



АУДИТ БЕЗОПАСНОСТИ KUBERNETES КЛАСТЕРА БЕЗ KUBERNETES КЛАСТЕРА



Сергей
Канибор

Luntry, R&D /
Container Security

Обо мне



Настоящая защита –
это не запреты, а правильно
расставленные ограничения

R&D / Container
Security в Luntry

Более 4 лет опыта
в ИБ

Специализация -
Безопасность
Контейнеров и Kubernetes

Редактор ТГ-канала
k8s (in) security

Багхантер

- Участник BI.ZONE Bug Bounty и Yandex Bug Bounty
- Автор зарегистрированных CVE и BDU

Спикер

VK Kubernetes
DevOpsConf
OFFZONE

BeКон
PHDays
DevOops



Agenda

- 01 Идея Cluster API
- 02 Безопасность Cluster API
- 03 Куда смотреть, чтобы было безопасно в будущем

Предыстория



Kubernetes Pentest

PEN TESTER

CORE
SECURITY
A HelpSystems Company



What my friends think I do



What my mom thinks I do



What society thinks I do



What hackers think I do

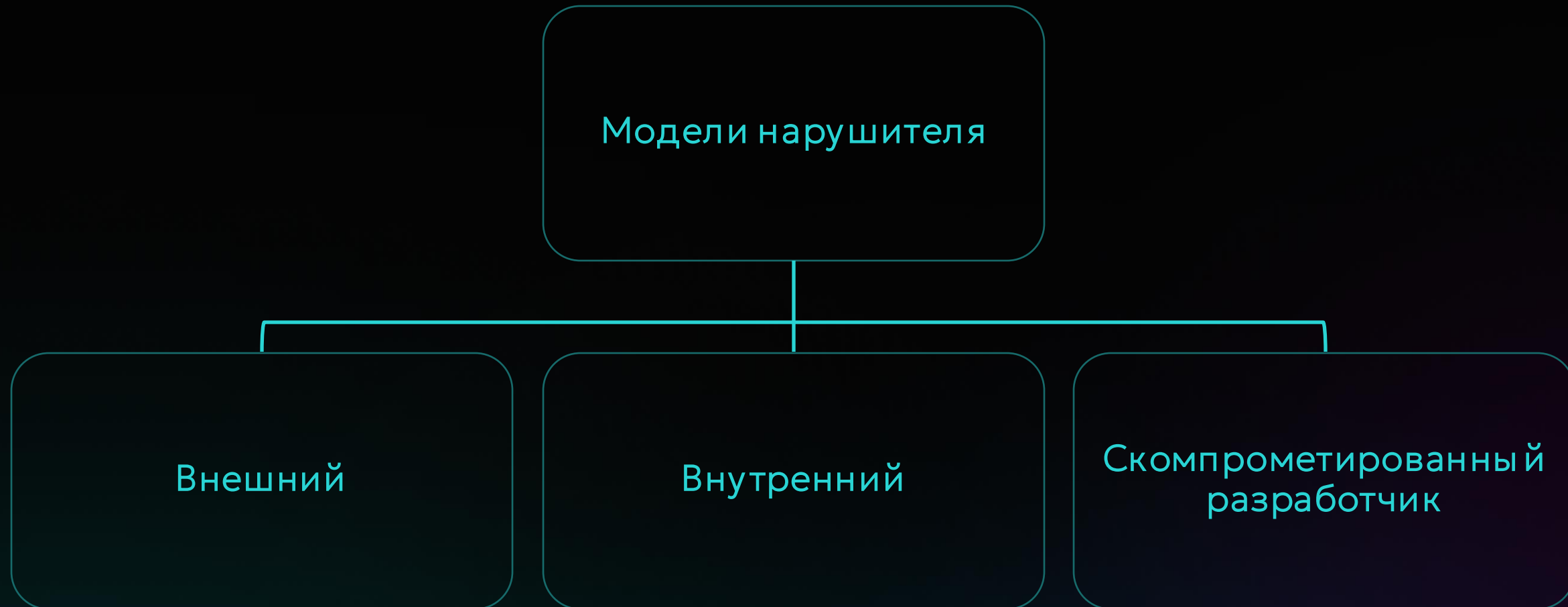


What I think I do



What I actually do

Модели нарушителя



Что мы проверяем?

```
└─ kubectl auth can-i --list
```

Resources

.

selfsubjectaccessreviews.authorization.k8s.io

selfsubjectrulesreviews.authorization.k8s.io

- Соответствие CIS K8s
- Политики Policy Engine
- Network Policy
- RBAC
- Эксплуатируем уязвимости рантайм и third-party компонентов

Non-Resource URLs	Resource Names	Verbs
[]	[]	[*]
[*]	[]	[*]
[]	[]	[create]
[]	[]	[create]
[/api/*]	[]	[get]
[/api]	[]	[get]
[/apis/*]	[]	[get]
[/apis]	[]	[get]
[/healthz]	[]	[get]
[/healthz]	[]	[get]
[/livez]	[]	[get]
[/livez]	[]	[get]
[/openapi/*]	[]	[get]
[/openapi]	[]	[get]
[/readyz]	[]	[get]
[/readyz]	[]	[get]
[/version/]	[]	[get]
[/version/]	[]	[get]
[/version]	[]	[get]
[/version]	[]	[get]

Что делать с Cluster API?

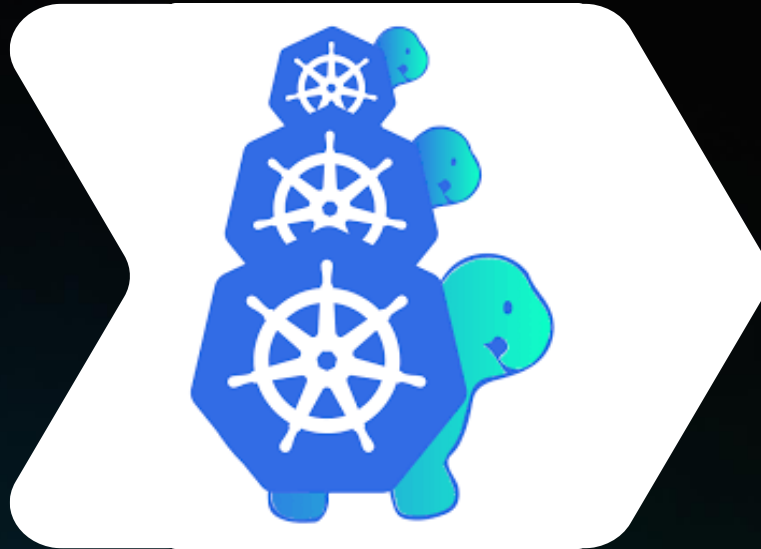




ИДЕЯ CLUSTER API

Проблемы и их решение

- Зоопарк кластеров
- Расхождение конфигураций
- Сложность обновлений и масштабирования



