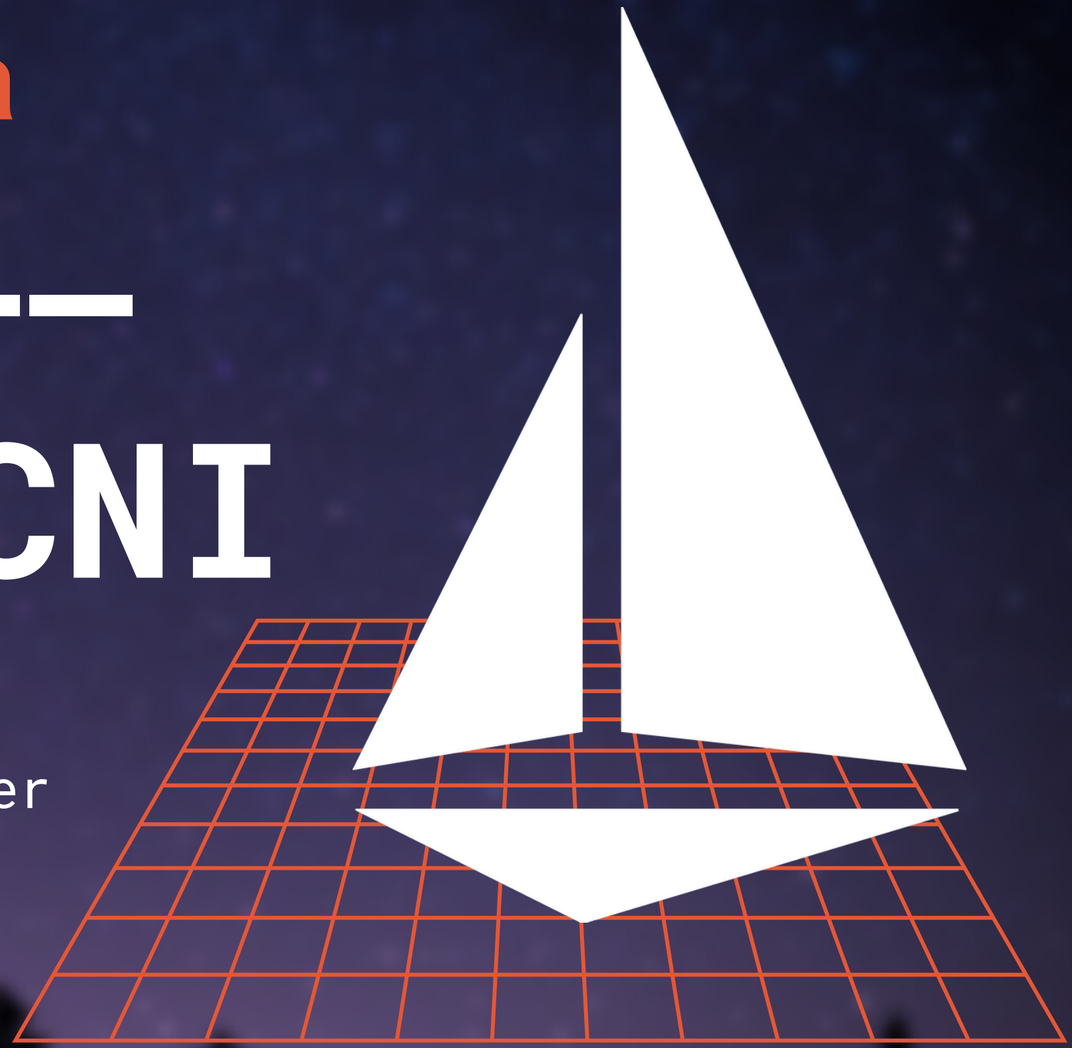
Istio Meetup China

服务网格安全——理解 Istio CNI



张之晗
Tetrate 工程师/Istio 社区 Release Manager

About me

Istio 1.10 Release Manager, Istio Community, 2021-Present

GetMesh(GetIstio) core contributor, Istio Community, 2021-Present

Tetrate Service Bridge developer, Tetrate.io, 2021-Present

Istio Developer(Security SIG), Istio Community, 2020-Present

Anthos Service Mesh, Google Inc, 2020

