsoft.com

retina.sh



github.com/microsoft/retina

Thank you!