- Интеграции
- Унификация процесса создания k8s кластеров
- Автоматизация развертывания
- Масштабирование и управление
- Единый контроль

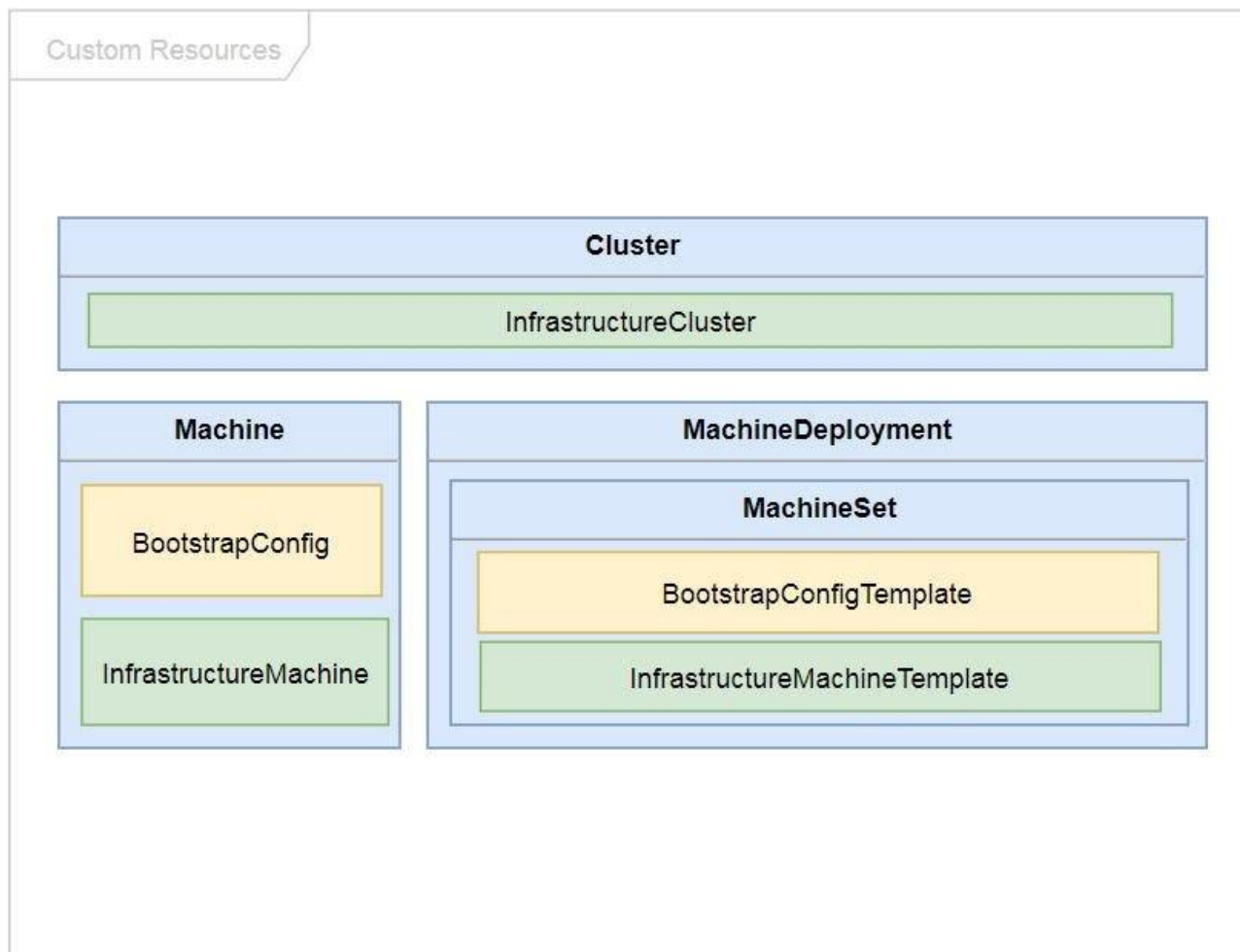
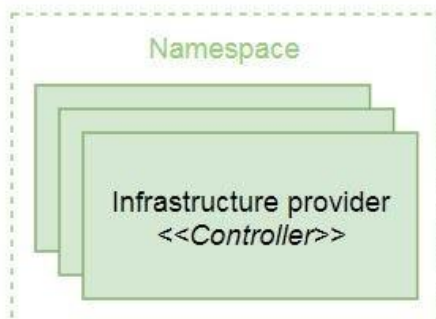
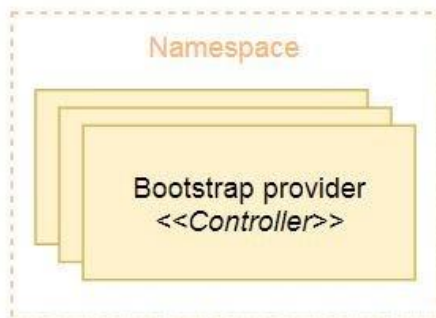
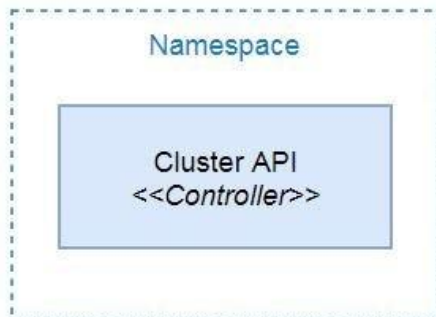
CAPi

- Начинаясь как проект SIG Cluster Lifecycle
- Первый релиз состоялся в июле 2018 года
- 3.7k звезд на GitHub
- Поддерживает десятки различных провайдеров
- Фреймворк для управления жизненным циклом Kubernetes кластеров

