KUBERNETES COMMUNITY DAYS BEIJING 2025

从一个安全漏洞聊起

深入探究Kubernetes的网络和应用安全

张晋涛 @ Kong Inc

个人介绍

- 张晋涛
- Kong Inc.
- CNCF Ambassador, KCD Organizer
- Kubernetes ingress-nginx maintainer
- LFAPAC Open Source Evangelist
- 公众号：MoeLove
- GitHub: tao12345666333

Content

目录

Part 01

探究 CVE-2024-7646

CVE-2024-7646 高危漏洞

KCD GROWING CLOUD NATIVE TOGETHER BEIJING

CVE-2024-7646 Detail

AWAITING ANALYSIS

This CVE record has been marked for NVD enrichment efforts.

Description

A security issue was discovered in ingress-nginx where an actor with permission to create Ingress objects (in the `networking.k8s.io` or `extensions` API group) can bypass annotation validation to inject arbitrary commands and obtain the credentials of the ingress-nginx controller. In the default configuration, that credential has access to all secrets in the cluster.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

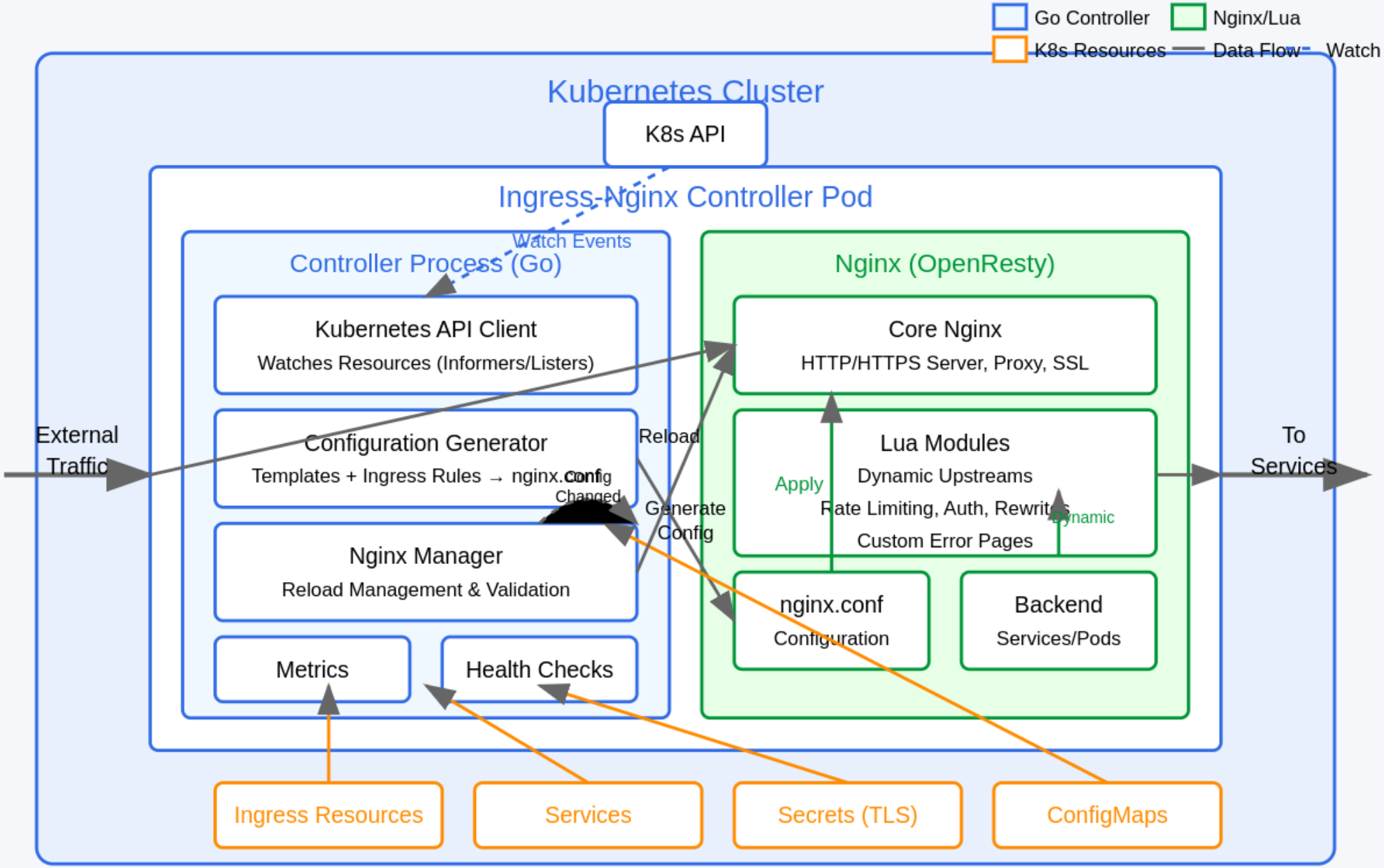
NVD	**NIST:** NVD	**Base Score:** N/A	NVD assessment not yet provided.
C	**CNA:** Kubernetes	**Base Score:** 8.8 HIGH	**Vector:** CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:
CVE-2024-7646
NVD Published Date:
08/16/2024
NVD Last Modified:
11/21/2024
Source:
Kubernetes