tetrate

Leading Cloud Native

Varun Talwar
Co-founder/CEO
Co-creator gRPC, Istio

Jeyappragash (JJ)
Co-founder
Chair CNCF SIG Security

Zack Butcher
Istio Steering Committee

Lizan Zhou
Envoy Senior Maintainer

Sheng Wu
Creator, SkyWalking

tetrate

Istio

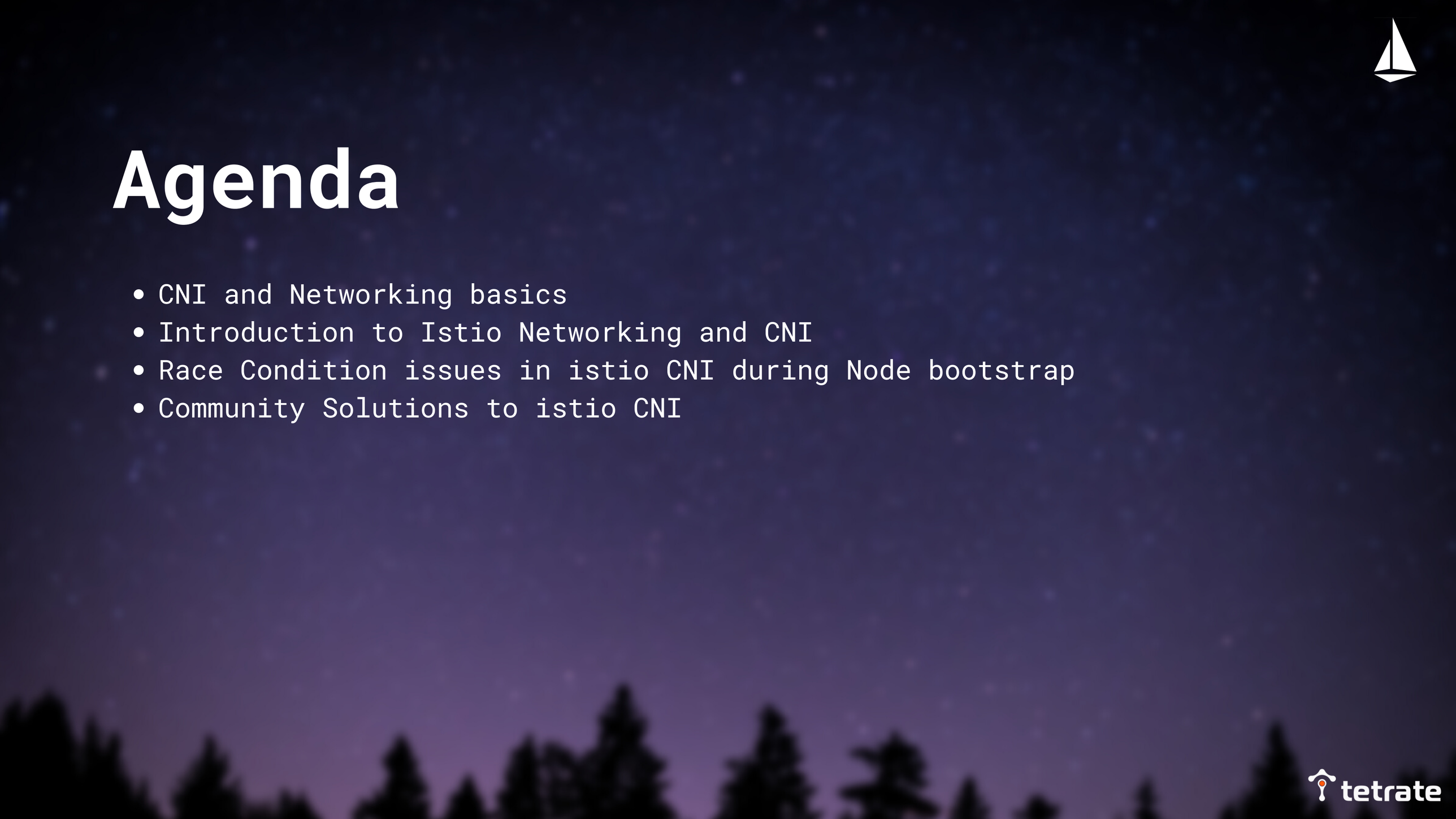
Istio is the industry-standard service mesh control plane that makes it easier to connect, observe, and secure microservices.