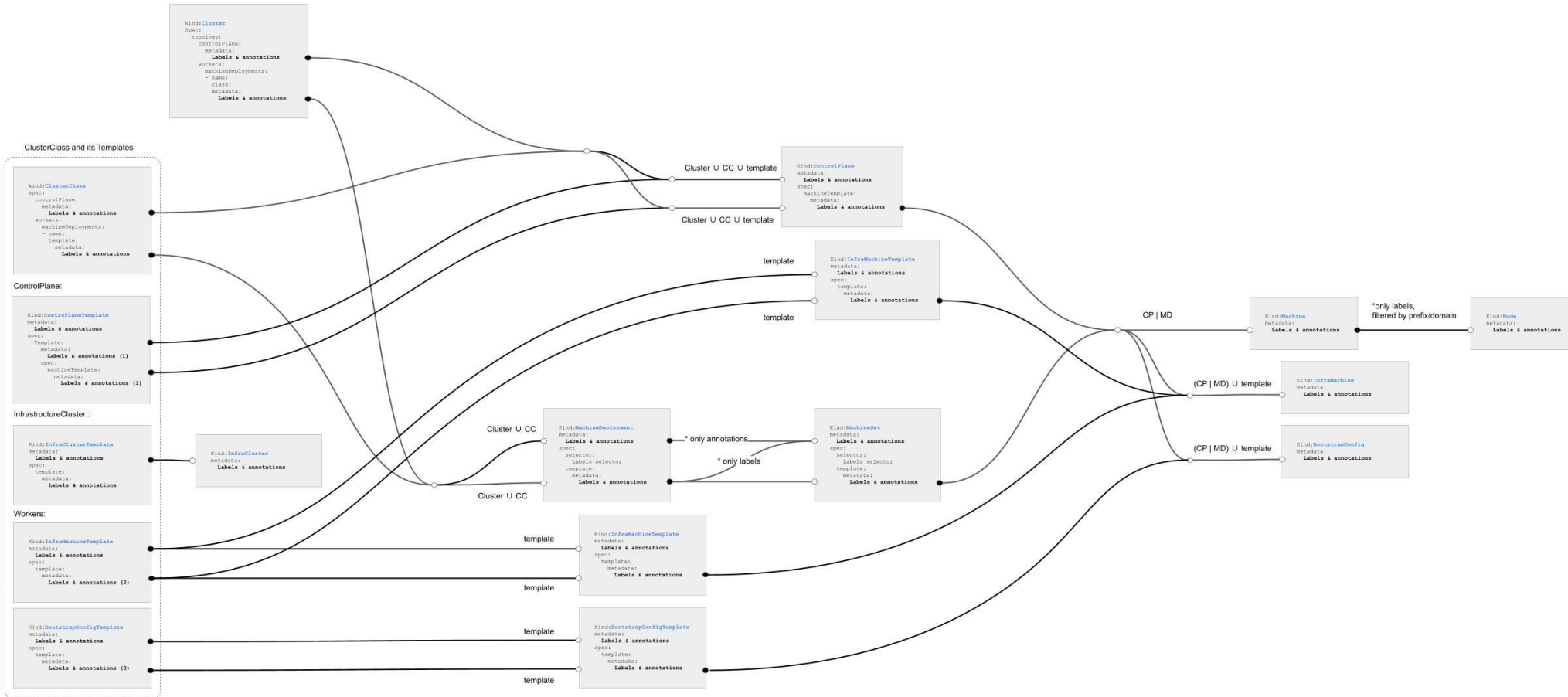
CAPI манифесты



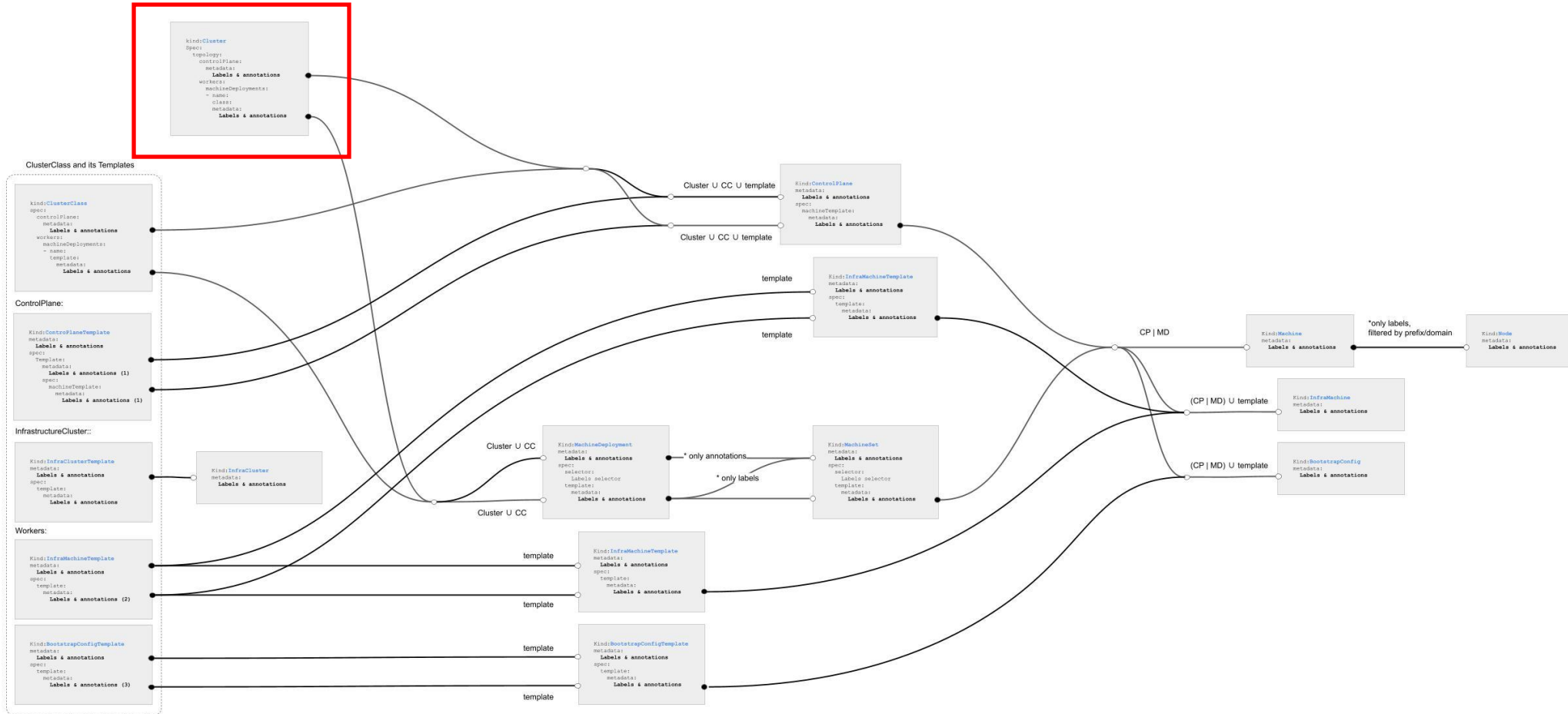
Management Cluster
Kubernetes



Metadata propagation



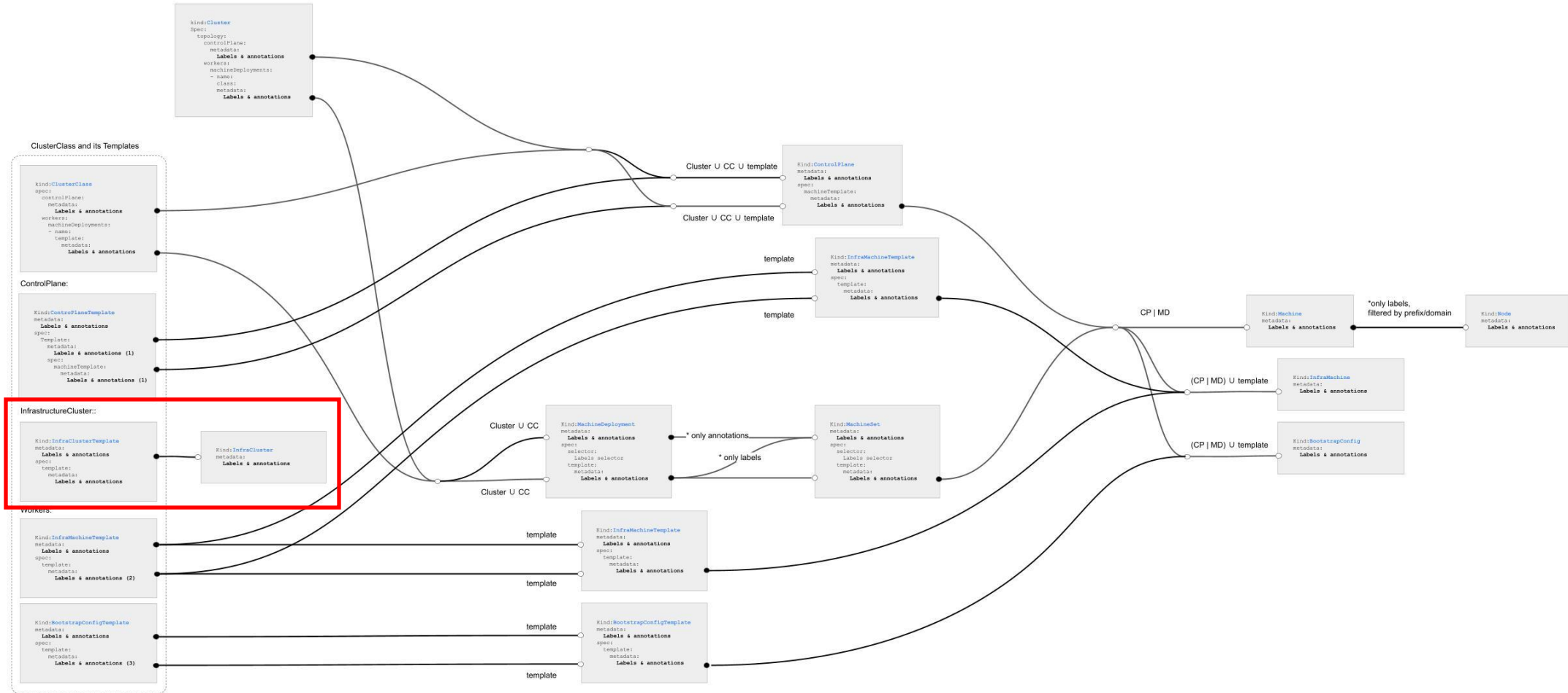
Cluster



Cluster Spec

```
spec:
  clusterNetwork:
    pods:
      cidrBlocks: ["192.168.0.0/16"]
    services:
      cidrBlocks: ["10.96.0.0/12"]
  infrastructureRef:
    apiVersion: infrastructure.cluster.x-k8s.io/v1beta1
    kind: AWSCluster
    name: my-cluster
  controlPlaneRef:
