СЛОМАТЬСЯ ИЛИ СТАТЬ СИЛЬНЕЕ?

Зарисовки инцидентов с k8s в инфре MWS Cloud



Иван Гулаков

Head of SRE, KORE,
MWS Cloud Platform



Иван Гулаков

Техлид DevOps-команды



Занимаюсь развитием и поддержкой инфраструктуры для облачных сервисов.

Люблю контейнеры, качу кубы, пилю решения «из коробки».

Есть 3 кота, которые тоже охотно используют коробочные решения.

9 лет в ИТ и ещё не помер.

О чем поговорим?

01 Helicopter view на инфру облака: распределение сервисов по k8s, глобальные и зональные кластера.

02 Как у нас устроен типовой HA кластер k8s.

03 Как происходит управление парком кластеров.

04 Интересные инциденты вокруг k8s их RCA.



2 разных kubernetes(?)

CLOUD PAAS



Managed K8S

CLOUD IAAS

INFRA



KORE k8s

Немного терминов

Dom0

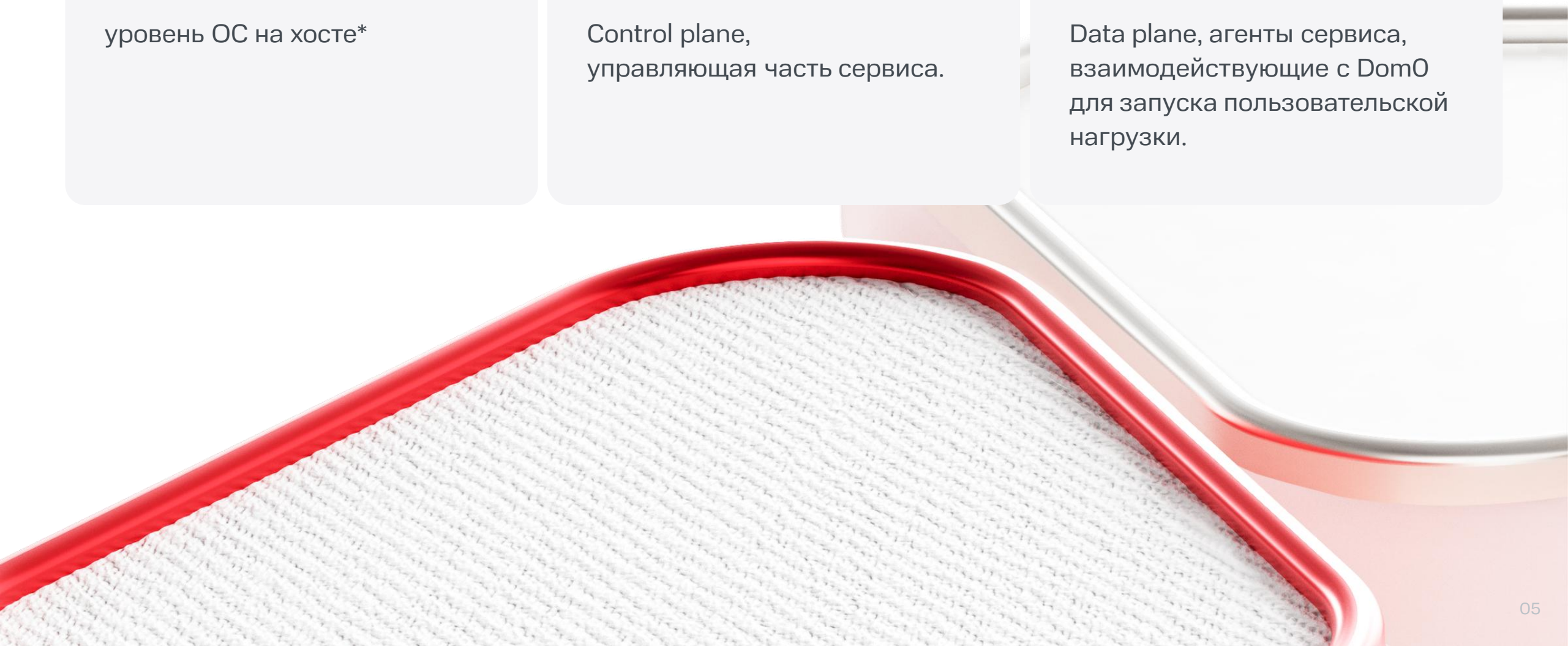
уровень ОС на хосте*

CPL

Control plane,
управляющая часть сервиса.

DPL

Data plane, агенты сервиса, взаимодействующие с Dom0 для запуска пользовательской нагрузки.



Вводные

01

Все сервисы запускаются в k8s.

02

Даже DPL часть сервисов.

03

Потеря CPL самого k8s не должна аффектить бизнес сервисы облака*



Типы кластеров

***-common**

Сервисные CPL + DB

***-compute**

Compute DPL

***-storage**

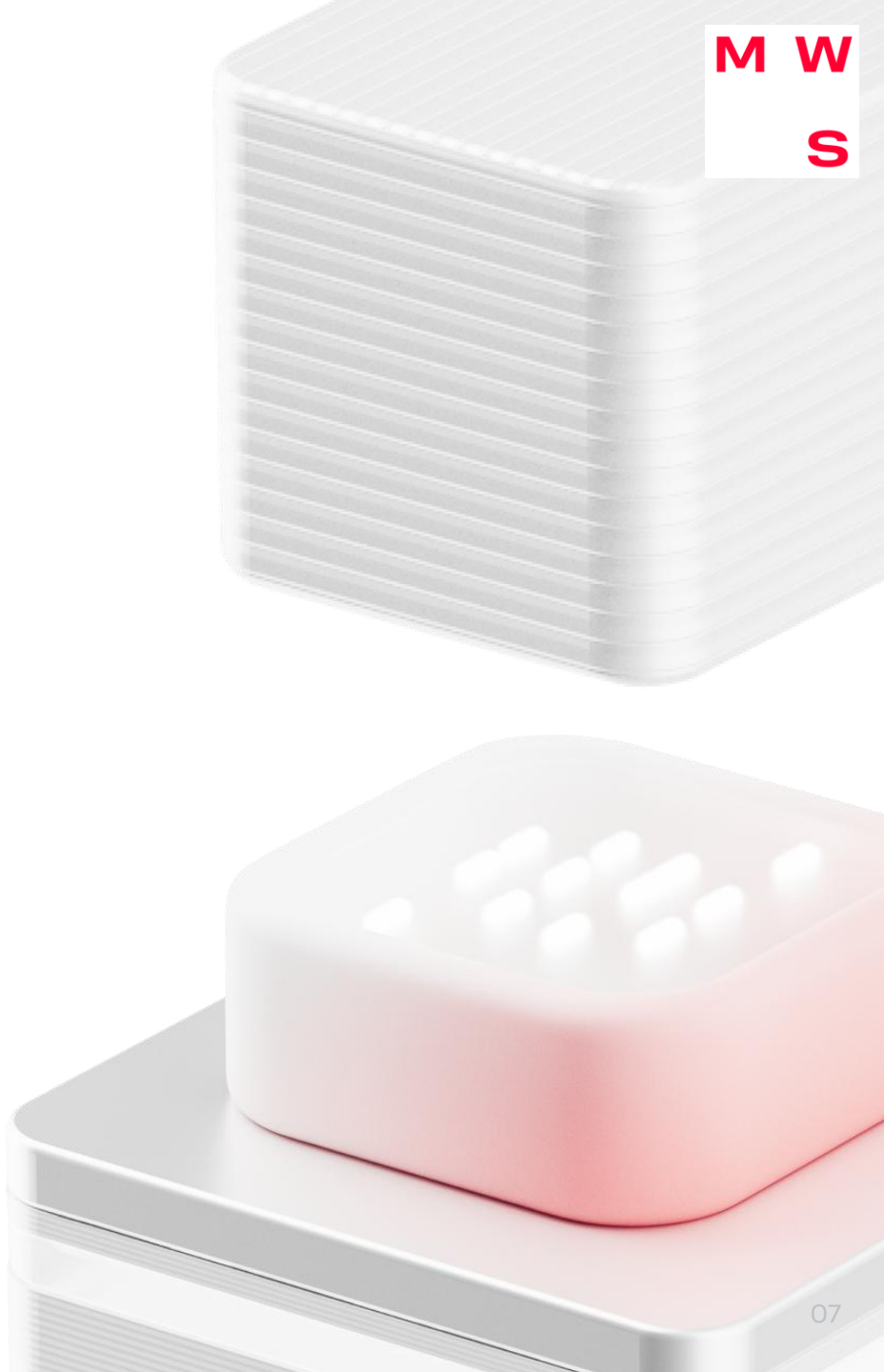
Storage DPL (CEPH)