envoy

Envoy is an edge and service proxy that allows traffic in an infrastructure to flow in a mesh, allowing you to visualize problem areas, tune performance, and add substrate features.

Skywalking

SkyWalking is an observability power tool that provides distributed tracing, service mesh telemetry analysis, metric aggregation and visualization for cloud-native workloads in a single platform.



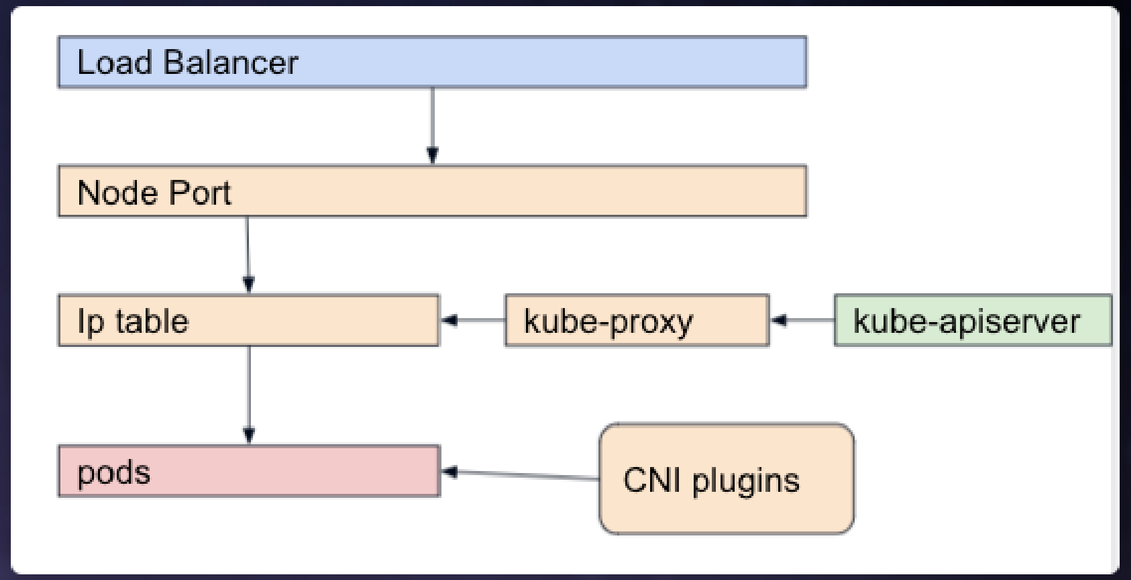
Agenda

- CNI and Networking basics
- Introduction to Istio Networking and CNI
- Race Condition issues in istio CNI during Node bootstrap
- Community Solutions to istio CNI

tetrate

CNI Basics

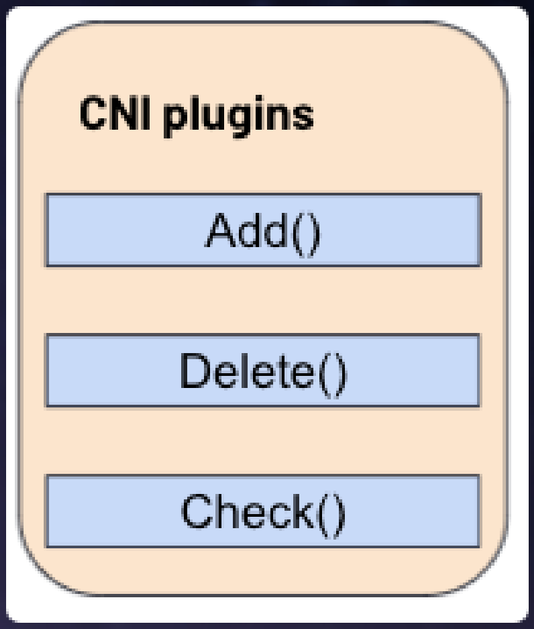
- Kube Proxy: exists in each node and manage iptable
- IPTables: Responsible for translating service IP addresses (which are static) into Pod IP addresses
- CNI plugins: allocate ip addresses for workloads exist in nodes