    apiVersion: controlplane.cluster.x-k8s.io/v1beta1
    kind: KubeadmControlPlane
    name: my-cluster-control-plane
```

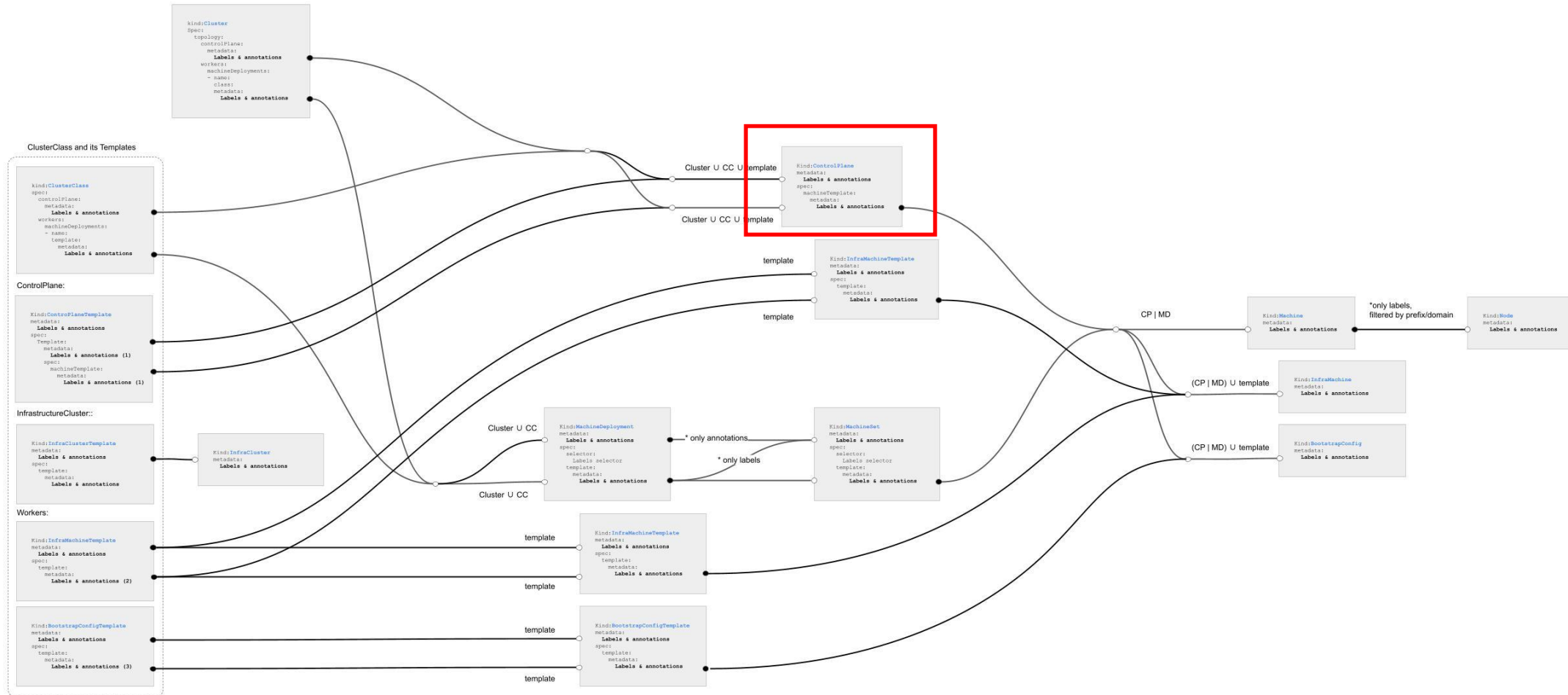
InfraCluster



InfraCluster Spec

```
spec:
  region: us-west-2
  network:
    vpc:
      id: "vpc-0abcd1234efgh5678"
    subnets:
      - id: "subnet-0abcd1234efgh5678"
        role: public
      - id: "subnet-0abcd1234efgh5679"
        role: private
  controlPlaneEndpoint:
    host: "my-cluster-api.example.com"
    port: 6443
```

