

# GOTC

## 全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

# OPEN SOURCE , OPEN WORLD #

**「开源云原生计算时代论坛」专场**

本期议题：生产环境下的 K8K 安全困境及应对措施

张晋涛 2021年07月10日

# 个人介绍

GOTC

- 张晋涛@支流科技
- Apache APISIX committer
- Kubernetes ingress-nginx reviewer
- containerd/Docker/Helm/Kubernetes/KIND contributor
- K8S 生态周报的维护者
- <https://github.com/tao12345666333>
- email: zhangjintao@apache.org



全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

# Agenda

GOTC

- 容器技术的利与弊
- K8S环境下的安全挑战
- K8S环境下安全问题的应对方式
- 总结

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

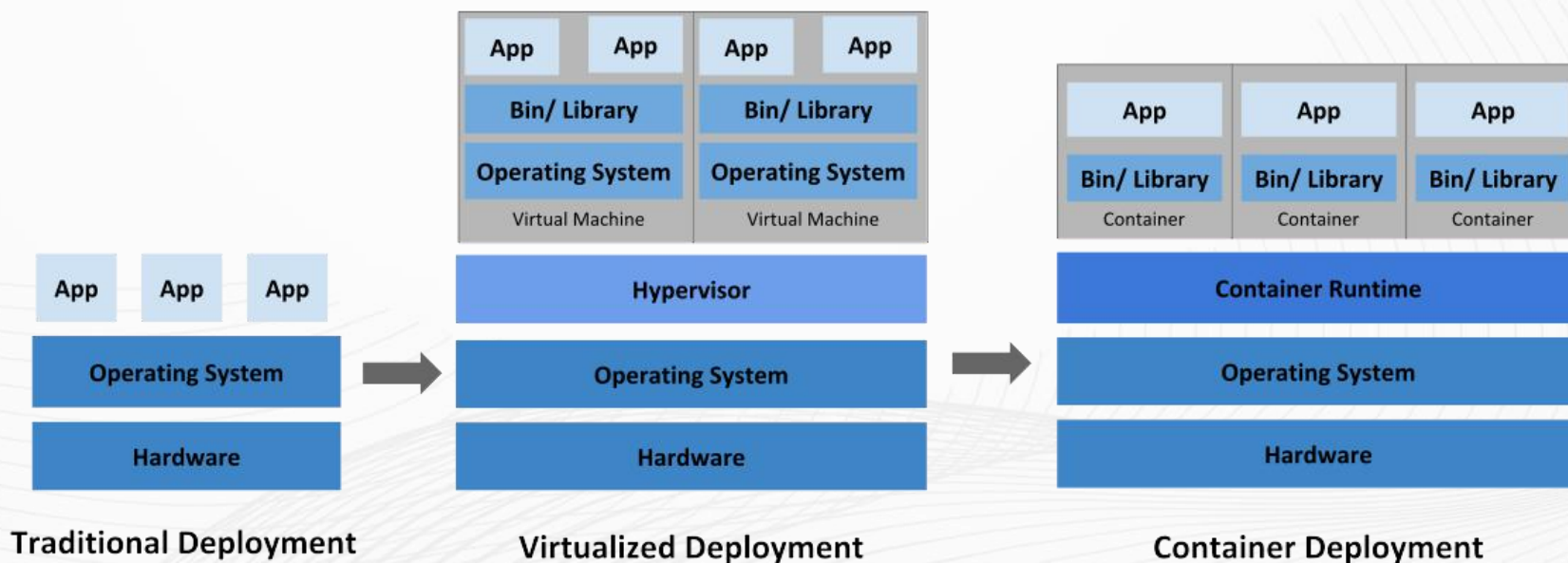
# 容器技术的利与弊

## 容器技术的优势

- 统一的交付单元
- 可移植性
- 资源隔离
- Cgroups
- Namespace
- 低成本
- 易于做 CI/CD

## 容器技术的弊端

- 隔离性不足
- 共享内核



# ► K8S环境下的安全挑战

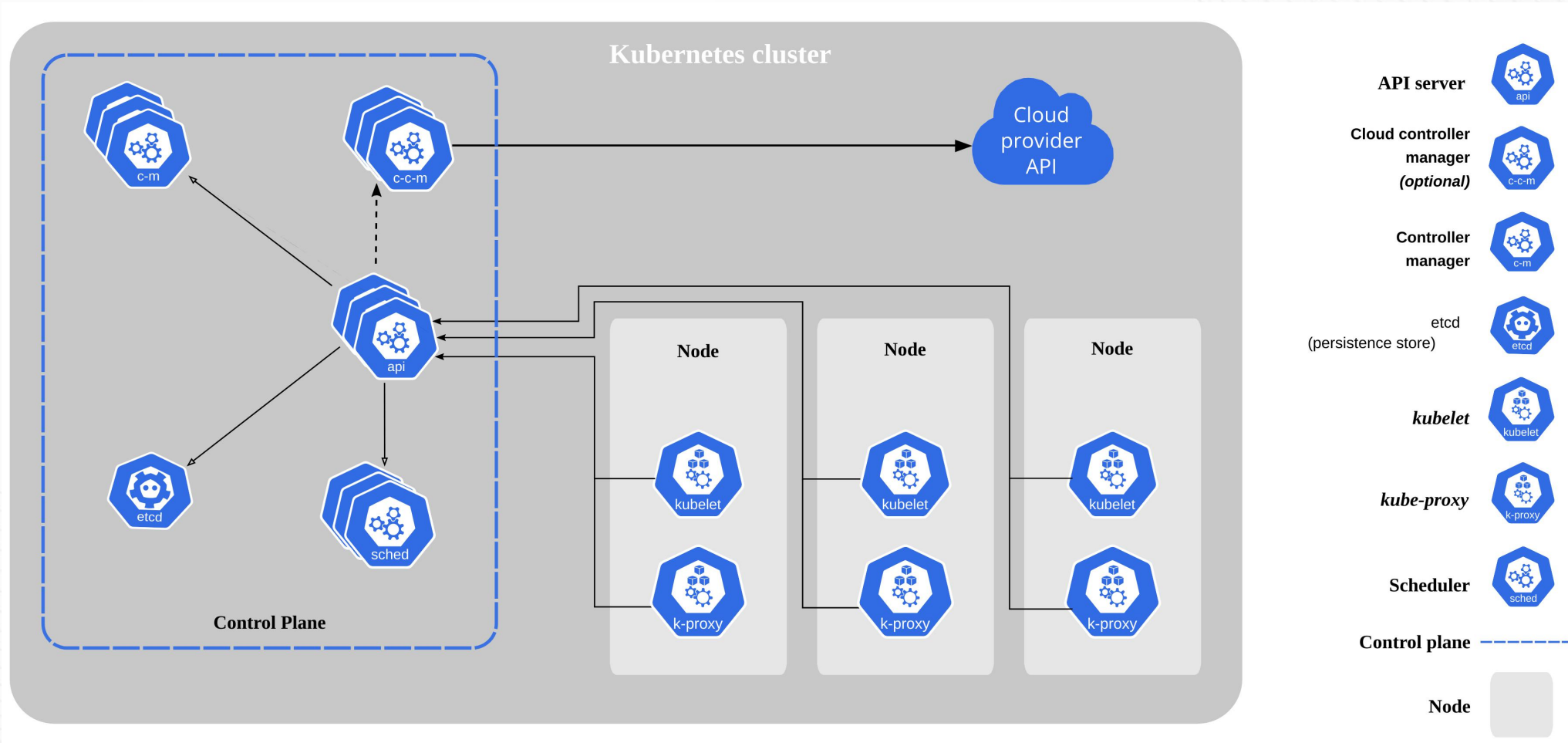
- 攻击面增加
- 供应链攻击
- 权限提升
- 网络安全
- 资源安全
- 数据安全
- 组件安全
- 运行时安全