tetrate

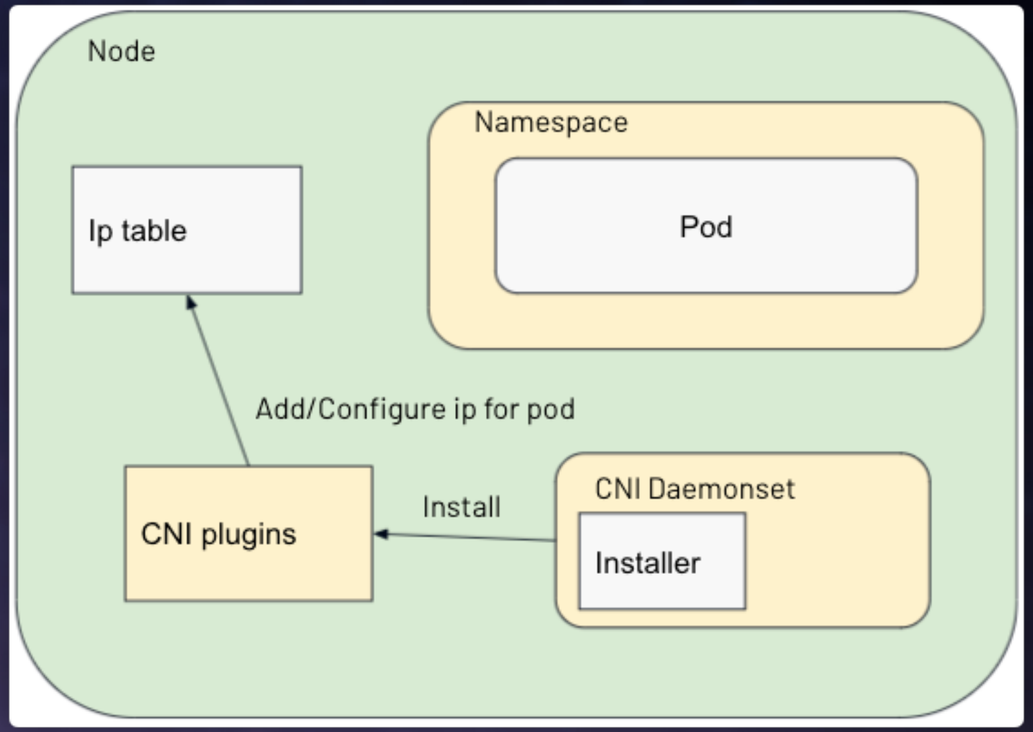
CNI interface

- Calico
- Antrea
- Flannel
- Istio CNI



CNI Daemonset

- Calico
- Antrea
- Flannel
- Istio CNI



Networking lifecycle (Istio Init)

- Start istio init container in workload
- Istiod watch updates & start networking sidecar proxy
- init container update iptable rule for proxy
- terminate init container
- Start workload with updated ip routing rules

Networking lifecycle (Istio CNI)

- Kubelet Start a pausing pod
- Kubelet invoke CNI plugins
- CNI plugins setup ip for pod
- Istio CNI install isidecar network routing rule to workload iptable

Benefits of Istio CNI

- No need for CAP_NET_ADMIN and CAP_NET_RAW permission
- No need for istio-init container means faster startup speed (need validation instead)

tetrate

Issue in Istio CNI

- Kubelet Start a pausing pod
- Kubelet invoke CNI plugins
- CNI plugins setup ip for pod
- Pod could get started in here and bypassing istio sidecar proxy(race condition)
- Istio CNI install sidecar network routing rule to workload iptable