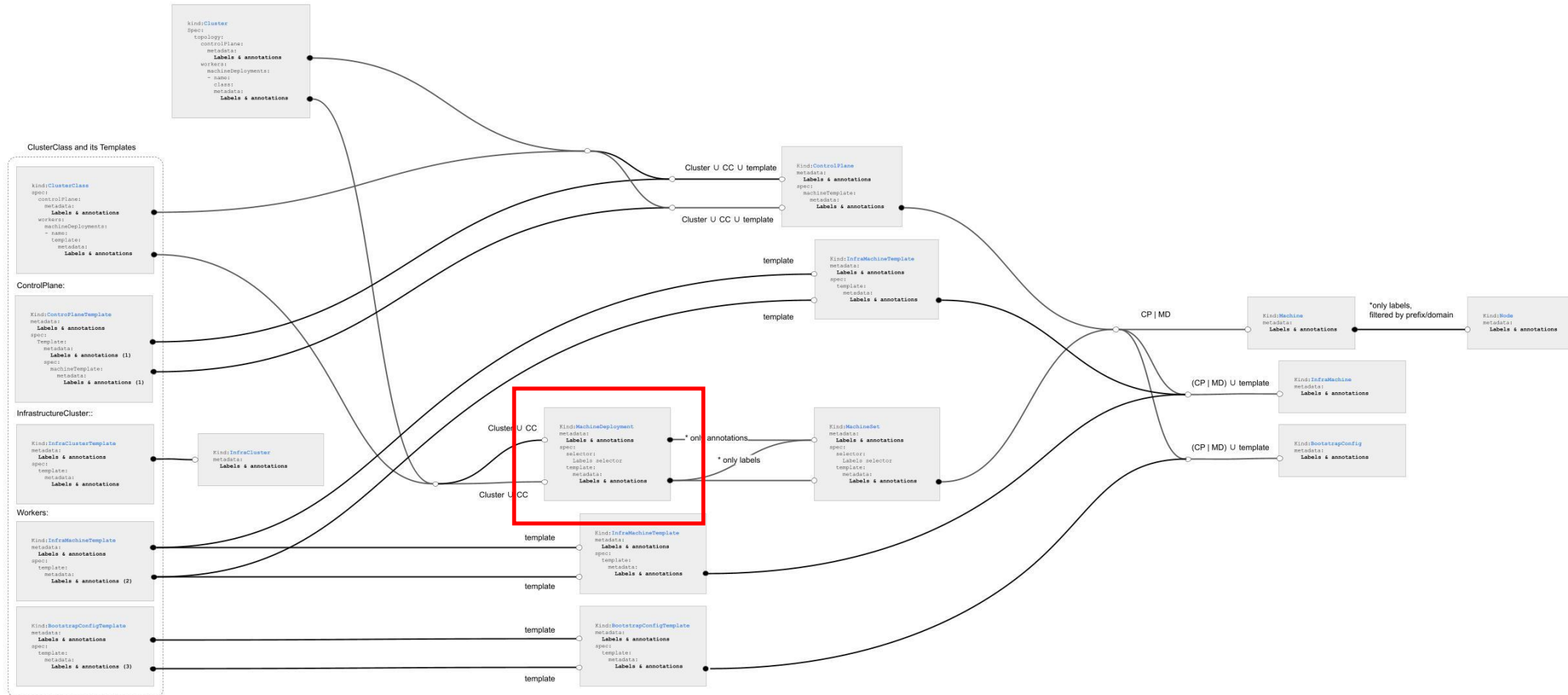
KubeadmControlPlane



KubeadmControlPlane Spec

```
spec:
  replicas: 3
  version: v1.27.3
  kubeadmConfigSpec:
    clusterConfiguration:
      apiServer:
        extraArgs:
          enable-admission-plugins: "NodeRestriction"
  infrastructureRef:
    apiVersion: infrastructure.cluster.x-
k8s.io/v1beta1
    kind: AWSMachineTemplate
    name: my-control-plane-machine-template
```