# K8S环境下的安全挑战

## 攻击面增加

- K8S自身组件
- 底层容器运行时

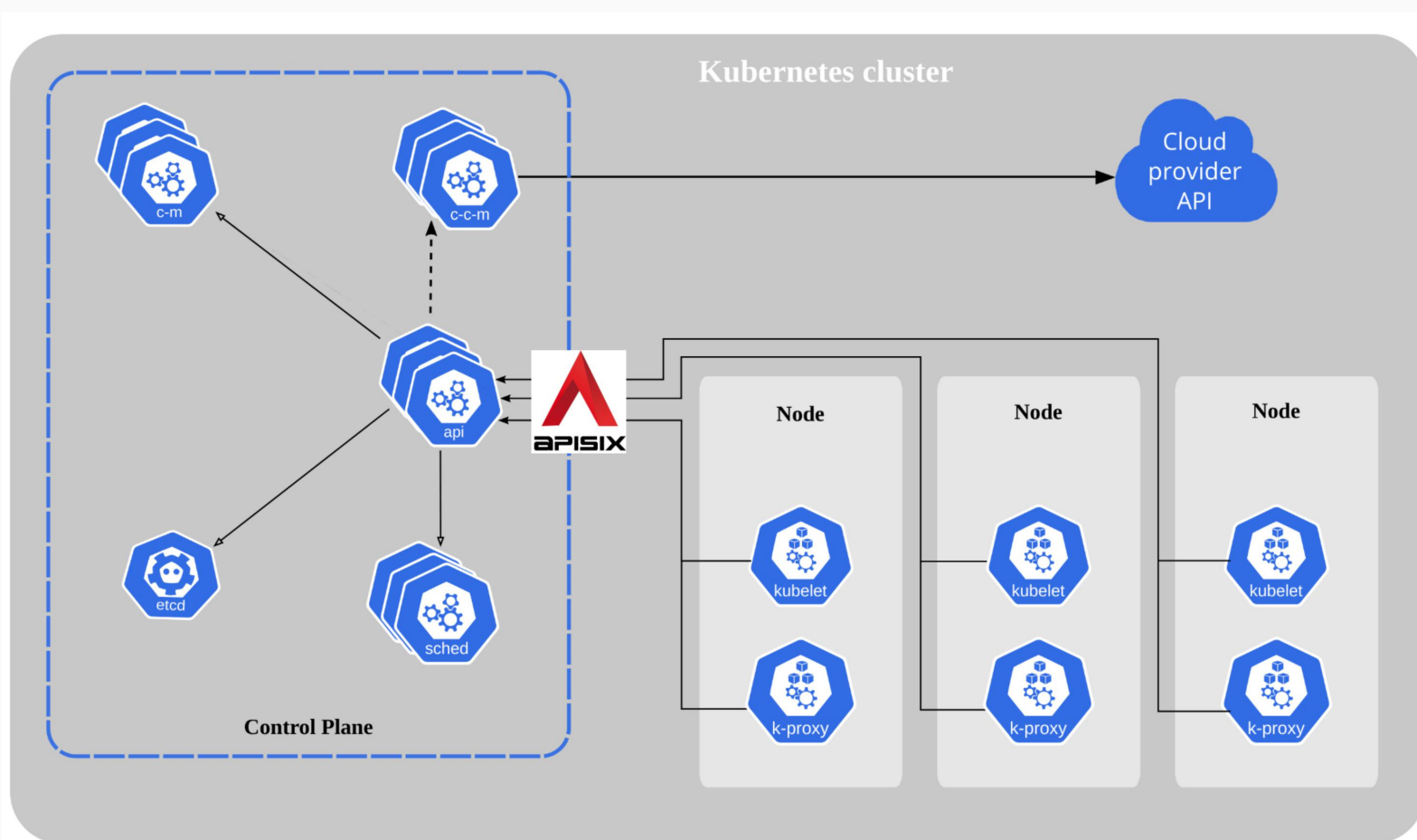


- CVE-2019-11253: 发送大型YAML/JSON对kube-apiserver DoS

# ► K8S环境下安全问题的应对方式

## 攻击面增加

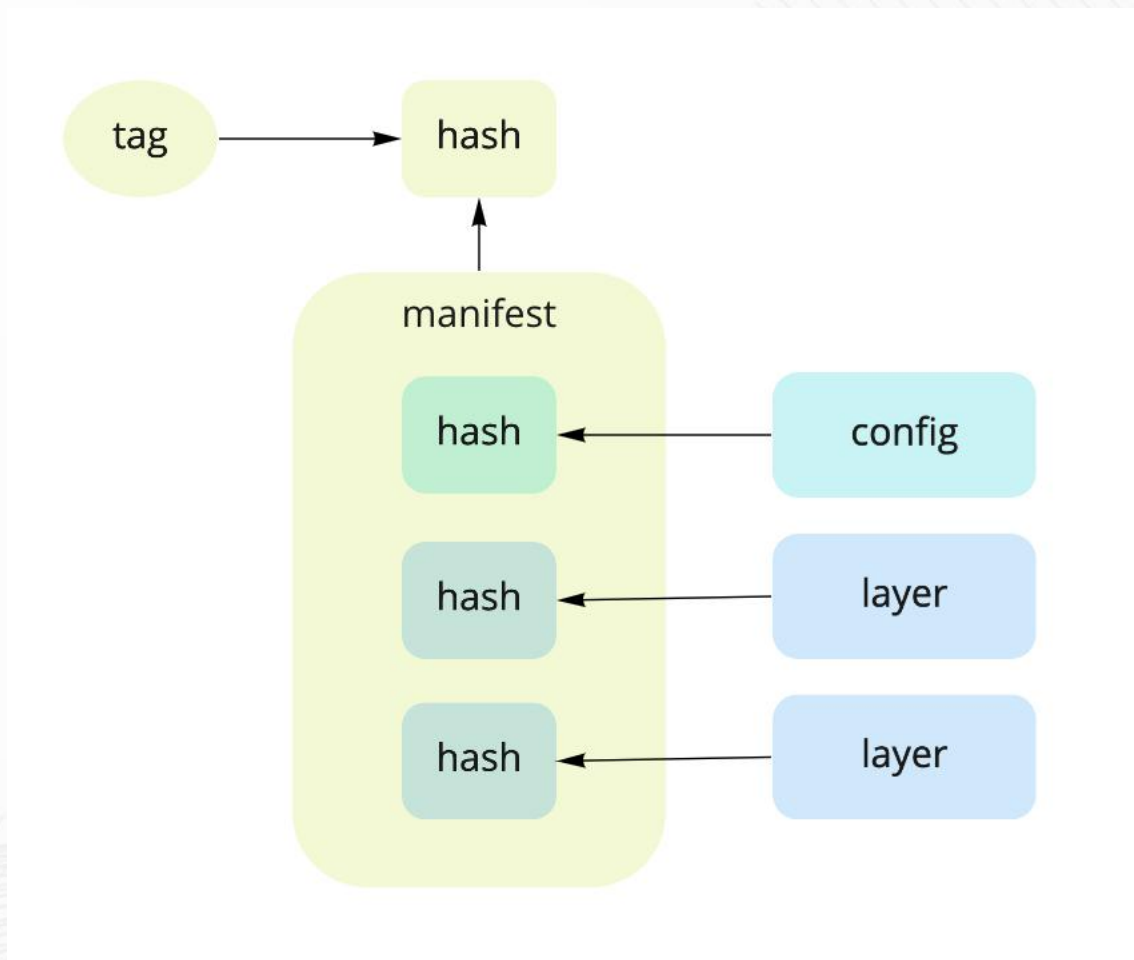
- 定义边界
- kube-apiserver 放在 LB 后,  
● 或者不暴露在公网
- Node 禁止 SSH
- 最小化权限



# ► K8S环境下的安全挑战

## 供应链攻击

- 不易生成 SBOM (软件材料清单)
- 恶意容器镜像
- 镜像内软件漏洞



图源: <https://nishakm.github.io/code/metadata/>



# ► K8S环境下安全问题的应对方式

## 供应链攻击

- 使用可信基础镜像 (Docker官方镜像)
- 及时更新
- 不安装debug工具
- Distross
- 镜像漏洞扫描
- DevSecOps

```
→ ~ docker scan redis:alpine

Testing redis:alpine ...

Package manager:   apk
Project name:      docker-image|redis
Docker image:      redis:alpine
Platform:          linux/amd64

√ Tested 17 dependencies for known vulnerabilities, no vulnerable paths found.
```

# ► K8S环境下的安全挑战

## 权限提升

- RBAC不合理(各种 controller/operator 中常见)
- 进入 Pod 内可操作 API
- 基础软件提权

```
● ● ●  
/ # TOKEN=$(cat /var/run/secrets/kubernetes.io/serviceaccount/token)  
/ # curl --cacert /var/run/secrets/kubernetes.io/serviceaccount/ca.crt -H "Authorization: Bearer  
$TOKEN" -s https://kubernetes.default:443/api/v1/xxxxx
```

# ▶ K8S环境下安全问题的应对方式

## 权限提升

- RBAC 配置review
- 如何开启 audit log
  - audit-log-path
  - audit-policy-file

```
kind: Cluster
apiVersion: kind.x-k8s.io/v1alpha4
nodes:
- role: control-plane
  extraMounts:
  - hostPath: /home/tao/audit/audit
    containerPath: /tmp/audit
- role: worker
kubeadmConfigPatches:
- |
  kind: ClusterConfiguration
  apiServer:
    extraArgs:
      audit-log-path: "/tmp/audit/audit.log"
      audit-policy-file:
"/tmp/audit/policy.yaml"
    extraVolumes:
    - name: audit
      hostPath: /tmp/audit
      mountPath: /tmp/audit
```