***-nlb/fw/decap/vpc/external/bla-bla-bla**

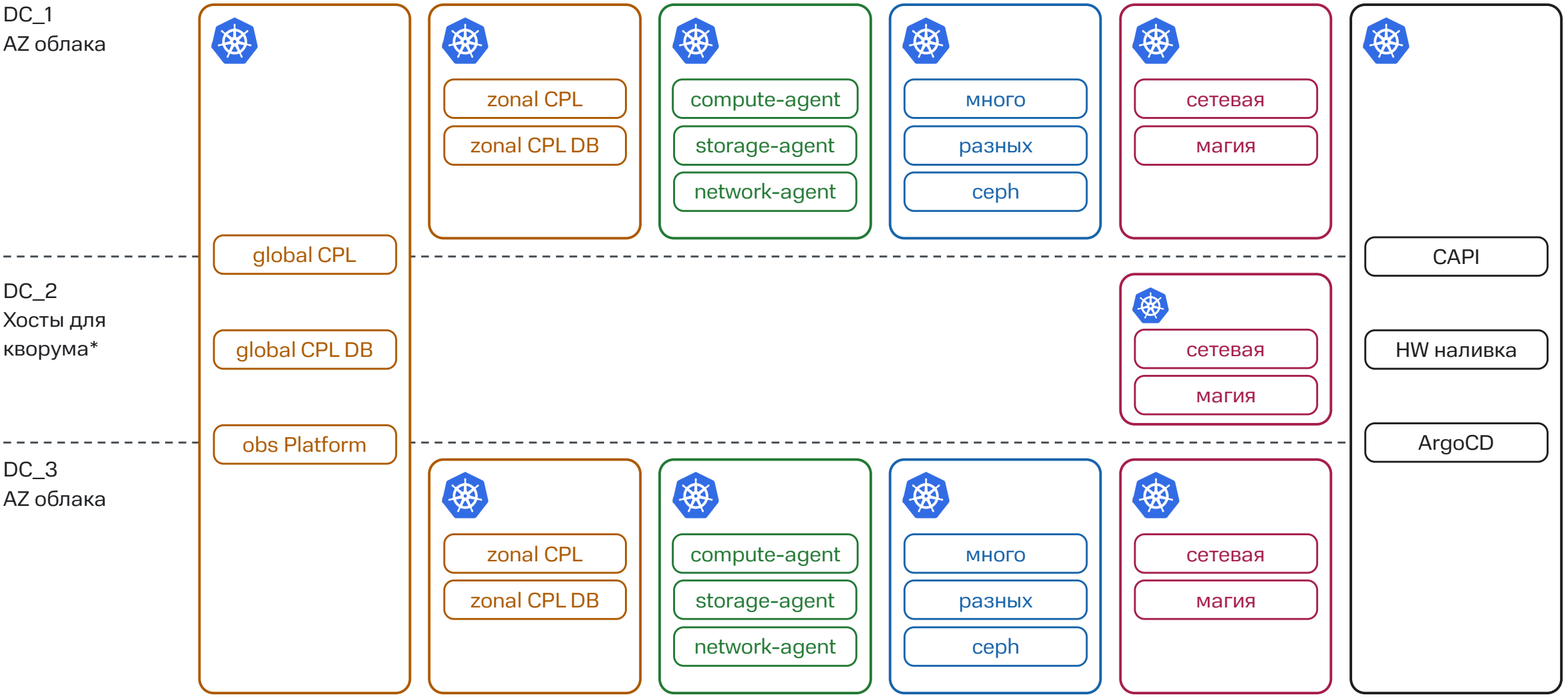
Сетевые и др. вспомогательные функции

***-mgmt**

Управление k8s (CAPI)



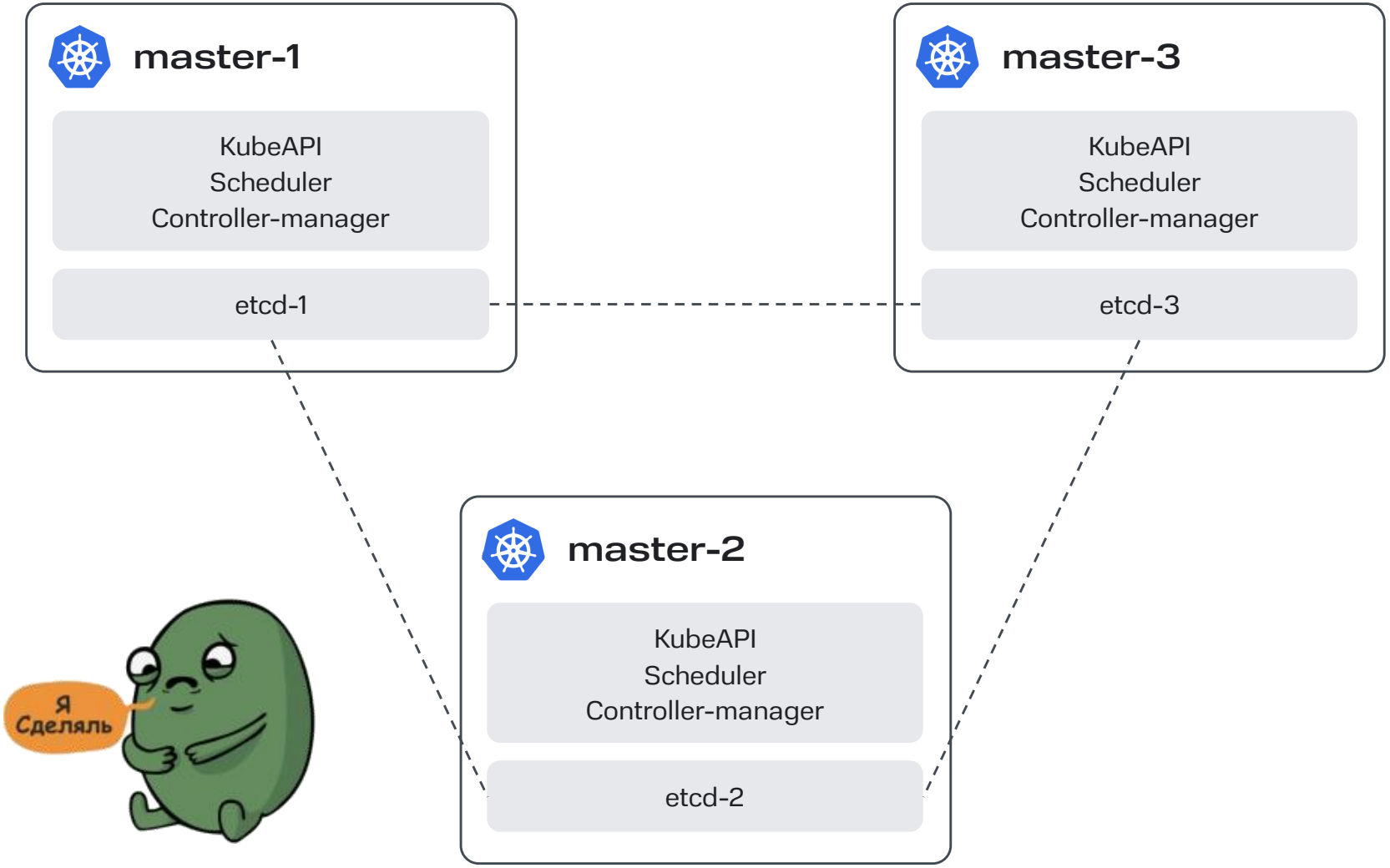
Ландшафт


DC_1
AZ облака
global CPL
global CPL DB
obs Platform
zonal CPL
zonal CPL DB
compute-agent
storage-agent
network-agent
много
разных
ceph
сетевая
магия
CAPI
HW наливка
ArgoCD
DC_2
Хосты для
кворума*
сетевая
магия
DC_3
AZ облака
zonal CPL
zonal CPL DB
compute-agent
storage-agent
network-agent
много
разных
ceph
сетевая
магия