MachineDeployment

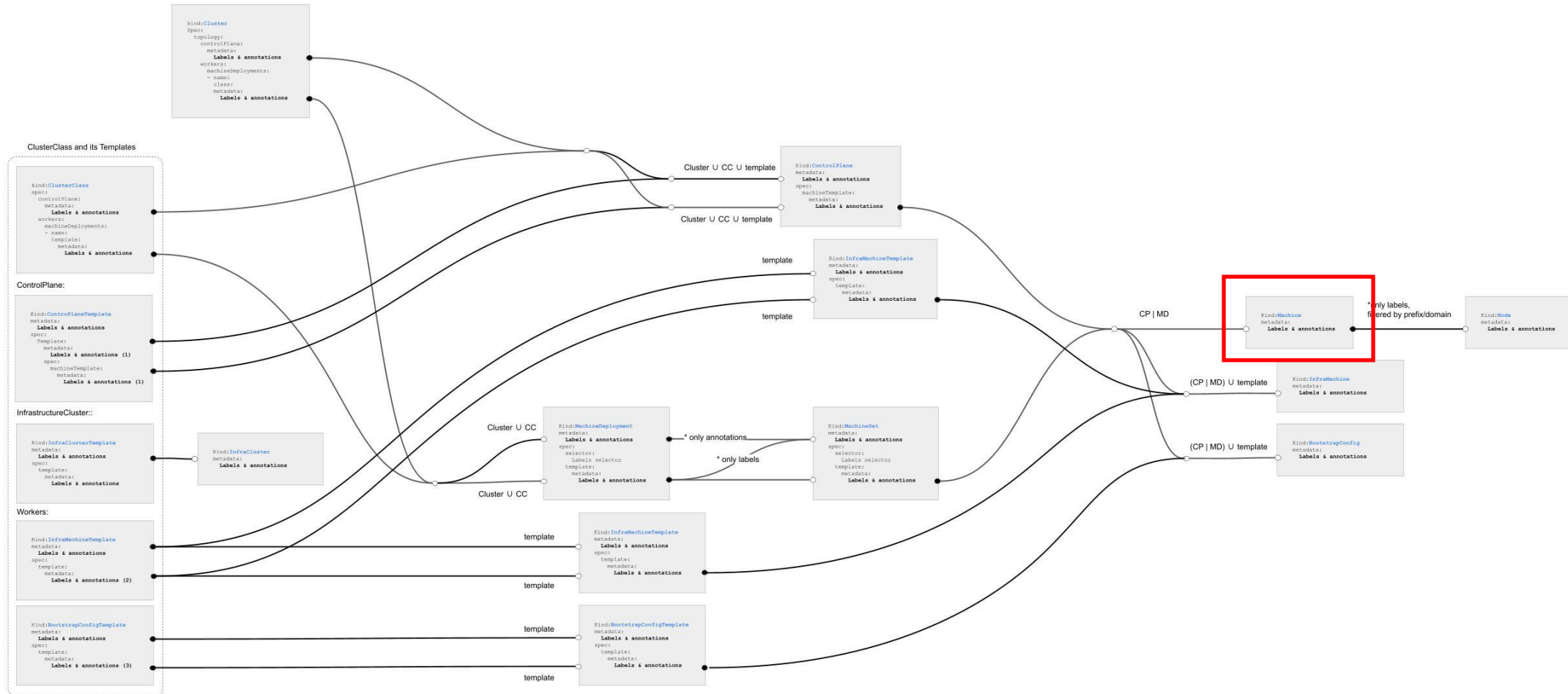


MachineDeployment Spec

spec:

```
  version: v1.27.3
  bootstrap:
    configRef:
      apiVersion: bootstrap.cluster.x-
k8s.io/v1beta1
      kind: KubeadmConfigTemplate
      name: my-cluster-md-0-bootstrap
    infrastructureRef:
      apiVersion: infrastructure.cluster.x-
k8s.io/v1beta1
      kind: AWSMachineTemplate
      name: my-cluster-md-0-machine-template
```

Machine



Machine Spec

```
spec:
  clusterName: my-cluster
  version: v1.27.3
  bootstrap:
    configRef:
      apiVersion: bootstrap.cluster.x-k8s.io/v1beta1
      kind: KubeadmConfig
      name: my-cluster-machine-1-bootstrap
  infrastructureRef:
    apiVersion: infrastructure.cluster.x-
k8s.io/v1beta1
    kind: AWSMachine
    name: my-cluster-machine-1
```



БЕЗОПАСНОСТЬ СAPI

Стандарты безопасности

- 01 CIS Kubernetes Benchmark
- 02 NSA/CISA Kubernetes Hardening Guide
- 03 Kubernetes Security Technical Implementation Guide (STIG)
- 04 PCI Security Standards Council
- 05 NIST Special Publication 800-190
- 06 Приказ ФСТЭК России N°118

Стандарты безопасности

- 01 Компоненты Control Plane
- 02 ETCD
- 03 Конфигурации Control Plane
- 04 Worker Nodes
- 05 Policies

CIS Kubernetes Benchmark

v1.10.0 - 09-23-2024

*порядка 130 проверок

Компоненты Control Plane

01 Конфигурационные файлы узлов Control Plane

02 API Server

03 Controller Manager

04 Scheduler

1.2.1 Ensure that the `--anonymous-auth` argument is set to false (Manual).....
1.2.2 Ensure that the `--token-auth-file` parameter is not set (Automated).....
1.2.3 Ensure that the `DenyServiceExternalIPs` is set (Manual)
1.2.4 Ensure that the `--kubelet-client-certificate` and `--kubelet-client-key` argumer
appropriate (Automated).....

2 etcd.....	
2.1 Ensure that the --cert-file and --key-file arguments are set as appropriate (Automated)	
2.2 Ensure that the --client-cert-auth argument is set to true (Automated).....	
2.3 Ensure that the --auto-tls argument is not set to true (Automated).....	
2.4 Ensure that the --peer-cert-file and --peer-key-file arguments are set as appropriate (Automated)	
2.5 Ensure that the --peer-client-cert-auth argument is set to true (Automated)	
2.6 Ensure that the --peer-auto-tls argument is not set to true (Automated)	
2.7 Ensure that a unique Certificate Authority is used for etcd (Manual).....	

Конфигурации Control Plane

01 Аутентификация и авторизация

02 Логирование/аудит

3 Control Plane Configuration	
3.1 Authentication and Authorization.....	
3.1.1 Client certificate authentication should not be used for users (Manual)	
3.1.2 Service account token authentication should not be used for users (Manual) .	
3.1.3 Bootstrap token authentication should not be used for users (Manual).....	
3.2 Logging.....	
3.2.1 Ensure that a minimal audit policy is created (Manual)	
3.2.2 Ensure that the audit policy covers key security concerns (Manual)	

Worker Nodes

01 Конфигурационные файлы узлов Worker Nodes

02 Конфигурация kubelet

- 4.2.1 Ensure that the `--anonymous-auth` argument is set to false (Automated)
- 4.2.2 Ensure that the `--authorization-mode` argument is not set to AlwaysAllow (Automated)
- 4.2.3 Ensure that the `--client-ca-file` argument is set as appropriate (Automated)
- 4.2.4 Verify that the `--read-only-port` argument is set to 0 (Manual)
- 4.2.5 Ensure that the `--streaming-connection-idle-timeout` argument is not set to 0 (Manual)
- 4.2.6 Ensure that the `--make-iptables-util-chains` argument is set to true (Automated)
- 4.2.7 Ensure that the `--hostname-override` argument is not set (Manual)

Policies

- 01 RBAC и Service Account
- 02 Pod Security Standards
- 03 Network Policies и CNI
- 04 Управление секретами
- 05 Сторонний Admission Controller
- 06 Общие политики