CVE-2024-7646 影响范围和攻击面

- ingress-nginx controller < v1.11.2
- ingress-nginx controller < v1.10.4
- 如果通过此漏洞越过 ingress-nginx annotation validation 的话，则可能注入漏洞代码，或者获取到 ingress-nginx controller 所在 Pod 的权限，并通过它访问到集群中的 secrets 资源。
- 核心攻击示例：content_by_l¥rua_block -> content_by_lua_block


Go Controller
Nginx/Lua
K8s Resources
Data Flow
Watch
Kubernetes Cluster
K8s API
Ingress-Nginx Controller Pod
Watch Events
Controller Process (Go)
Kubernetes API Client
Watches Resources (Informers/Listers)
Configuration Generator
Templates + Ingress Rules → nginx.conf
Nginx Manager
Reload Management & Validation
Metrics
Health Checks
Nginx (OpenResty)
Core Nginx
HTTP/HTTPS Server, Proxy, SSL
Lua Modules
Dynamic Upstreams
Rate Limiting, Auth, Rewrites
Custom Error Pages
nginx.conf
Configuration
Backend
Services/Pods
External Traffic
Reload
Config Changed
Generate Config
Apply
Dynamic
To Services
Ingress Resources
Services
Secrets (TLS)
ConfigMaps

CVE-2024-7646 的修复

chore: make the auth verify regex more strict #11717

Edit | Code

Merged | k8s-ci-robot merged 1 commit into `kubernetes:main` from `tao12345666333:make-auth-regex-more-strict` on Aug 2, 2024

Conversation 11 | Commits 1 | Checks 44 | Files changed 1 | +1 -1

tao12345666333 commented on Aug 2, 2024 — Member

What this PR does / why we need it:

Reviewers
- Gacko
- strongjz

Perform some cleaning operations on line breaks. #11720

Edit | Code

Merged | k8s-ci-robot merged 1 commit into `kubernetes:main` from `tao12345666333:deal-with-line-break` on Aug 2, 2024

Conversation 9 | Commits 1 | Checks 44 | Files changed 1 | +14 -0

tao12345666333 commented on Aug 2, 2024 — Member

What this PR does / why we need it:

Process the line breaks so that the generated configuration is more intuitive.