Internal HA в k8s: наши любимые сети



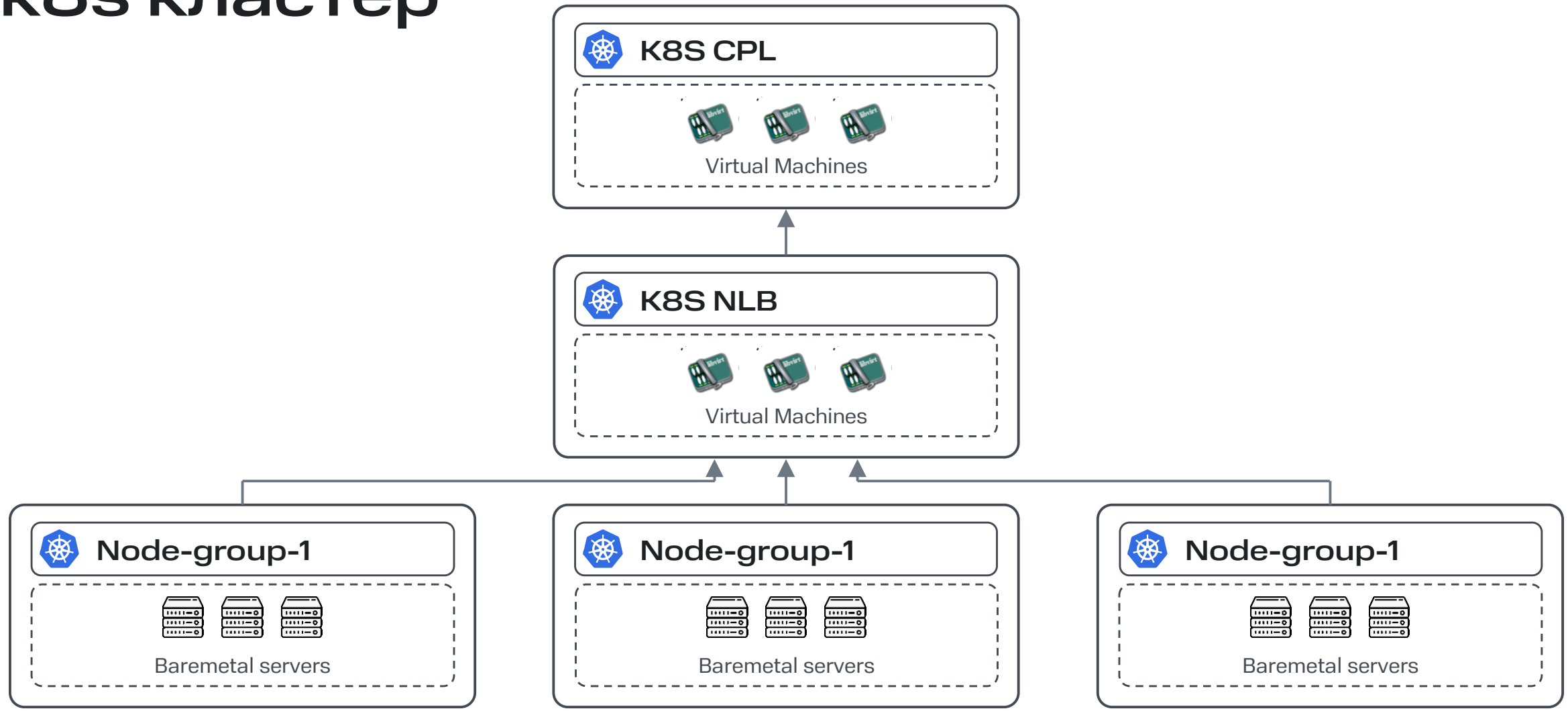
K8S HA: ожидание



K8S HA: реальность

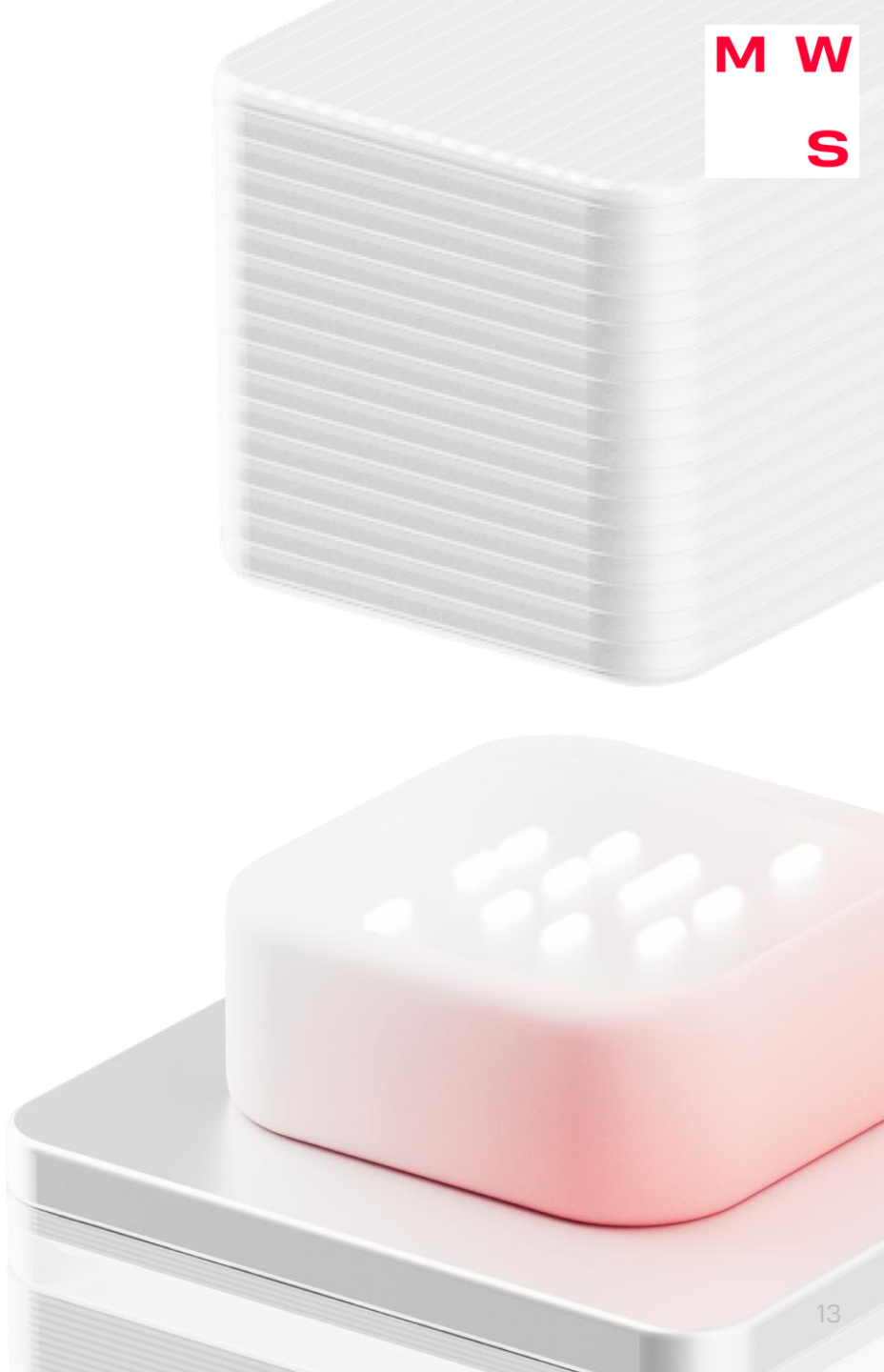


Типовой k8s кластер



Типовой k8s кластер

- Все мастера k8s запущены в виде ВМ.
- Для запуска ВМ используется ванильный libvirt + обвязка. Миграция ВМ отсутствует.
- Все NLB для kubeAPI запущены в виде отдельных ВМ.
- Воркеры – baremetal сервера с 4 сетевыми интерфейсами.