# ▶ K8S环境下安全问题的应对方式

## 权限提升

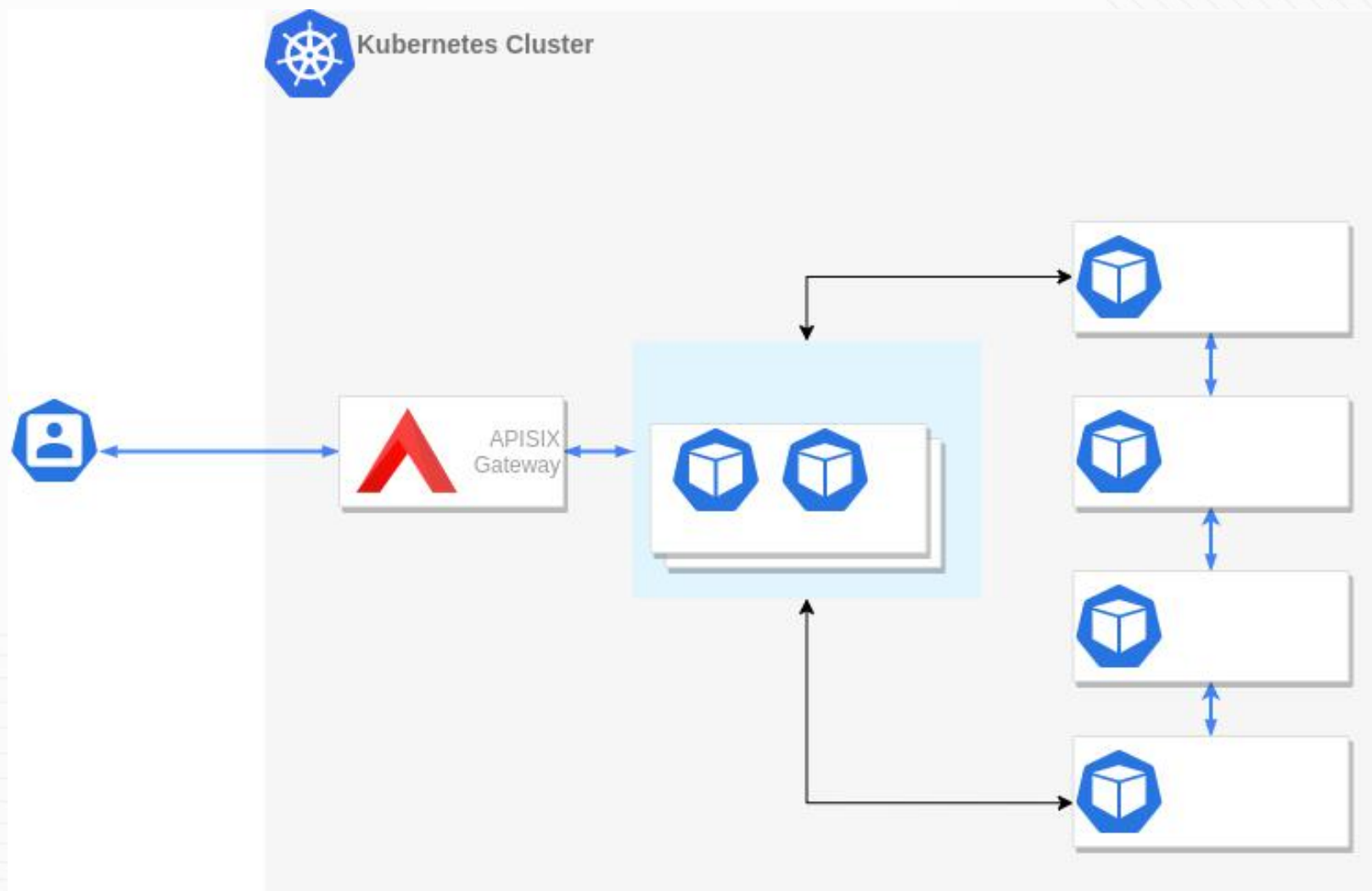
- Audit log 可记录操作行为, 响应状态码, UA, 时间等
- authorization.k8s.io/reason: 说明了 RBAC 规则决策的原因

```
{
  "kind": "Event",
  "apiVersion": "audit.k8s.io/v1",
  "level": "Request",
  "auditID": "027ddabb-c691-4524-aadd-0f1cf48efb34",
  "stage": "ResponseComplete",
  "requestURI": "/api/v1/namespaces/kube-system/configmaps",
  "verb": "list",
  "user": {
    "username": "system:serviceaccount:default:redis",
    "uid": "1982601b-4967-40cf-96f1-c456352bf1d2",
    "groups": [
      "system:serviceaccounts",
      "system:serviceaccounts:default",
      "system:authenticated"
    ],
    "extra": {
      "authentication.kubernetes.io/pod-name": ["redis"],
      "authentication.kubernetes.io/pod-uid": ["ba8c23b8-928b-4bc0-8bdd-3b227dab903e"]
    },
    "sourceIPs": ["172.18.0.3"],
    "userAgent": "curl/7.77.0",
    "objectRef": {
      "resource": "configmaps",
      "namespace": "kube-system",
      "apiVersion": "v1"
    },
    "responseStatus": {
      "metadata": {},
      "code": 200
    },
    "requestReceivedTimestamp": "2021-07-01T01:36:01.571190Z",
    "stageTimestamp": "2021-07-01T01:36:01.574197Z",
    "annotations": {
      "authorization.k8s.io/decision": "allow",
      "authorization.k8s.io/reason": "RBAC: allowed by ClusterRoleBinding \"redis-admin\" of ClusterRole \"cluster-admin\" to ServiceAccount \"redis/default\""
    }
  }
}
```

# K8S环境下的安全挑战

## 网络安全

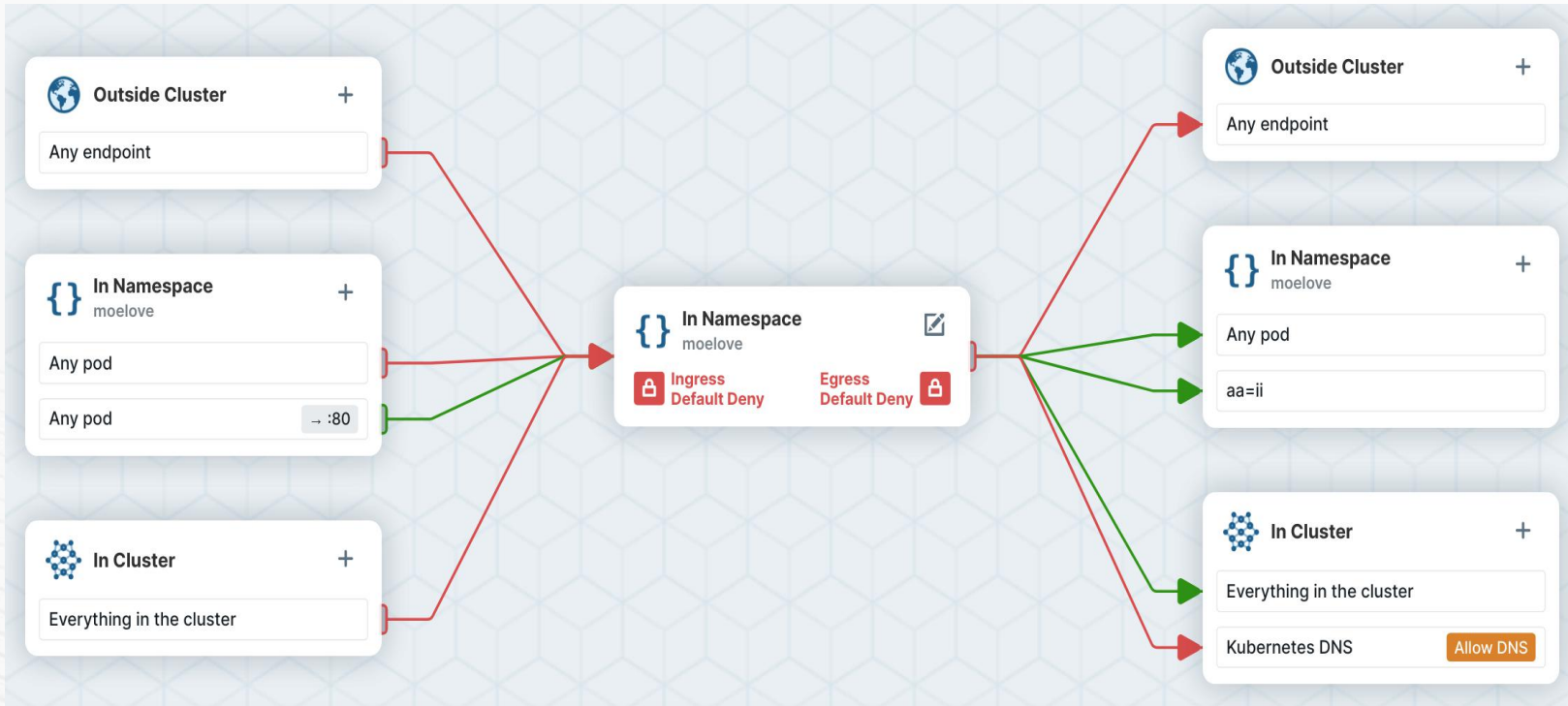
- 恶意访问
- 容器身份未标识
- 链接未加密
- 外层网关提供入口保护
- (南北向流量)