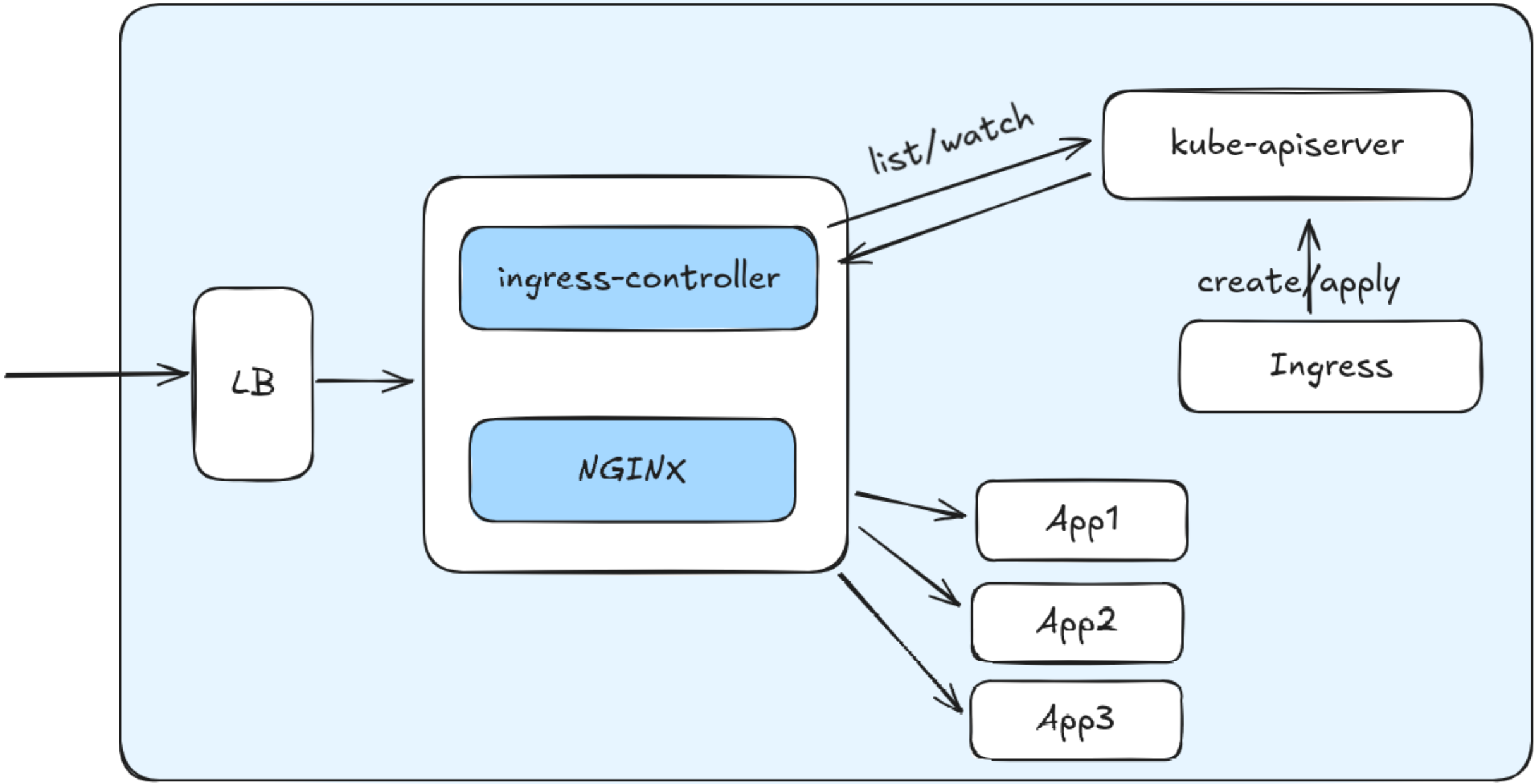
Types of changes

Reviewers
- Gacko ✓
- strongjz