5 Policies	215
5.1 RBAC and Service Accounts	216
5.1.1 Ensure that the cluster-admin role is only used where required (Manual)	217
5.1.2 Minimize access to secrets (Manual)	219
5.1.3 Minimize wildcard use in Roles and ClusterRoles (Manual)	221
5.1.4 Minimize access to create pods (Manual)	223
5.1.5 Ensure that default service accounts are not actively used. (Manual)	225
5.1.6 Ensure that Service Account Tokens are only mounted where necessary (Manual)	227
5.1.7 Avoid use of system:masters group (Manual)	229
5.1.8 Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster (Manual)	231
5.1.9 Minimize access to create persistent volumes (Manual)	233
5.1.10 Minimize access to the proxy sub-resource of nodes (Manual)	234
5.1.11 Minimize access to the approval sub-resource of certificatesigningrequests objects (Manual)	236
5.1.12 Minimize access to webhook configuration objects (Manual)	238
5.1.13 Minimize access to the service account token creation (Manual)	240
5.2 Pod Security Standards	241
5.2.1 Ensure that the cluster has at least one active policy control mechanism in place (Manual)	242
5.2.2 Minimize the admission of privileged containers (Manual)	243
5.2.3 Minimize the admission of containers wishing to share the host process ID namespace (Manual)	245
5.2.4 Minimize the admission of containers wishing to share the host IPC namespace (Manual)	247
5.2.5 Minimize the admission of containers wishing to share the host network namespace (Manual)	249
5.2.6 Minimize the admission of containers with allowPrivilegeEscalation (Manual)	251
5.2.7 Minimize the admission of root containers (Manual)	253
5.2.8 Minimize the admission of containers with the NET_RAW capability (Manual)	255
5.2.9 Minimize the admission of containers with added capabilities (Manual)	257
5.2.10 Minimize the admission of containers with capabilities assigned (Manual)	259
5.2.11 Minimize the admission of Windows HostProcess Containers (Manual)	261
5.2.12 Minimize the admission of HostPath volumes (Manual)	263
5.2.13 Minimize the admission of containers which use HostPorts (Manual)	264
5.3 Network Policies and CNI	265
5.3.1 Ensure that the CNI in use supports Network Policies (Manual)	266
5.3.2 Ensure that all Namespaces have Network Policies defined (Manual)	268
5.4 Secrets Management	270
5.4.1 Prefer using secrets as files over secrets as environment variables (Manual)	271
5.4.2 Consider external secret storage (Manual)	273
5.5 Extensible Admission Control	274
5.5.1 Configure Image Provenance using ImagePolicyWebhook admission controller (Manual)	275
5.7 General Policies	277
5.7.1 Create administrative boundaries between resources using namespaces (Manual)	278
5.7.2 Ensure that the seccomp profile is set to docker/default in your pod definitions (Manual)	280
5.7.3 Apply Security Context to Your Pods and Containers (Manual)	282
5.7.4 The default namespace should not be used (Manual)	284

Чем проверять?

01 Kube-bench

02 Скрипты

03 Что-то своё



Инструменты

Минусы

- Внутренний регламент (может быть что угодно)
- Для полного покрытия нужно писать что-то своё

Плюсы

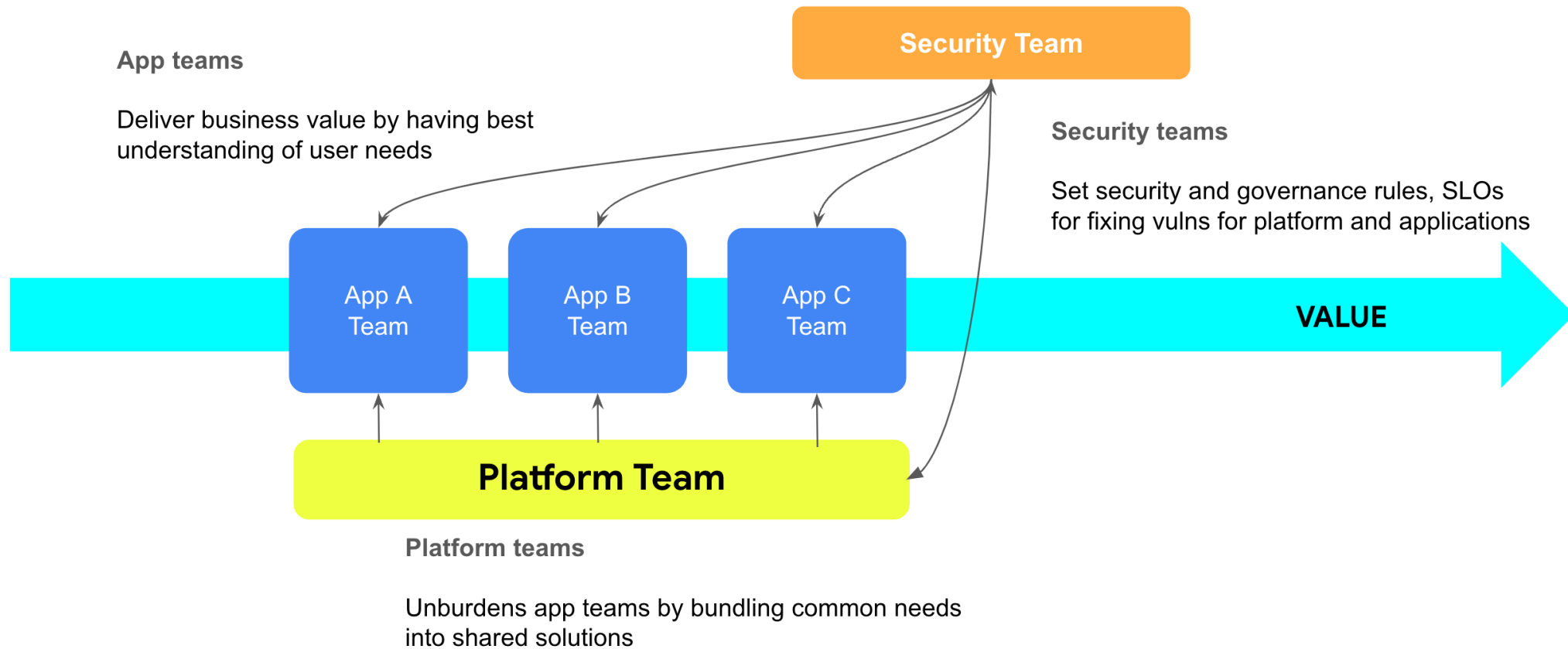
- Open Source ▣

**Куда смотреть, чтобы
было безопасно в
будущем**



КУДА СМОТРЕТЬ,
ЧТОБЫ БЫЛО БЕЗОПАСНО
В БУДУЩЕМ

Shift Down Security

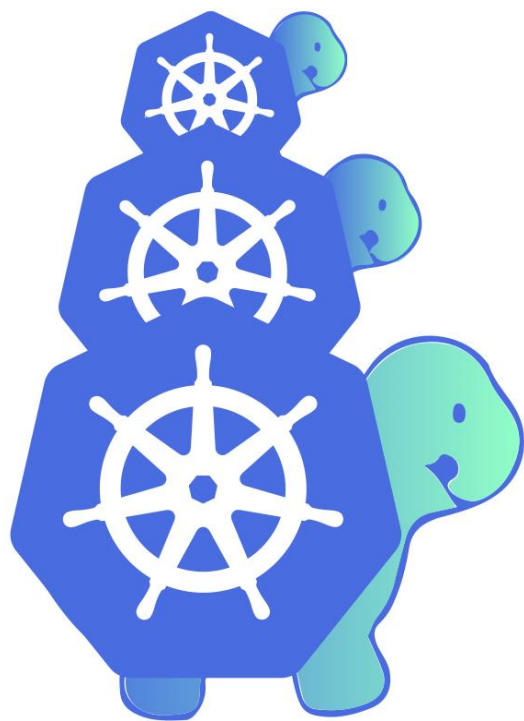


Всё есть YAML

- 01 Kubernetes – декларативная система
- 02 Любой ресурс в Kubernetes – это YAML
- 03 API манифесты – также набор YAML'ов

Уже понимаете, к чему я?