# K8S环境下安全问题的应对方式

## 网络安全

- 使用NetworkPolicy控制进出流量规则



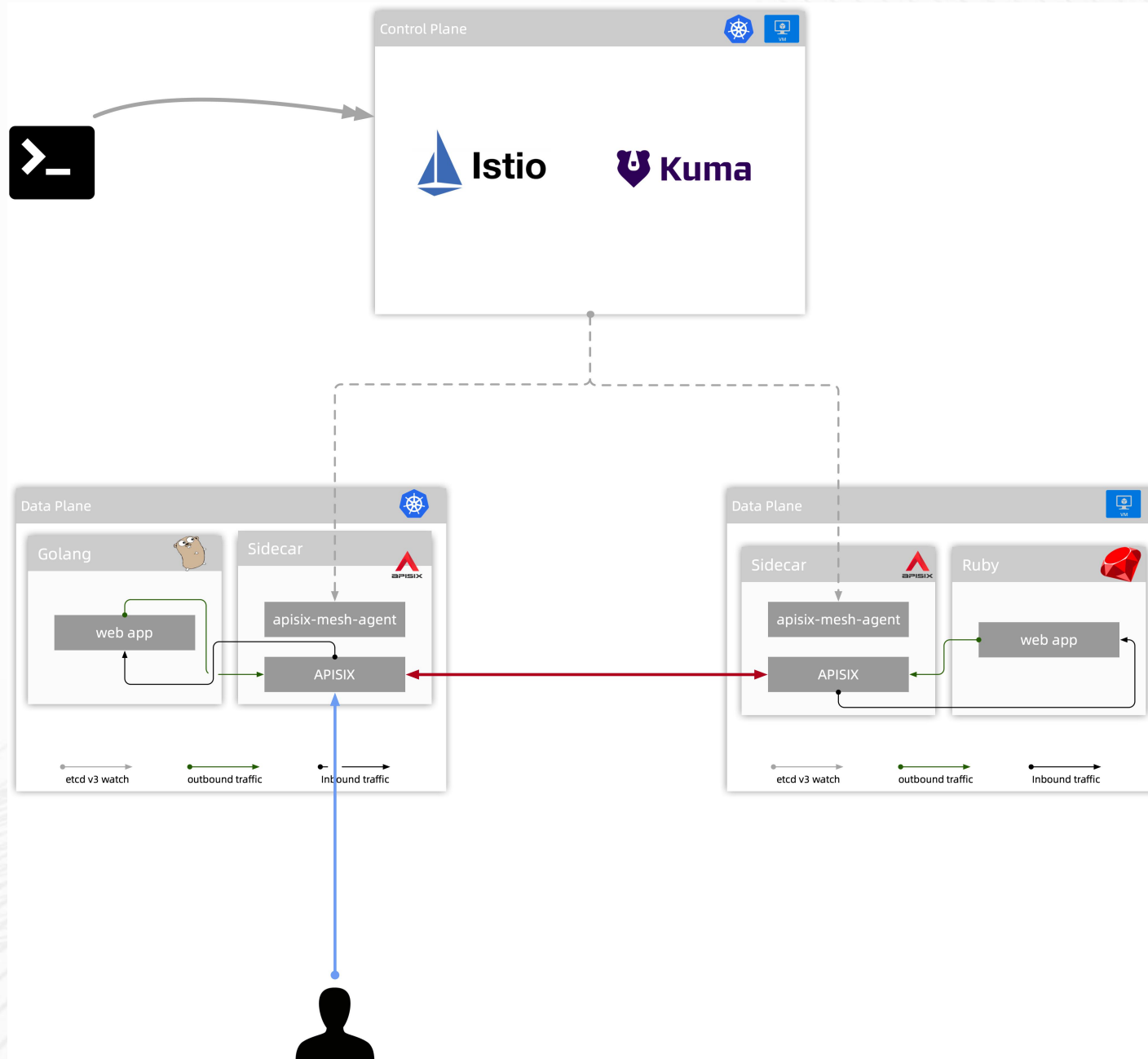
Network Policy Editor: <https://editor.cilium.io/>

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
spec:
  podSelector:
    matchLabels:
      role: db
  policyTypes:
  - Ingress
  ingress:
  - from:
    - ipBlock:
        cidr: 172.17.0.0/16
        except:
        - 172.17.1.0/24
    - namespaceSelector:
        matchLabels:
          project: myproject
    - podSelector:
        matchLabels:
          role: frontend
  ports:
  - protocol: TCP
    port: 6379
```

# K8S环境下安全问题的应对方式

## 网络安全

- service mesh
- mTLS
- 东西向流量



# ► K8S环境下的安全挑战

GOTC

## 资源安全

- 资源超售
- 过度征用资源
- OOM
- 驱逐



全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE



# ▶ K8S环境下安全问题的应对方式

## 资源安全

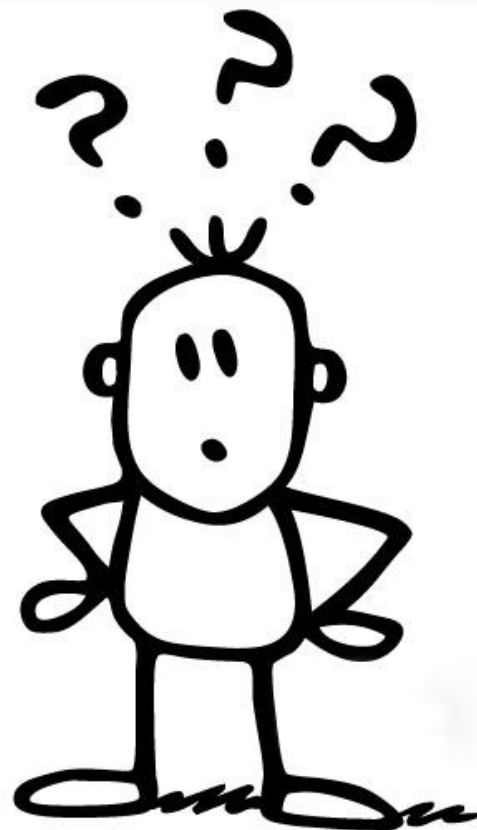
- 为 namespace 设置 Limit Range
- 设置 request 和 limit
- 合理的 QoS
  - Guaranteed
  - Burstable
  - BestEffort