Сетевой стек в k8s

CNI

Cilium (ebpf DPL)

Kube-proxy

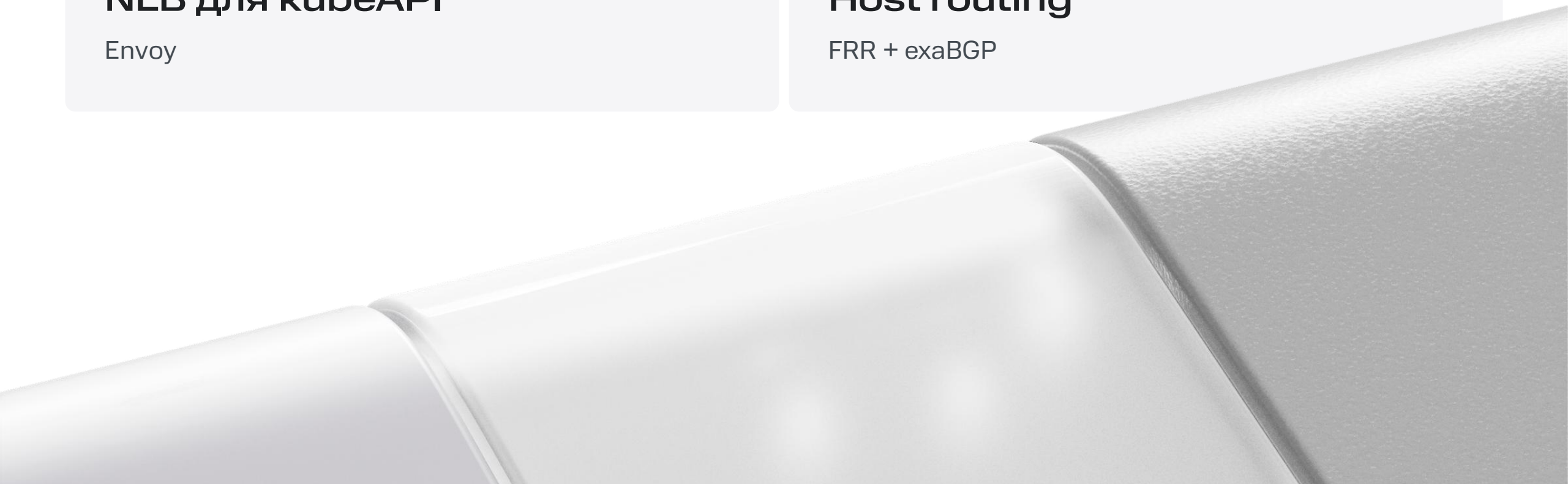
заменен cilium

NLB для kubeAPI

Envoy

Host routing

FRR + exaBGP



K8S service/pod сети и наши реализации

Pod Network

маршрутизируемый IPv6 префикс

Service ClusterIP

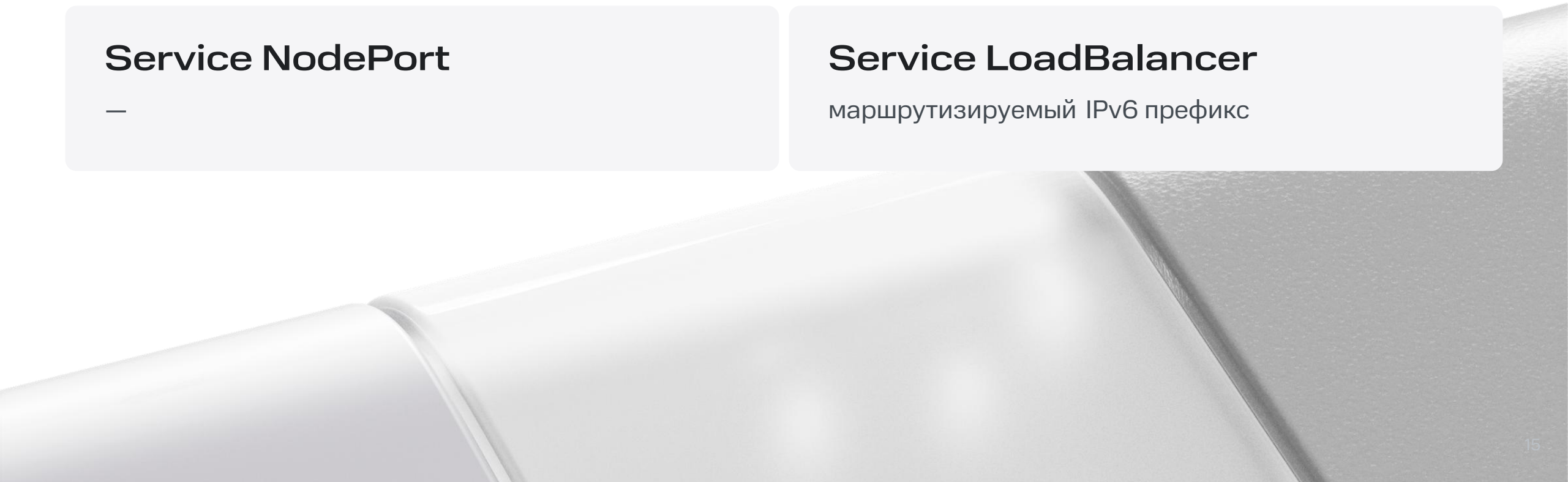
немаршрутизируемый IPv6 префикс