Используем Policy Engine



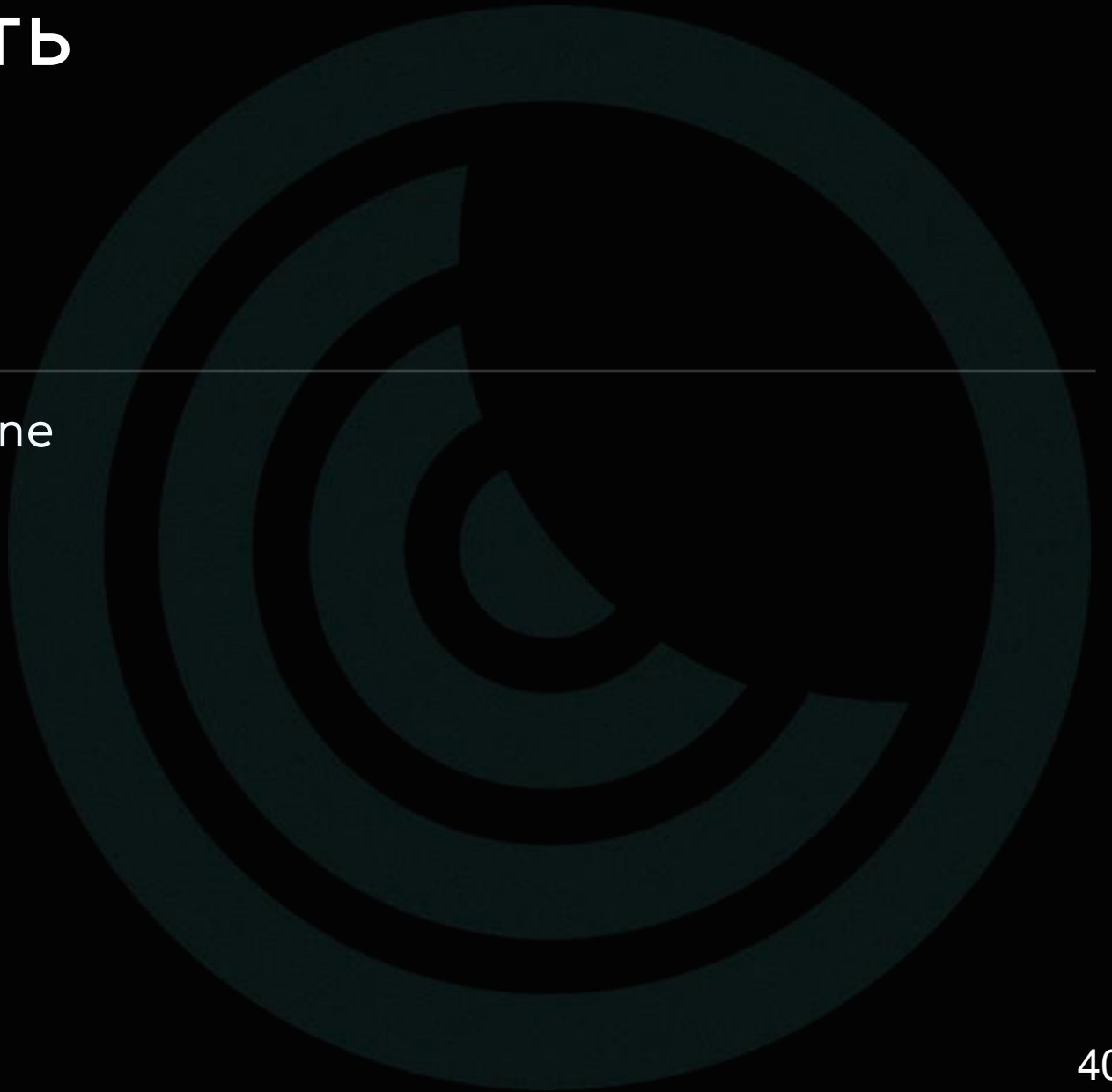
Kyverno

Для чего может быть полезно

-
- Проверить кластера еще на этапе провижининга
 - Удешевить и ускорить исправление мисконфигов

Что можно проверить

-
- Флаги компонентов Control & Data Plane
 - Версии ядра / ОС / container runtime



Что нельзя проверить

-
- Содержимое YAML манифестов
 - securityContext
 - Network Policy



Примеры

rules:

- name: validate-kubeadmcontrolplane-secure-params

match:

any:

- resources:

kinds:

- KubeadmControlPlane.controlplane.cluster.x-k8s.io

validate:

message: "KubeadmControlPlane must follow CIS Kubernetes Benchmark"

pattern:

spec:

kubeadmConfigSpec:

clusterConfiguration:

apiServer:

extraArgs:

audit-policy-file: "/etc/kubernetes/config/audit-policy.yaml",

authorization-mode: "RBAC,Node",

bind-address: "127.0.0.1",

enable-admission-plugins: "NamespaceLifecycle,NodeRestriction"

Примеры

```
rules:
- name: validate-kubeadmcontrolplane-secure-params
  match:
    any:
      - resources:
          kinds:
            - KubeadmControlPlane.controlplane.cluster.x-k8s.io
  validate:
    message: "KubeadmControlPlane must follow CIS Kubernetes Benchmark"
    pattern:
      spec:
        kubeadmConfigSpec:
          files:
            - content: |
                authentication:
                  anonymous:
                    enabled: false
                  webhook:
                    cacheTTL: 10s
                    enabled: true
                  x509:
                    clientCAFile: /etc/kubernetes/pki/ca.crt
                authorization:
                  mode: AlwaysAllow
```

ИТОГИ

CAPI / CIS K8s Benchmark	1	2	3	4	5
KubeadmControlPlane	59/59	7/7	5/5		0/35
KubeadmConfigTemplate				24/24	0/35

Порядка 73% процентов проверок CIS K8S Benchmark можно выполнить без существования кластера!

Вместо заключения

01

Kubernetes в каждый дом

02

Никогда не забывать про безопасность K8s

03

Можно сделать кластер безопасным, даже когда его не существует



📍 [luntry_official](#)

🌐 [luntry.ru](#)

📰 [luntrysolution](#)

✉ info@luntry.ru

📺 [luntrysolution](#)

СЕРГЕЙ КАНИБОР
R&D / Container Security Luntry

✉ sk@luntry.ru

📍 [@r0binak](#)

СПАСИБО
ЗА ВНИМАНИЕ