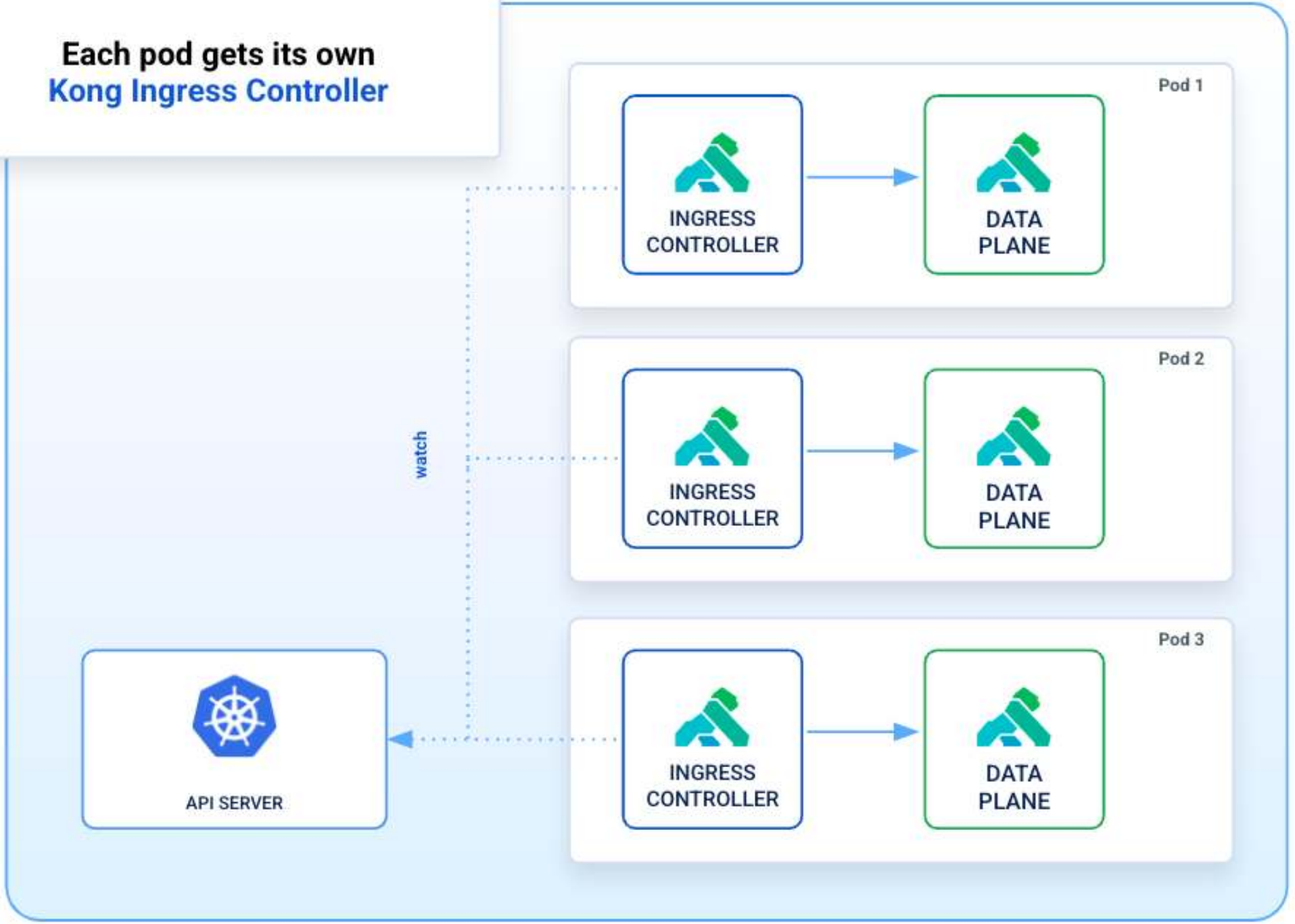
Assignees
- Gacko

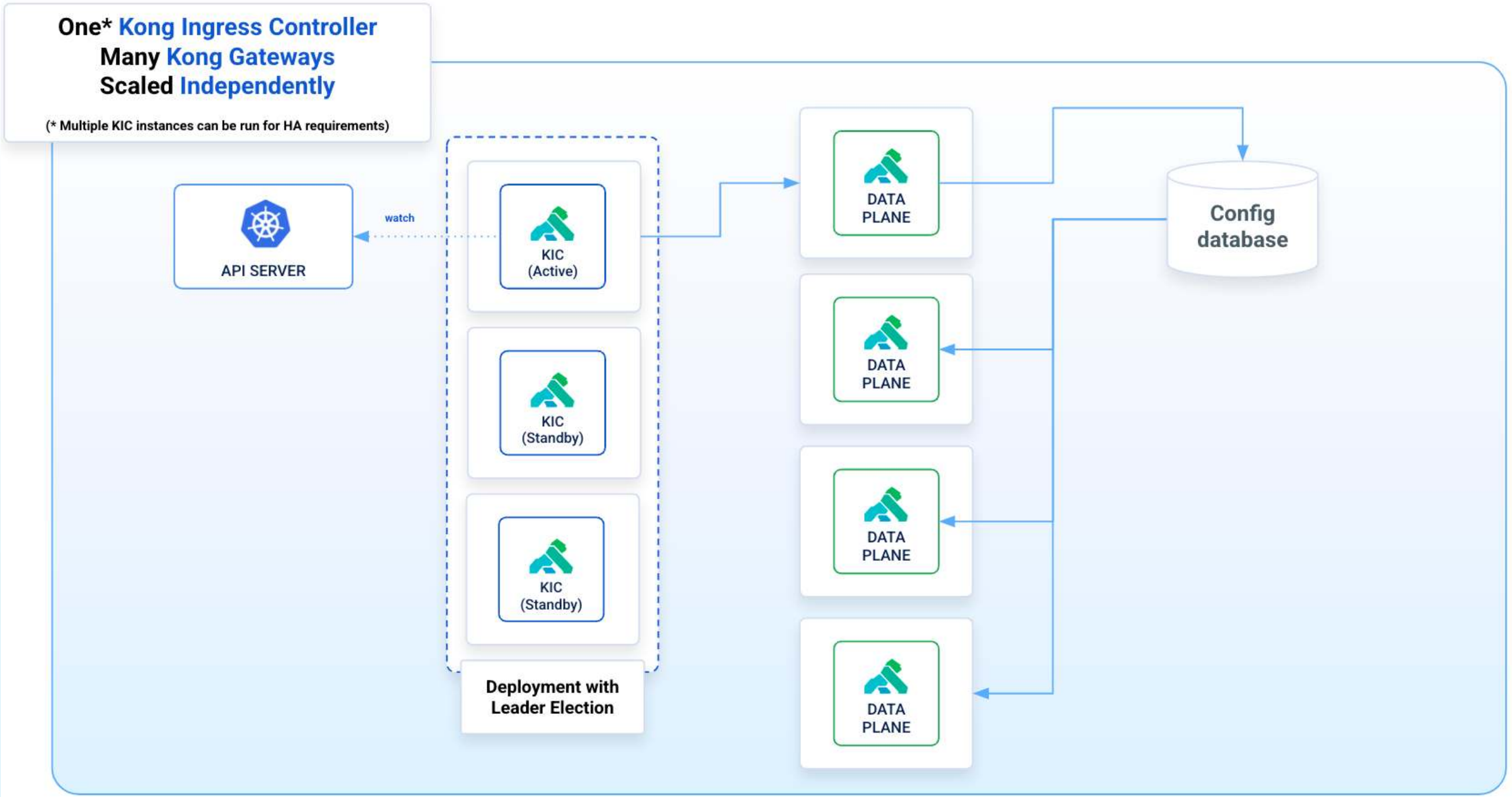
Part 02

Kubernetes中的网络


list/watch
kube-apiserver
ingress-controller
create/apply
Ingress
LB
NGINX
App1
App2
App3