```
X cat <<EOF | kubectl apply -f -
apiVersion: v1
kind: LimitRange
metadata:
  name: cpu-limit-range
spec:
  limits:
  - max:
    cpu: "800m"
    min:
    cpu: "200m"
    type: Container
---
apiVersion: v1
kind: Pod
metadata:
  name: pod-cpu-oversize
spec:
  containers:
  - name: cpu-oversize
    image: redis:alpine
    resources:
      limits:
        cpu: "1000m"
      requests:
        cpu: "500m"
EOF
limitrange/cpu-limit-range created
Error from server (Forbidden): error when creating "STDIN":
pods "pod-cpu-oversize" is forbidden:
maximum cpu usage per Container is 800m, but limit is 1
```

# ► K8S环境下的安全挑战

## 数据安全

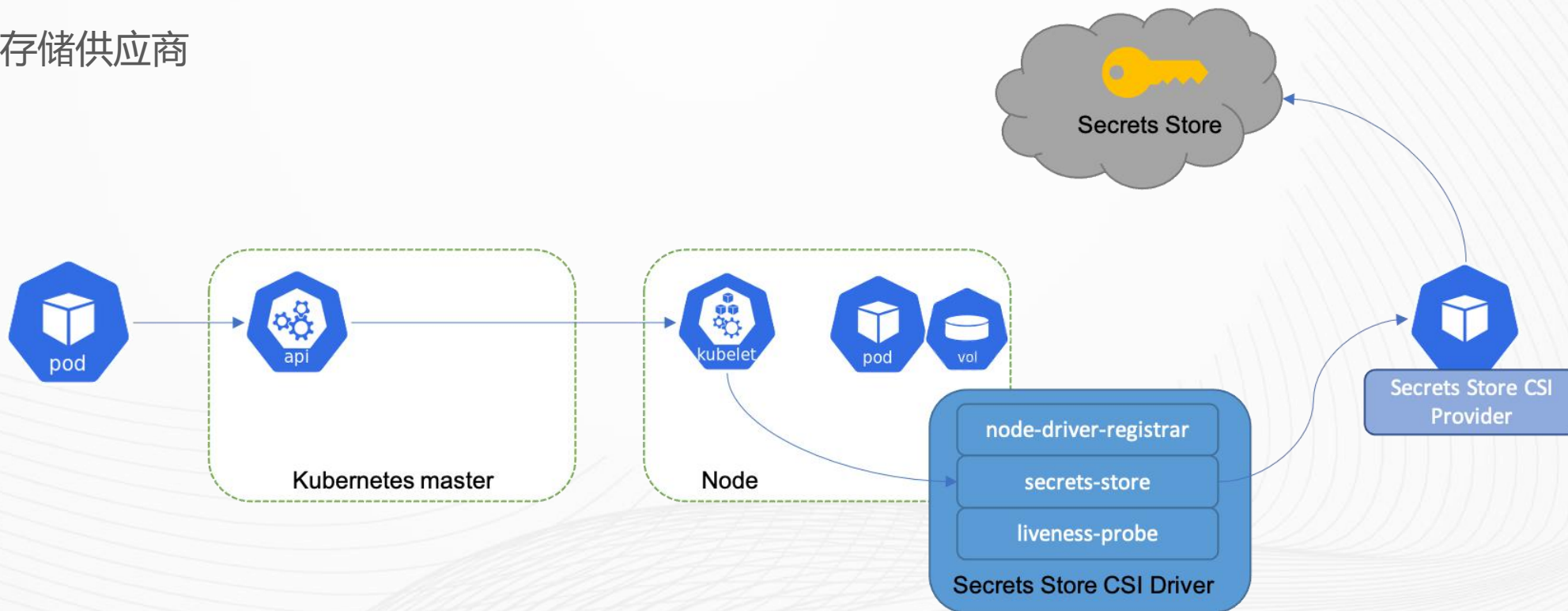
- Secrets not secret
- Base64 编码
- etcd 中数据可获取



# K8S环境下安全问题的应对方式

## 数据安全

- Kubernetes Secrets Store CSI Driver