Service NodePort

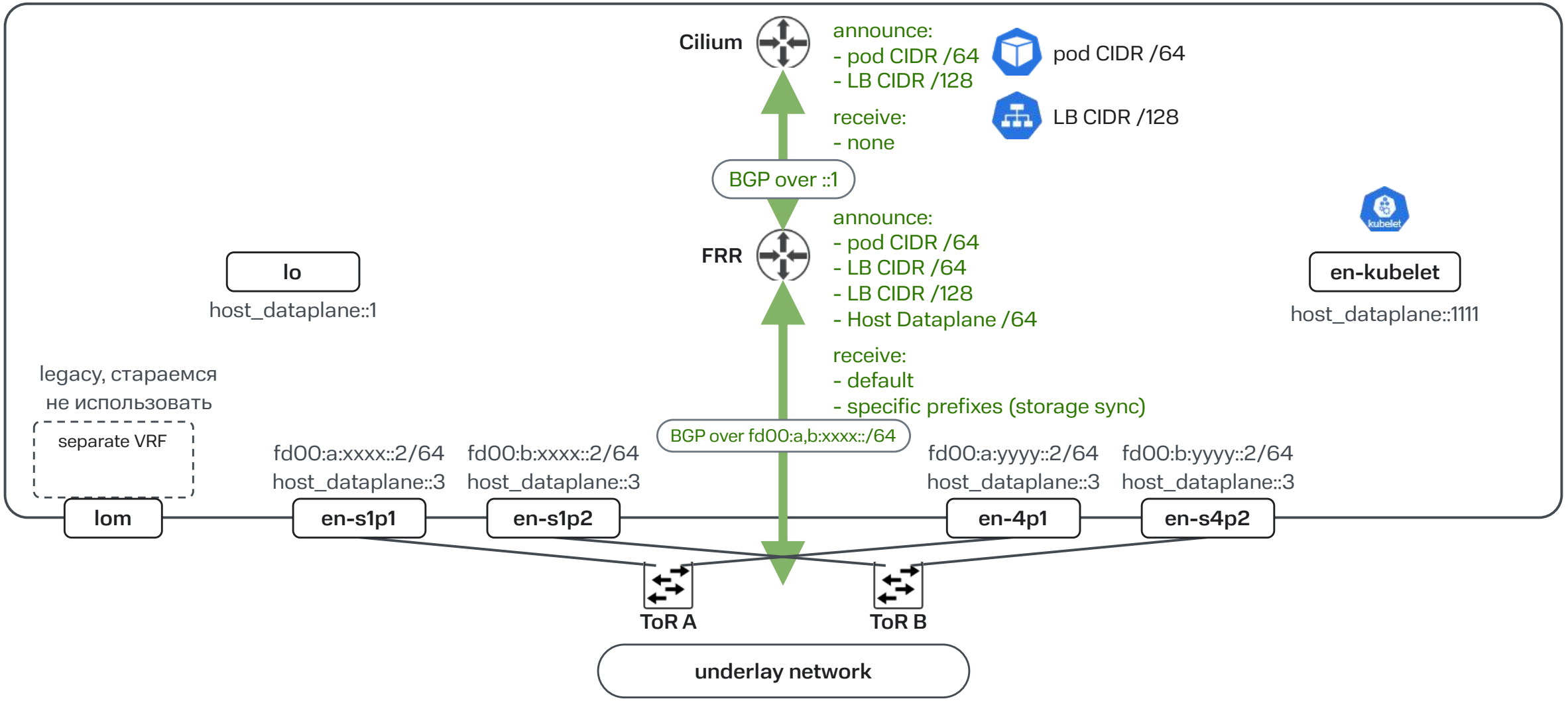
—

Service LoadBalancer

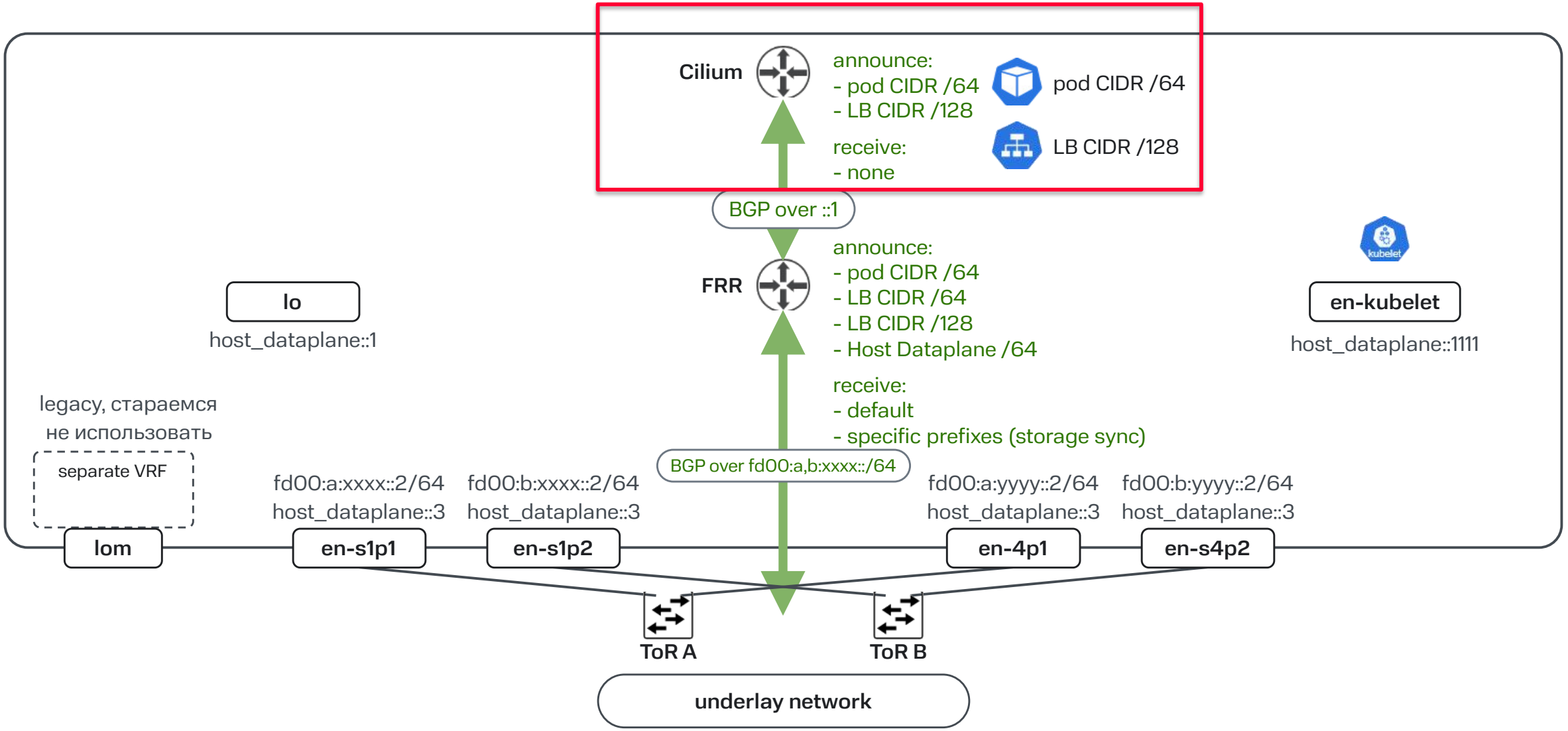
маршрутизируемый IPv6 префикс



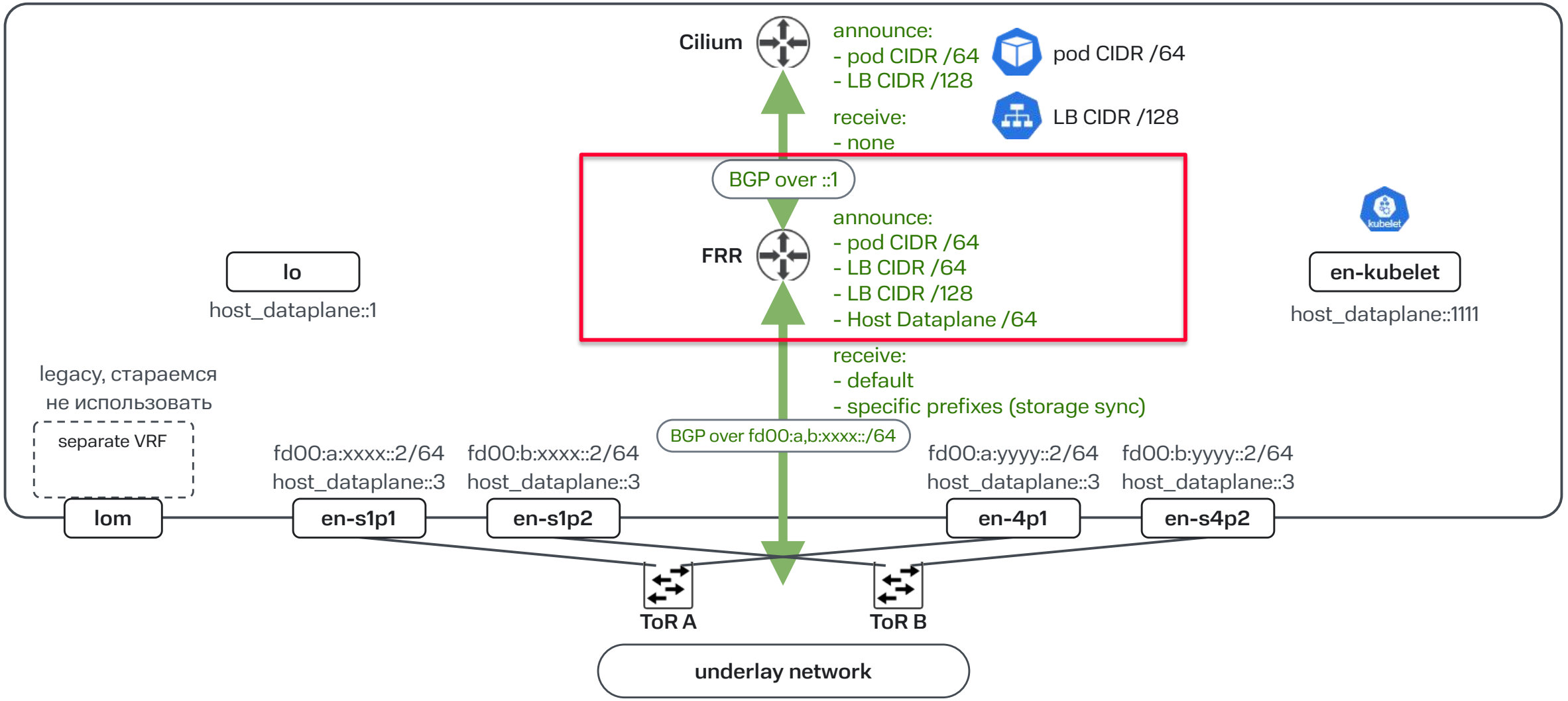
Устройство хостовой и подовой сети



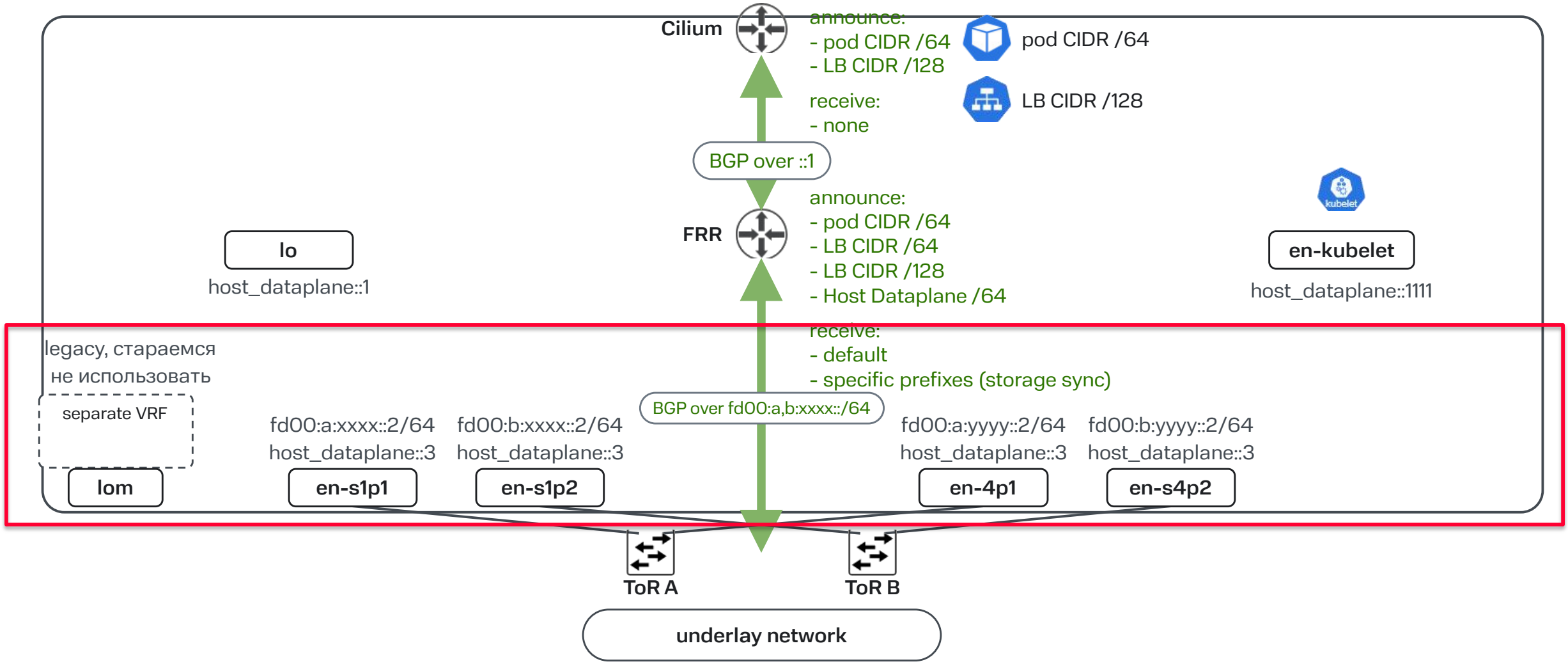
Устройство хостовой и подовой сети