Issue in Istio CNI

- Kubelet Start a pausing pod
- Kubelet invoke CNI plugins
- CNI plugins setup ip for pod
- Pod could get started in here and bypassing istio sidecar proxy(race condition)
- Istio CNI install sidecar network routing rule to workload iptable

Issue in Istio CNI

- Could happen in suddenly increased nodes and premptable nodes
- Bypassing all iptable rules set by data plane proxies

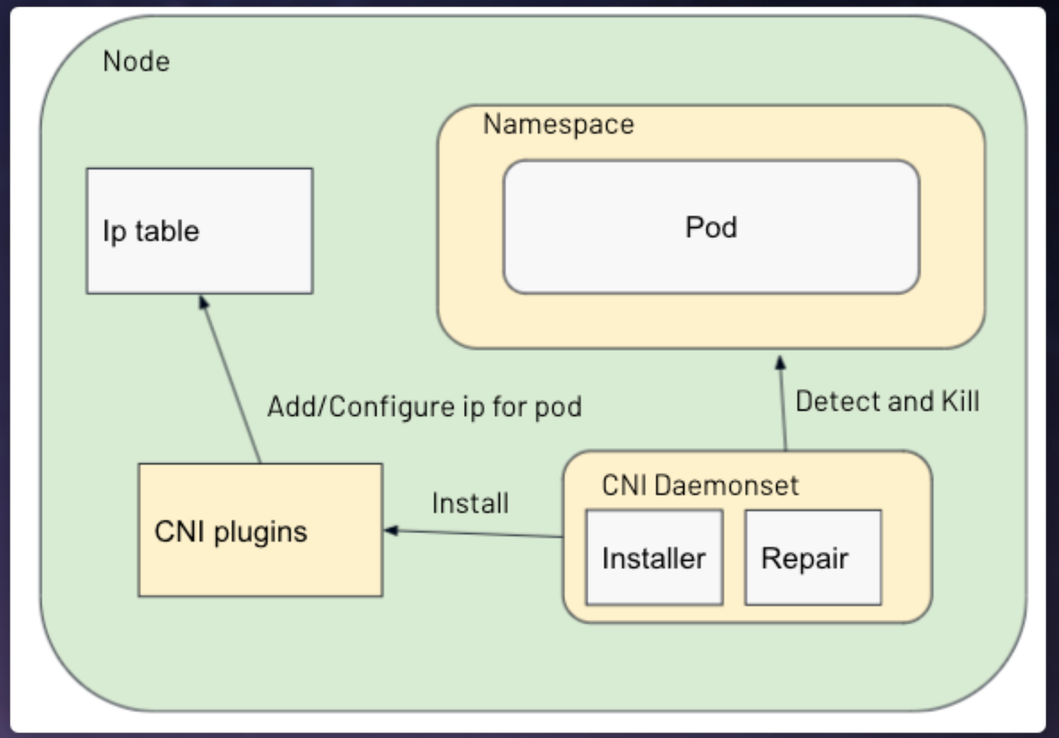
Troubleshooting Istio CNI

- Check the istio proxy container through nsenter
- Check CNI logs in kubelet (journalctl)
- Will do:
  - grafana board
  - istio CNI logging on daemonset
  - istioctl scanning tool designed for CNI