  - [kubernetes-sigs/secrets-store-csi-driver](https://kubernetes-sigs.github.io/secrets-store-csi-driver/)
- 支持多种密钥存储供应商
  - AWS
  - Azure
  - GCP
  - Vault



# K8S环境下的安全挑战

## 组件安全

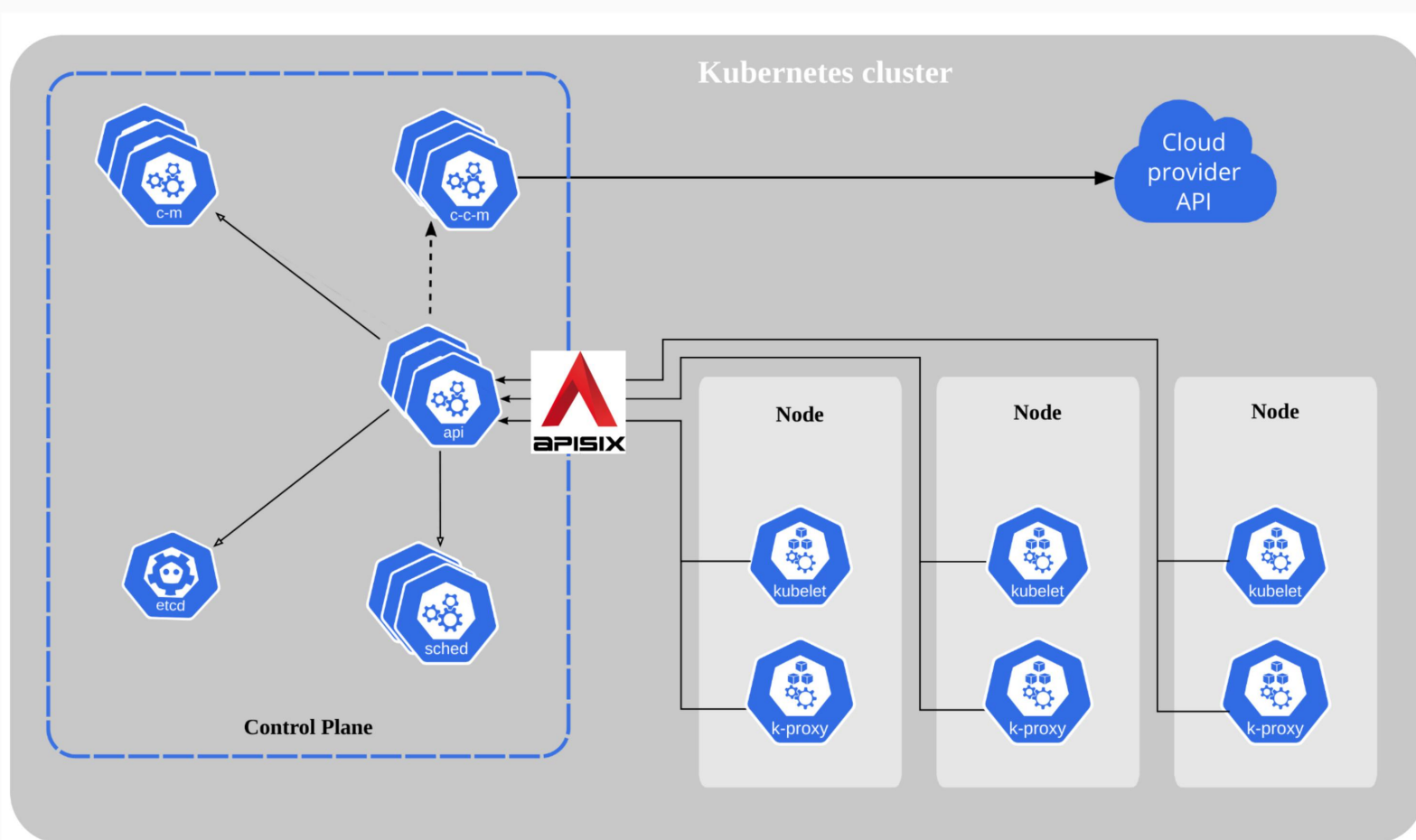
- CVE 漏洞及 POC
- 配置不规范
- 直接暴露在公网
- 匿名访问

[Security Advisory] CVE-2021-25737: Holes in EndpointSlice Validation Enable Host Network Hijack – A security issue w...	5月19日
[Kubernetes Java Client] CVE-2021-25738: Code exec via yaml parsing – Hello Kubernetes Community, A security issue ...	5月18日
[Security Advisory] CVE-2021-25736: Windows kube-proxy LoadBalancer contention – Hello Kubernetes Community, A s...	5月11日
[Security Advisory] CVE-2020-8562: Bypass of Kubernetes API Server proxy TOCTOU – Hello Kubernetes Community, A ...	5月5日
CVE-2021-25735: Validating Admission Webhook does not observe some previous fields – A security issue was discove...	4月15日