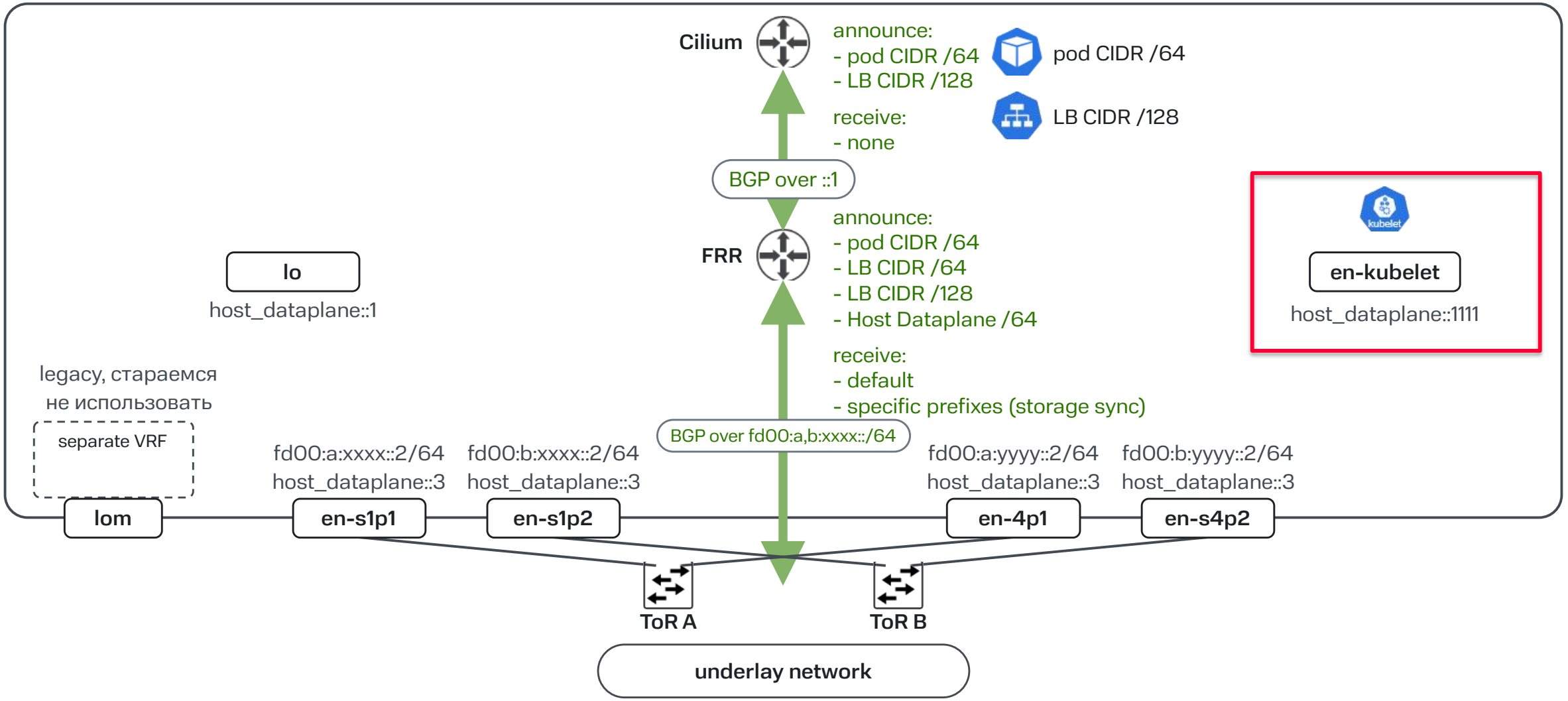
Устройство хостовой и подовой сети



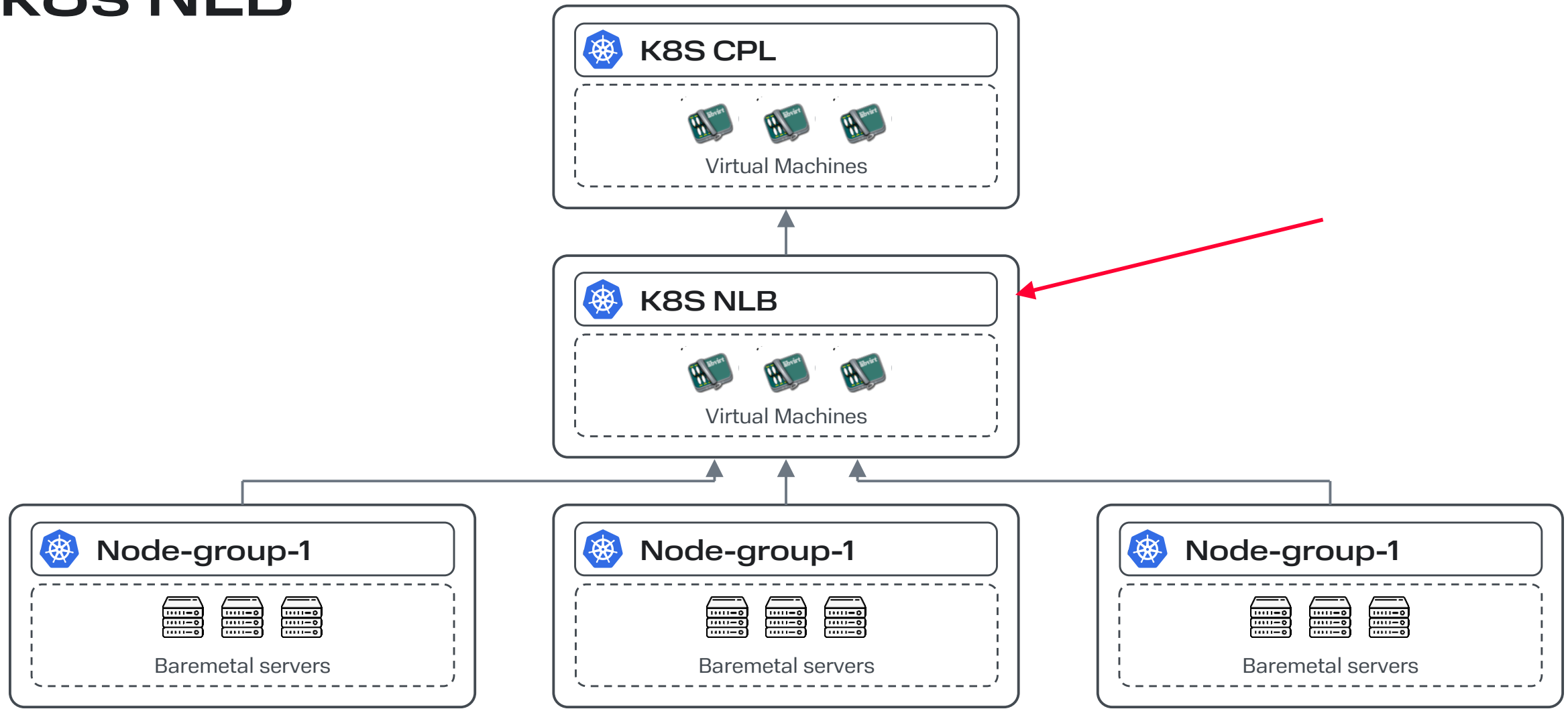
Устройство хостовой и подовой сети



Устройство хостовой и подовой сети



Зачем нужен k8s NLB



Зачем нужен k8s NLB

01

Балансировка подключений внешних клиентов

kubectl

02

Балансировка подключений вида

worker -> master (kubelet)