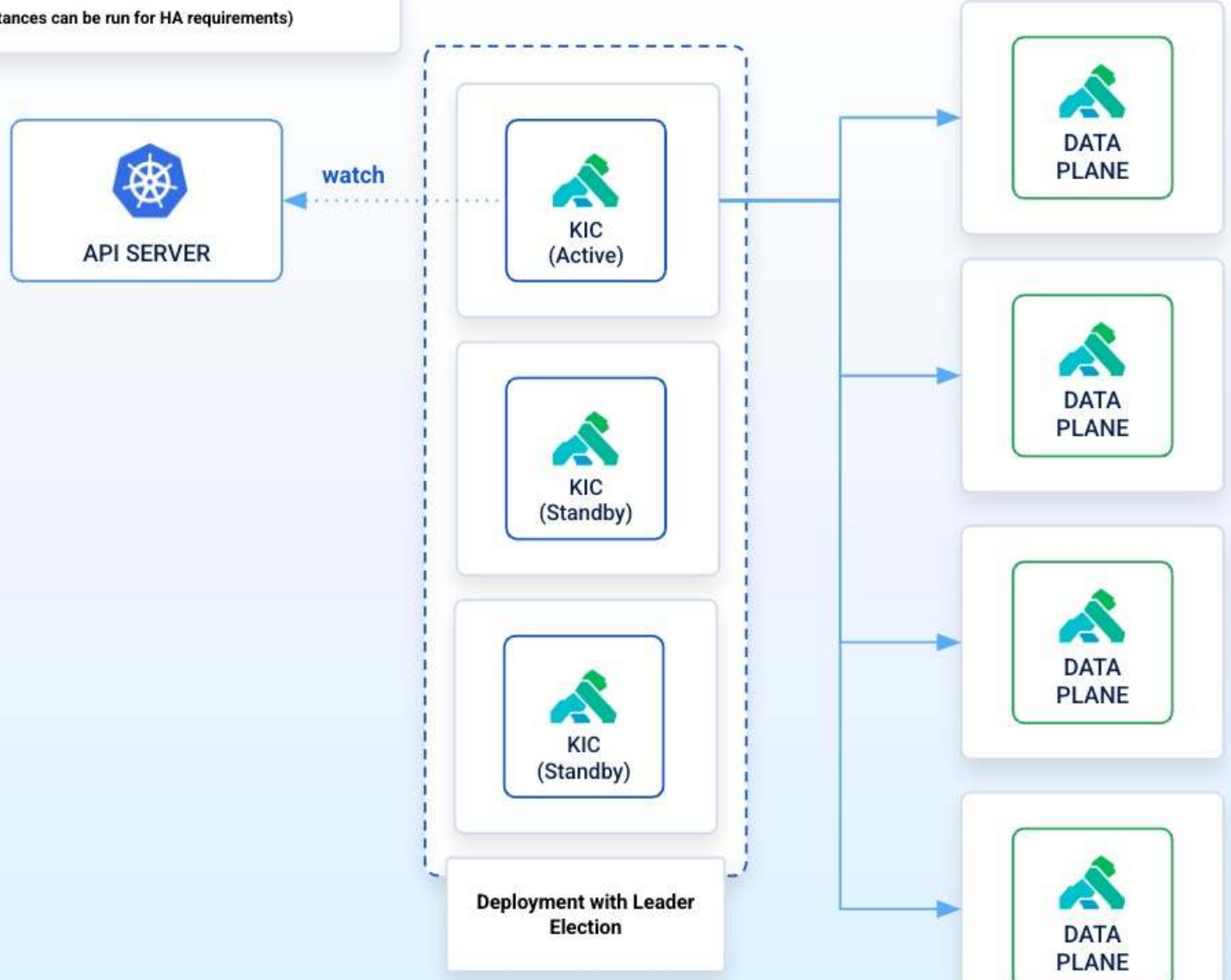
Each pod gets its own Kong Ingress Controller




One* Kong Ingress Controller
Many Kong Gateways
Scaled Independently
(* Multiple KIC instances can be run for HA requirements)
API SERVER
watch
KIC
(Active)
KIC
(Standby)
KIC
(Standby)
Deployment with
Leader Election
DATA
PLANE
DATA
PLANE
DATA
PLANE
DATA
PLANE
Config
database

One* Kong Ingress Controller
Many Kong Gateways
Scaled Independently

(* Multiple KIC instances can be run for HA requirements)