Fwd: [Security Advisory] CVE-2020-8570: Path Traversal bug in the Java Kubernetes Client – ----- Forwarded message...	1月12日

# K8S环境下安全问题的应对方式

## 组件安全

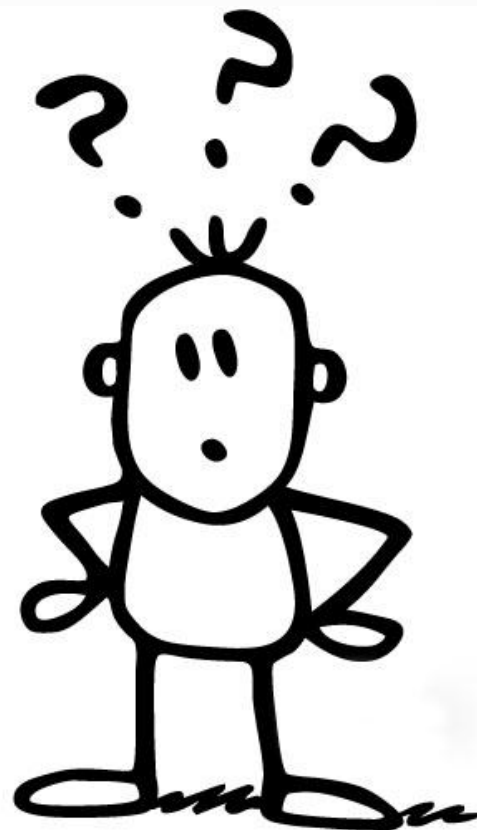
- 关注CVE漏洞及 POC
- 及时升级或绕过漏洞
- 不直接暴露在公网或增加认证
- 关闭匿名访问



# ► K8S环境下的安全挑战

## 运行时安全

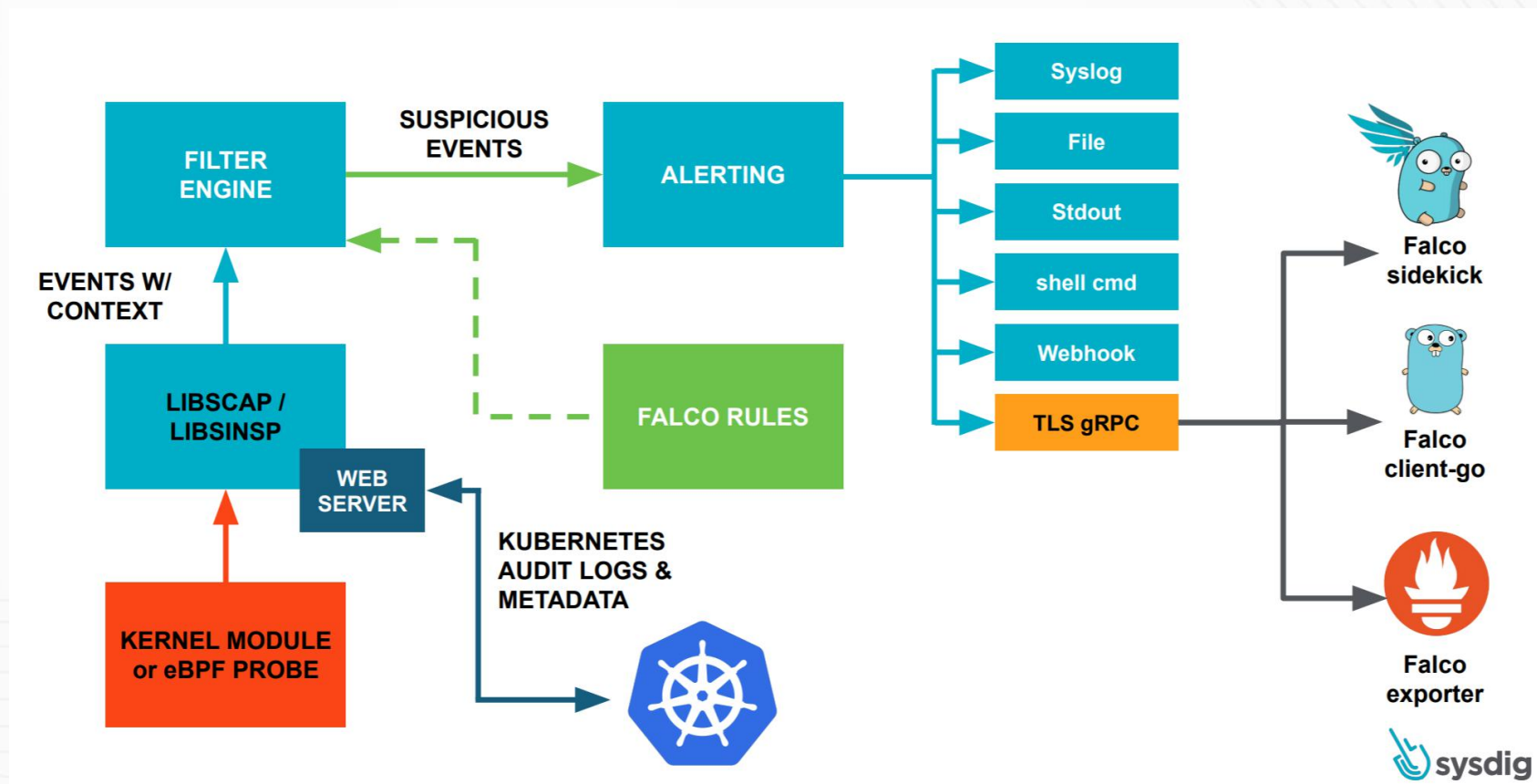
- 恶意操作
- 被攻击
- 非预期行为
- 未解决的漏洞
- 不安全配置
- 用户证书泄漏



# K8S环境下安全问题的应对方式

## 运行时安全

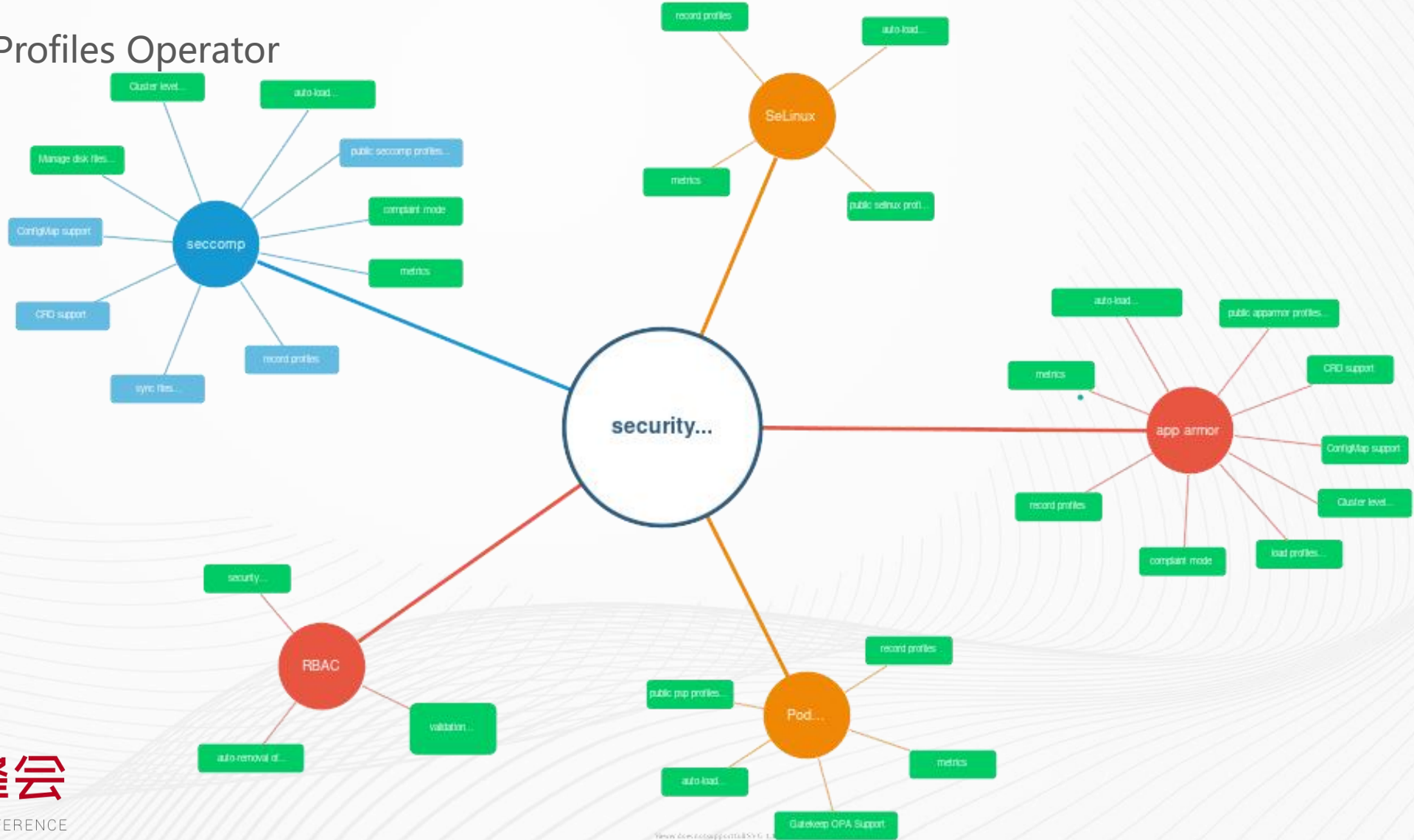
### ● Falco



# K8S环境下安全问题的应对方式

## 运行时安全

- Kubernetes Security Profiles Operator
- seccomp is GA
- 权限最小化





- 权限最小化
- 使用 Apache APISIX 等LB提供边界安全
- 及时关注安全漏洞和更新
- 优化配置
- 关注日志
- K8S生态周报
- <https://github.com/tao12345666333/practical-kubernetes>



**GOTC**

**THANKS**

**全球开源技术峰会**

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE