Improving Kubernetes Security with the Konnectivity Proxy

Joseph Anttila Hall
Senior Software Engineer
Google

Michael McCune
Senior Principal Software Engineer
Red Hat

Hello!

- Joseph Antilla Hall
- Software Engineer @ Google
- GKE (cluster control plane) for 3 years
- jkh52 on GitHub

- Michael McCune
- Software Engineer @ Red Hat
- Cloud Infrastructure and Autoscaling
- Kubernetes ecosystem for 7 years
- elmiko on GitHub

Forecast

- Overview: What is Konnectivity
  - Why, How
- Experience running Konnectivity at GKE scale
  - Why, How
  - Challenges
- Join us! How to get involved with the community.

Overview: What is Konnectivity

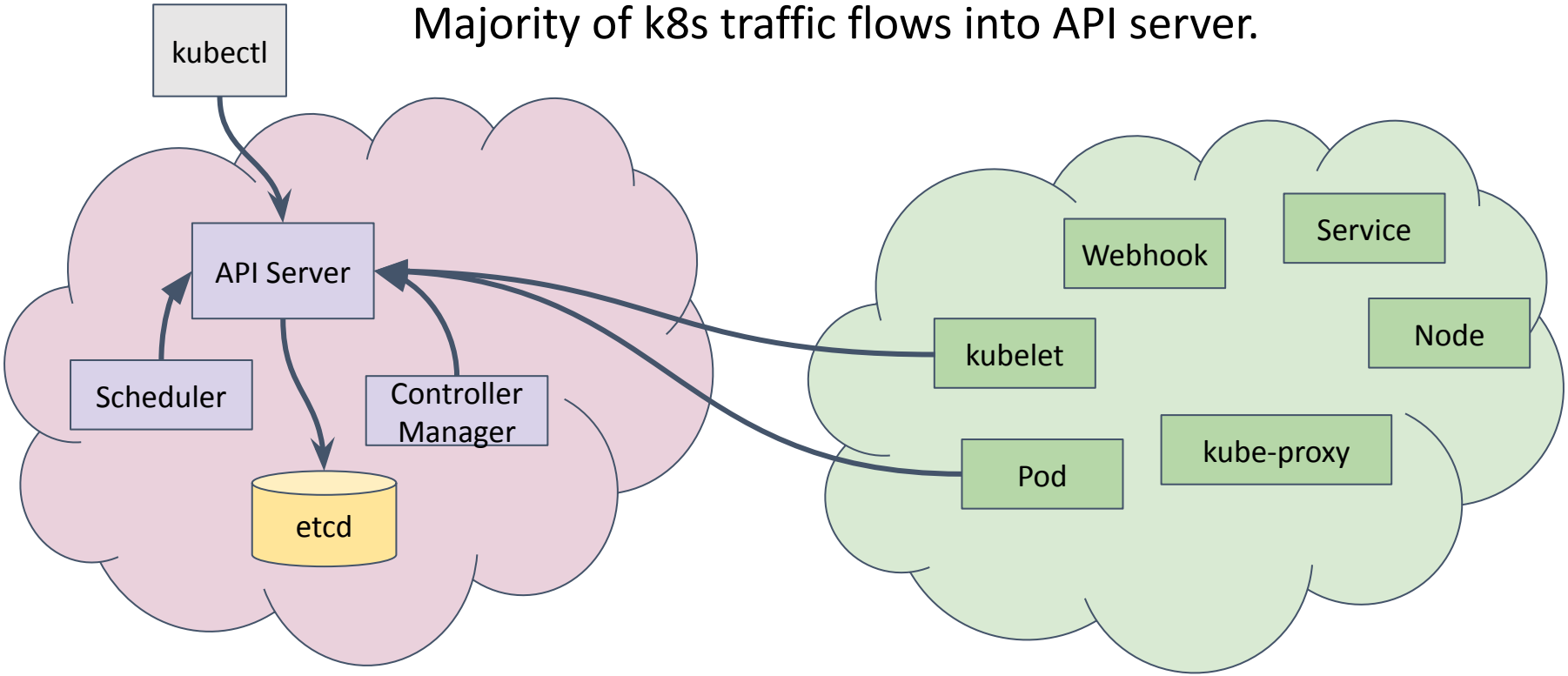
- A TCP level proxy for routing network communications from a K8s API Server to the Cluster Network
- Subproject of SIG API Machinery and SIG Cloud Provider
- Utilizes a server and agent topology
- Not a generalized proxy
- KEP 1281 (Beta)

Previous talks:

- 2019 China: https://www.youtube.com/watch?v=y0DBopR17-s
- 2022 Detroit: https://www.youtube.com/watch?v=0yltsB3Cbr4

Overview: Why?