Part 03

Kubernetes中的应用安全

Pod安全

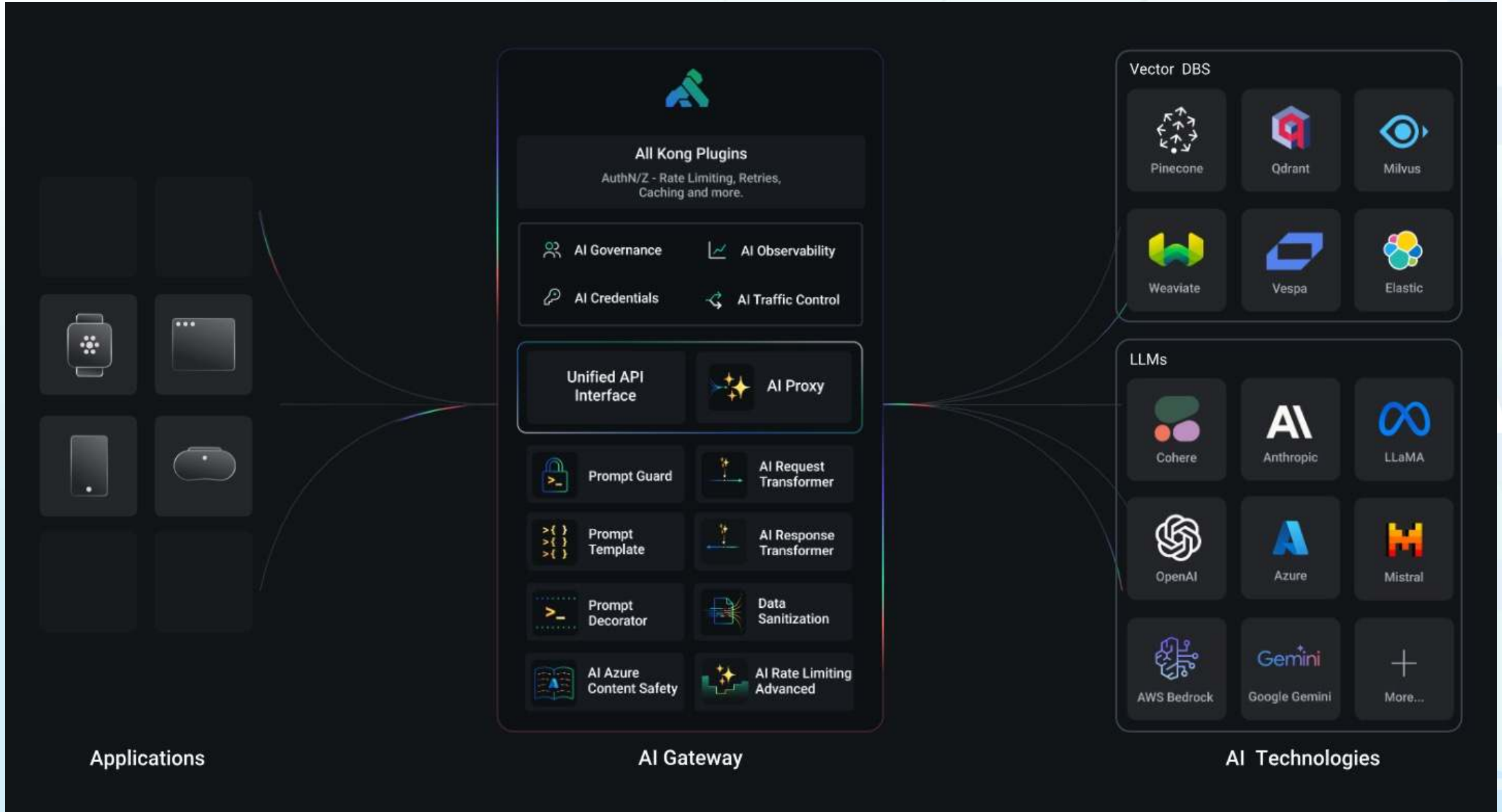
- 最小化权限
- 减少攻击面
- 供应链安全

网络安全

- API Gateway & 正确的配置
- HTTPS
- 。。。

- AI 时代：AI Gateway

AI 时代：Kong AI Gateway



Part 04
总结

复杂性不可避免，但有解决之道

- Kubernetes 是复杂的
- Kubernetes 的网络是复杂的
- Kubernetes 中的应用安全是复杂的

Thanks.