tetrate

Repair controller

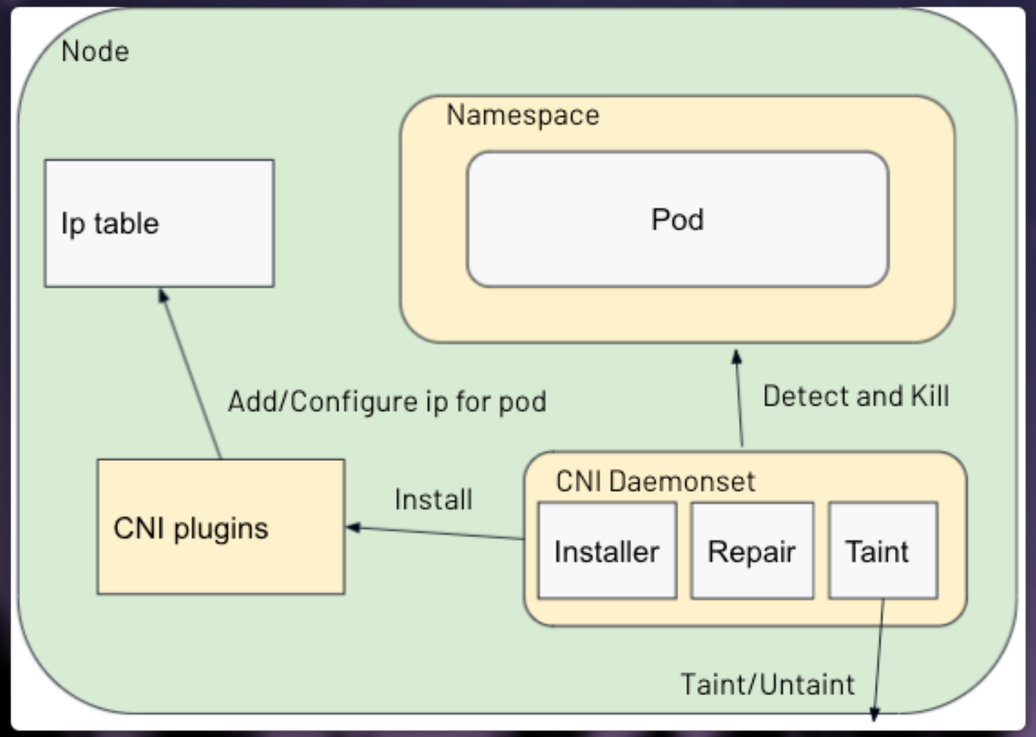
- Valid through istio-init (iptable)
- Detect crashloop init container
- Kill and Restart them



tetrate

Taint controller

- No need for istio init container (faster startup speed)
- Taint Node when istio CNI did not get installed, and unTaint node when they are ready
- Inspired by kubernetes planned extension (Node Readiness Gate)