Majority of k8s traffic flows into API server.



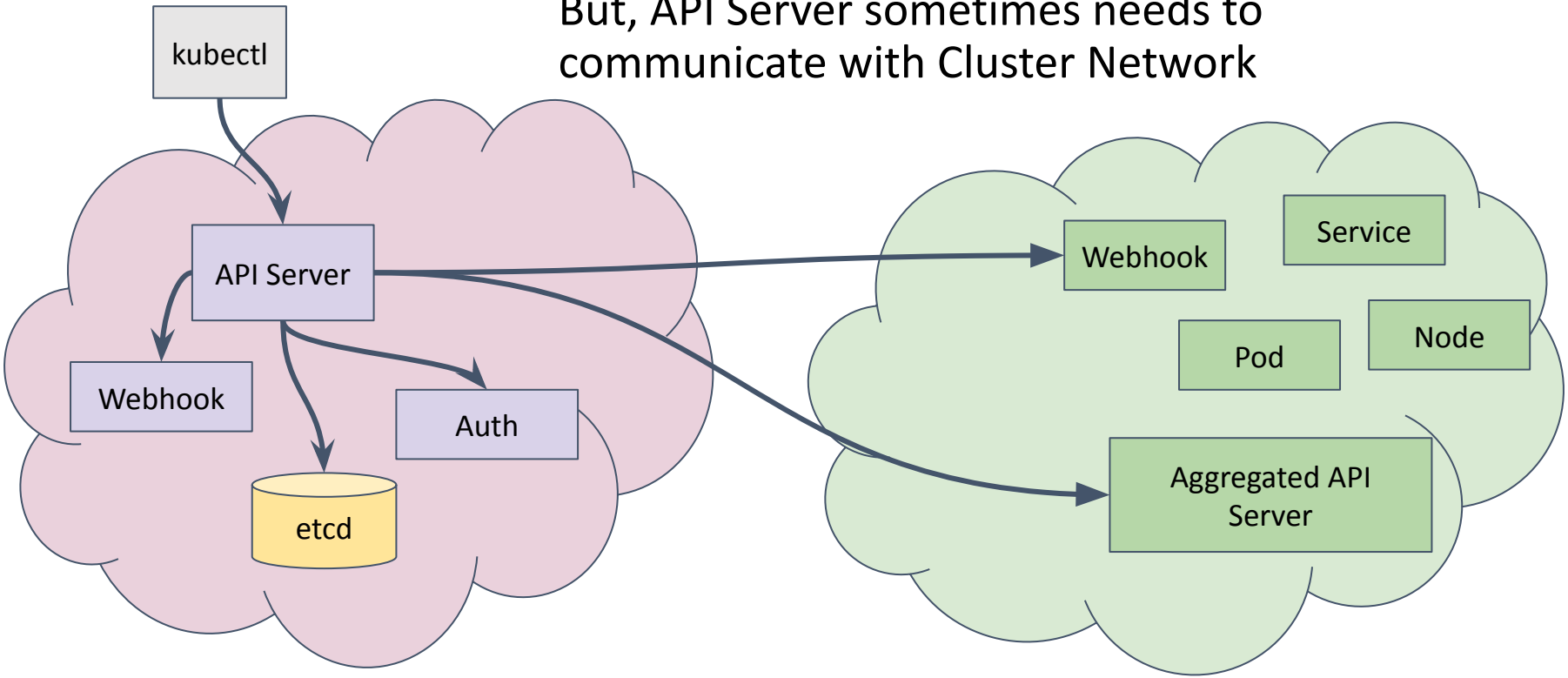
https://kubernetes.io/docs/concepts/architecture/control-plane-node-communication/#node-to-control-plane

Overview: Why?

But, API Server needs to communicate to Cluster Network

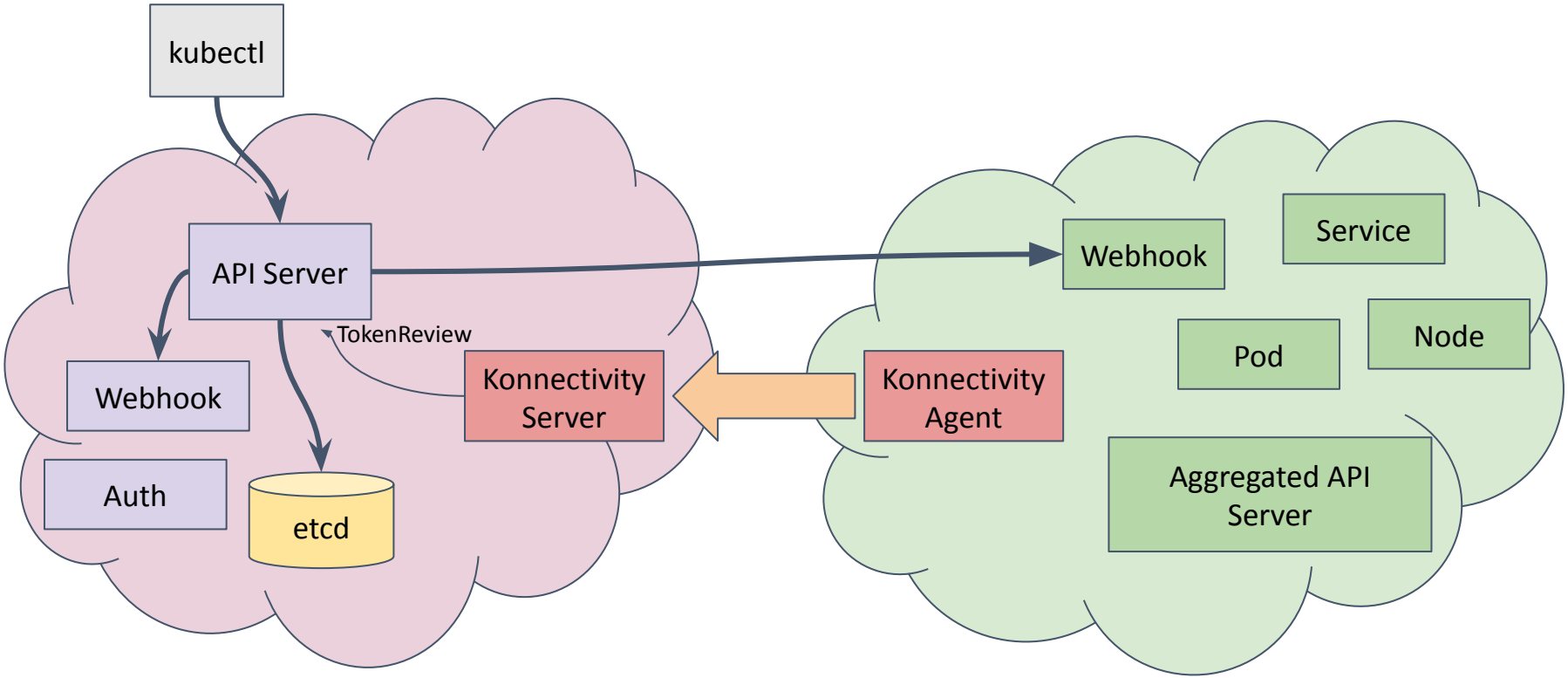
- Webhooks
- Aggregated API Servers
- Pod (logs, attach, etc)
- Services (proxy)

Overview: How?

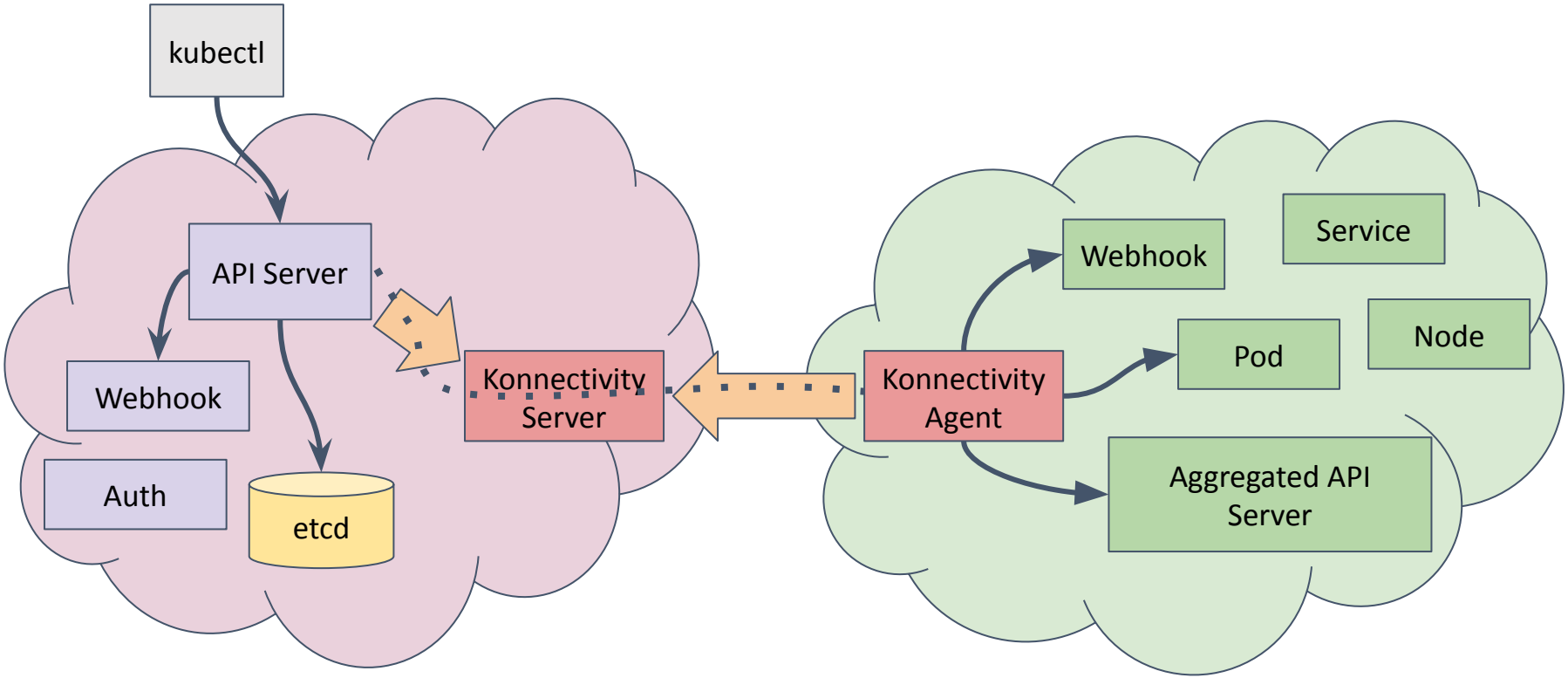


https://kubernetes.io/docs/concepts/architecture/control-plane-node-communication/#control-plane-to-node

Overview: How?



Overview: How?



API Server with EgressSelectorConfiguration of type "cluster" (also possible: controlplane, etcd).

Overview: How?

- Try it out!
  https://kubernetes.io/docs/tasks/extend-kubernetes/setup-konnectivity/

How does it help improve security?

Inspired by this email, as cited by KEP 1281

[ANNOUNCE] Security Impact of Kubernetes API server external IP address proxying

1224 views

Jessie Frazelle Jan 4, 2019, 2:00:22 PM

to kubernetes-sec...@googlegroups.com

Hello Kubernauts,

full email link

Running on GKE: Why?

Pre-2021

- Relied on SSH tunnels (deprecated)
- Needed a replacement before removed (v1.22)

2022+

- Unify around Private Service Connect based clusters

Running on GKE: How?

- Deployment, not daemonset
  - Efficient use of resources
  - Scalability
- Phased migration
  - Install Konnectivity Server and Agent
  - Configure API Server only after observing Ready

Running on GKE: Challenges

2021

- Users can break it (firewall rules, Node taints, etc)

2022

- Encountered rare but impactful issues
- Theme: can act as a domino
  - Controller busy-loop -> Konnectivity overloaded -> CP Egress degraded
  - Bad webhook -> Konnectivity deadlocked -> CP Egress unavailable
- Difficult and expensive to debug
  - streaming TCP packets across 3+ binaries
  - binary version skew

Running on GKE: Recently

2022

Re-stabilization effort

- Several new metrics, including API server (client lib)
- Test improvements
- Eliminate (last?) race / resource leak bugs

2023

- Has been stable
- second wave of migrations (for Private Service Connect based clusters)

Join Us!

KubeCon CloudNativeCon North America 2023

- Active discussions around path to GA.
- Help us make the user experience better!
- Come to a project meeting, on alternating Wednesdays @ 16:00 UTC
  - Agenda document link
- Investigate the source code here: https://github.com/kubernetes-sigs/apiserver-network-proxy/

Stay in touch

Joseph Anttila Hall
jkh@google.com

Michael McCune
@elmiko@fosstodon.org