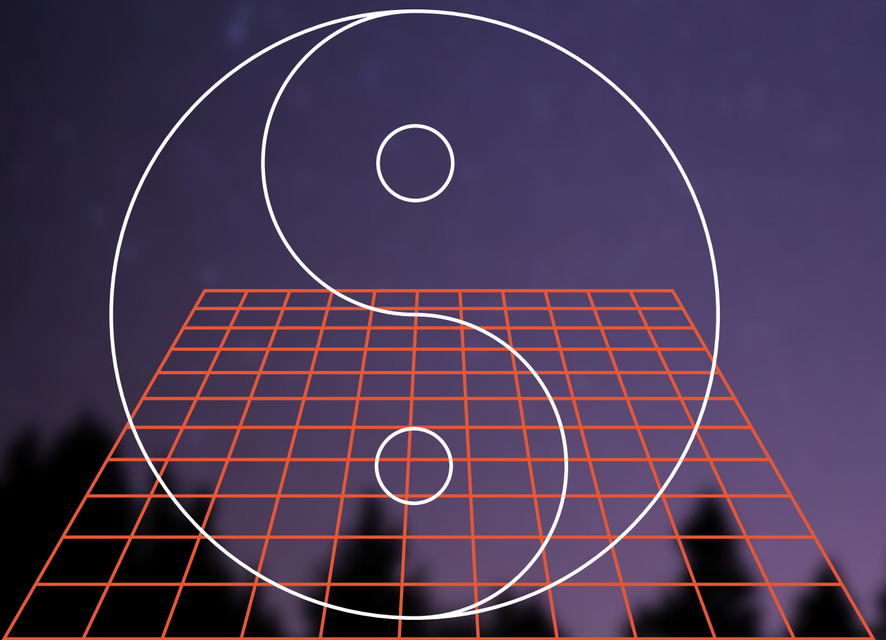
tetrate

Useful links

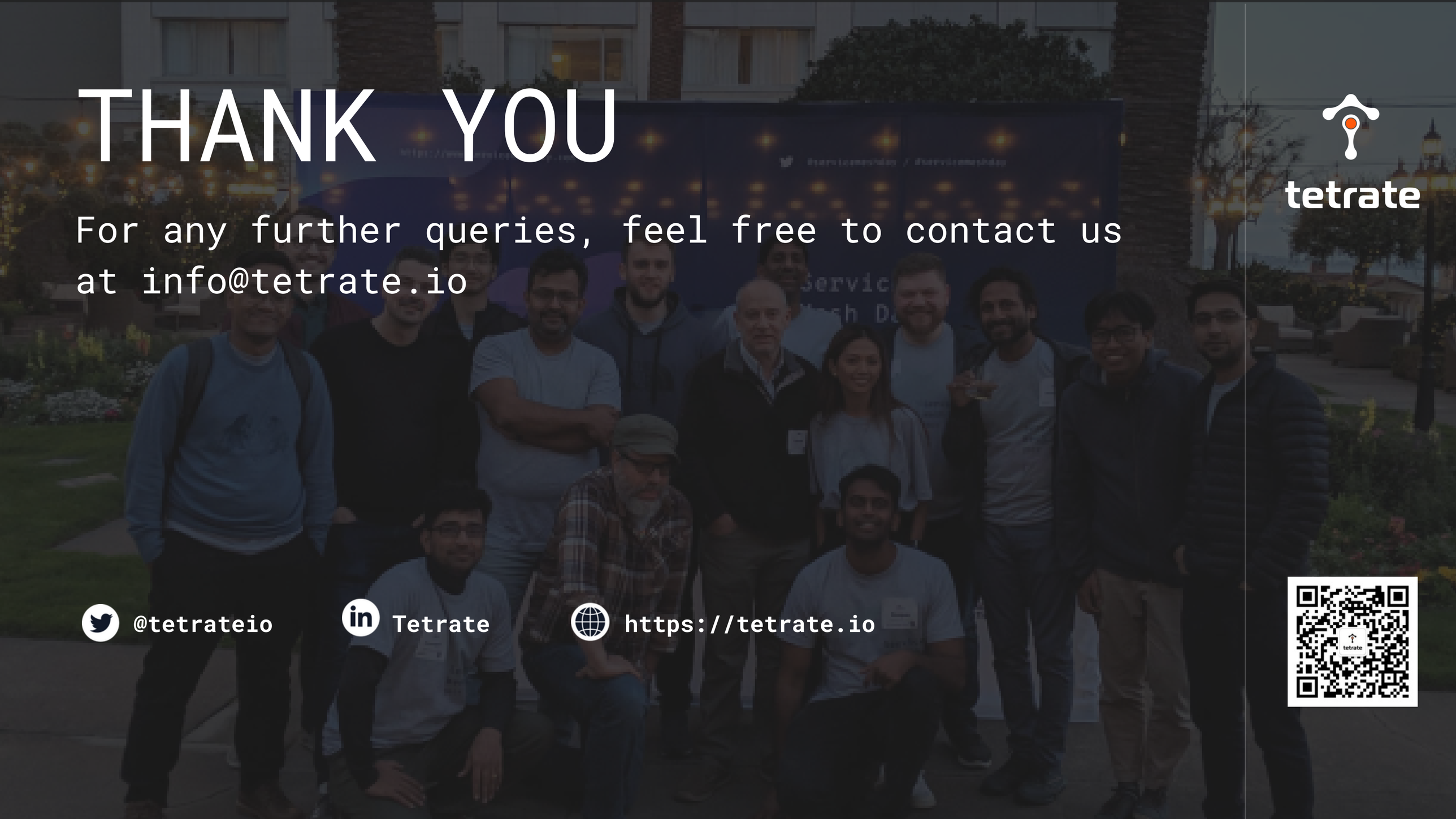
- CNI beta RFC
- Istio CNI Race Condition Mitigation
- CNI beta Graduation
- Kubernets Node Readiness Gates

tetrate

Q&A



tetrate



THANK YOU

For any further queries, feel free to contact us at info@tetrate.io

tetrate

@tetrateio

Tetrate

https://tetrate.io