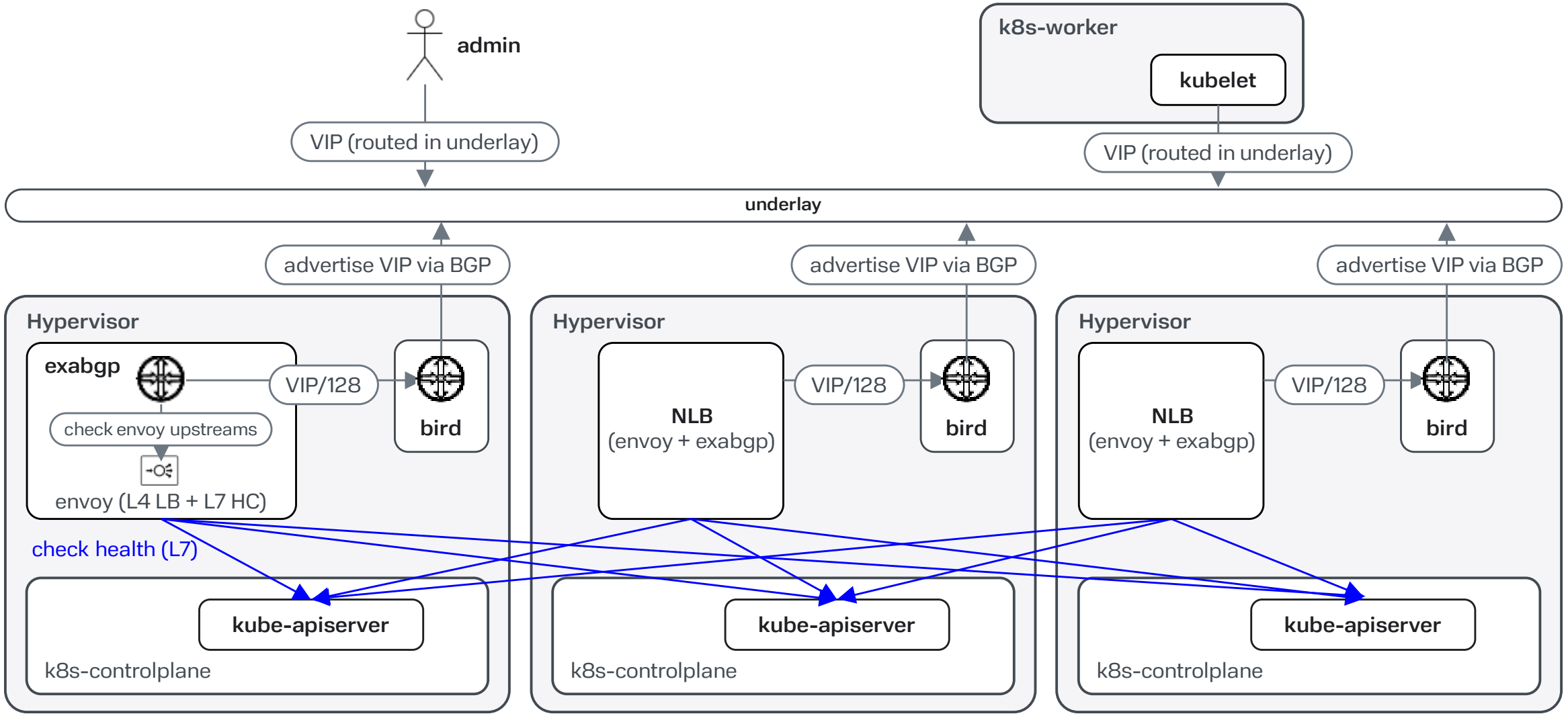
03

Балансировка k8s service сети

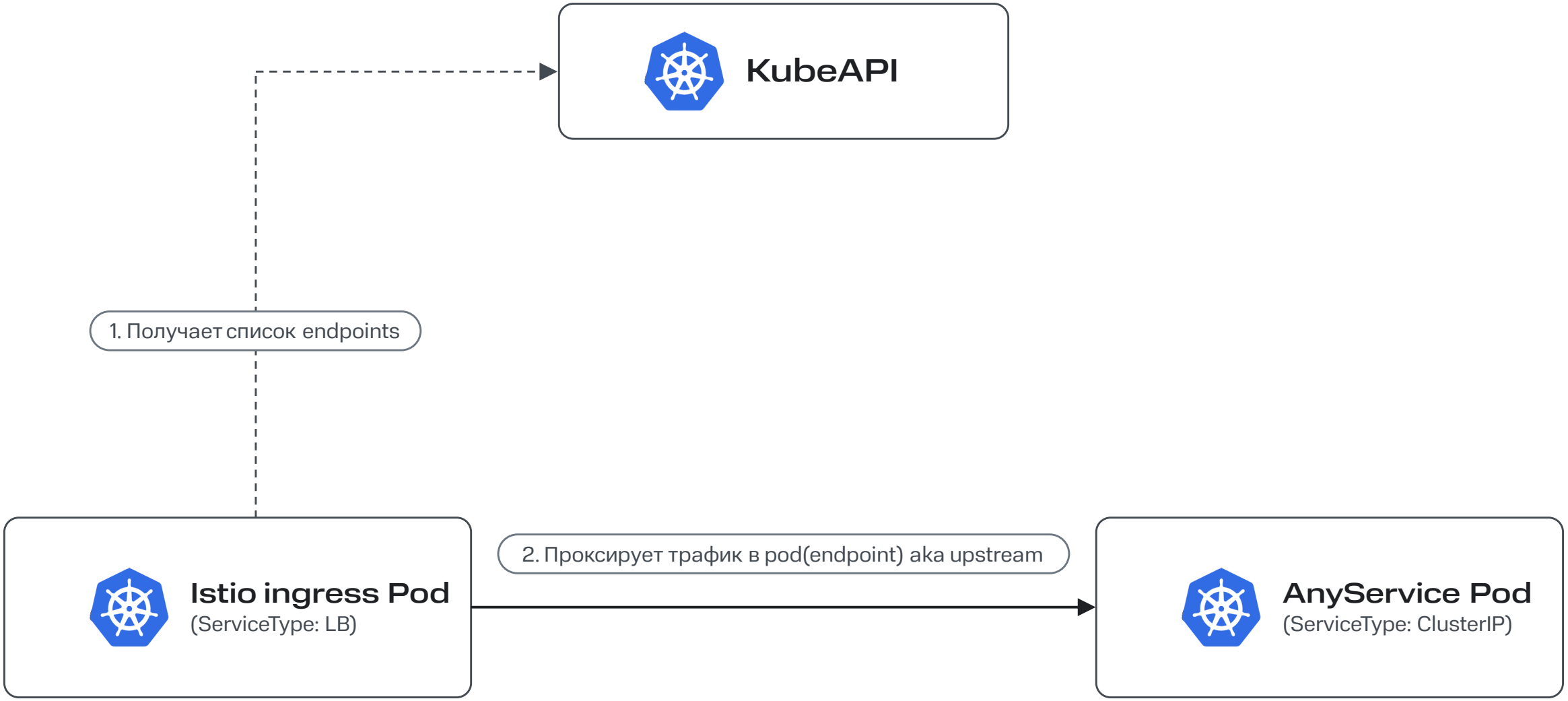
type: ClusterIP



Устройство k8s NLB



Istio ingress



Cilium endpoint

01

Сетевая конфигурация

02

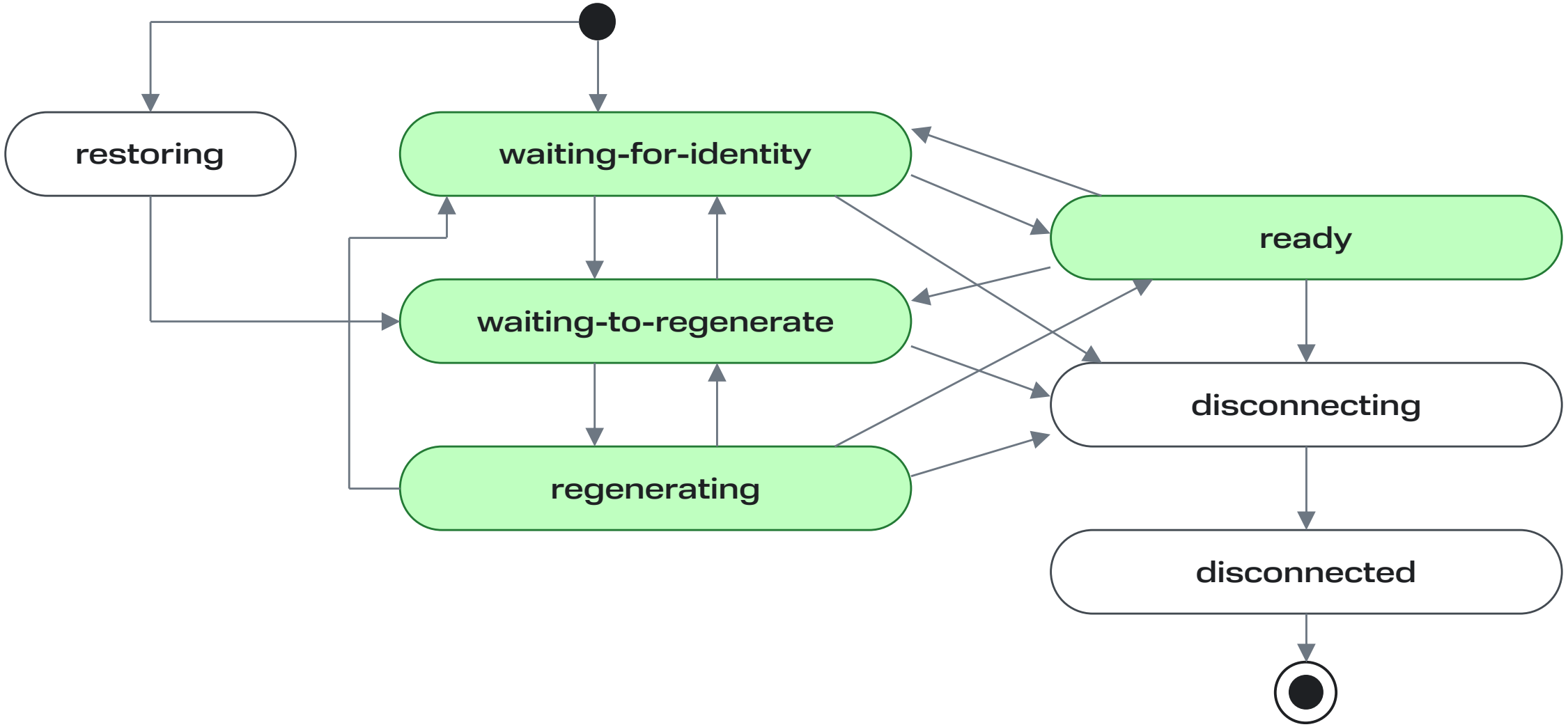
Network policies

03

Метадата



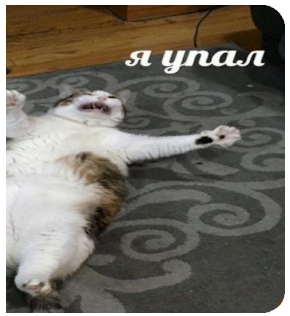
Cilium endpoint

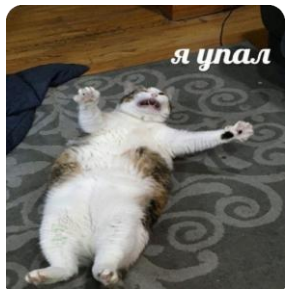


DC_1
AZ облака

DC_2
Хосты для кворума*

DC_3
AZ облака







zonal CPL
zonal CPL DB

compute-agent
storage-agent
network-agent

много
разных
ceph

сетевая
магия

сетевая
магия

zonal CPL
zonal CPL DB

compute-agent
storage-agent
network-agent

много
разных
ceph

сетевая
магия

CAPI

HW наливка

ArgoCD

RSS Консоль

← Инциденты

Недоступность сервисов облака

Уровень влияния	Критичный
Сервисы	Compute, VPC, Certificate Manager, Artifact Registry, Managed Kubernetes, IAM
Начало	12.12.2025, 10:25 (МСК)
Завершение	12.12.2025, 10:40 (МСК)

История событий

12.12.2025, 10:25 (МСК)
Обнаружен

Обнаружена недоступность управляющих сервисов облака. Работоспособность виртуальных машин не нарушена. Команда работает над устранением неполадки.

12.12.2025, 10:40 (МСК)
Решён

Проблема устранена

Инцидент 1: отказ kube API NLB

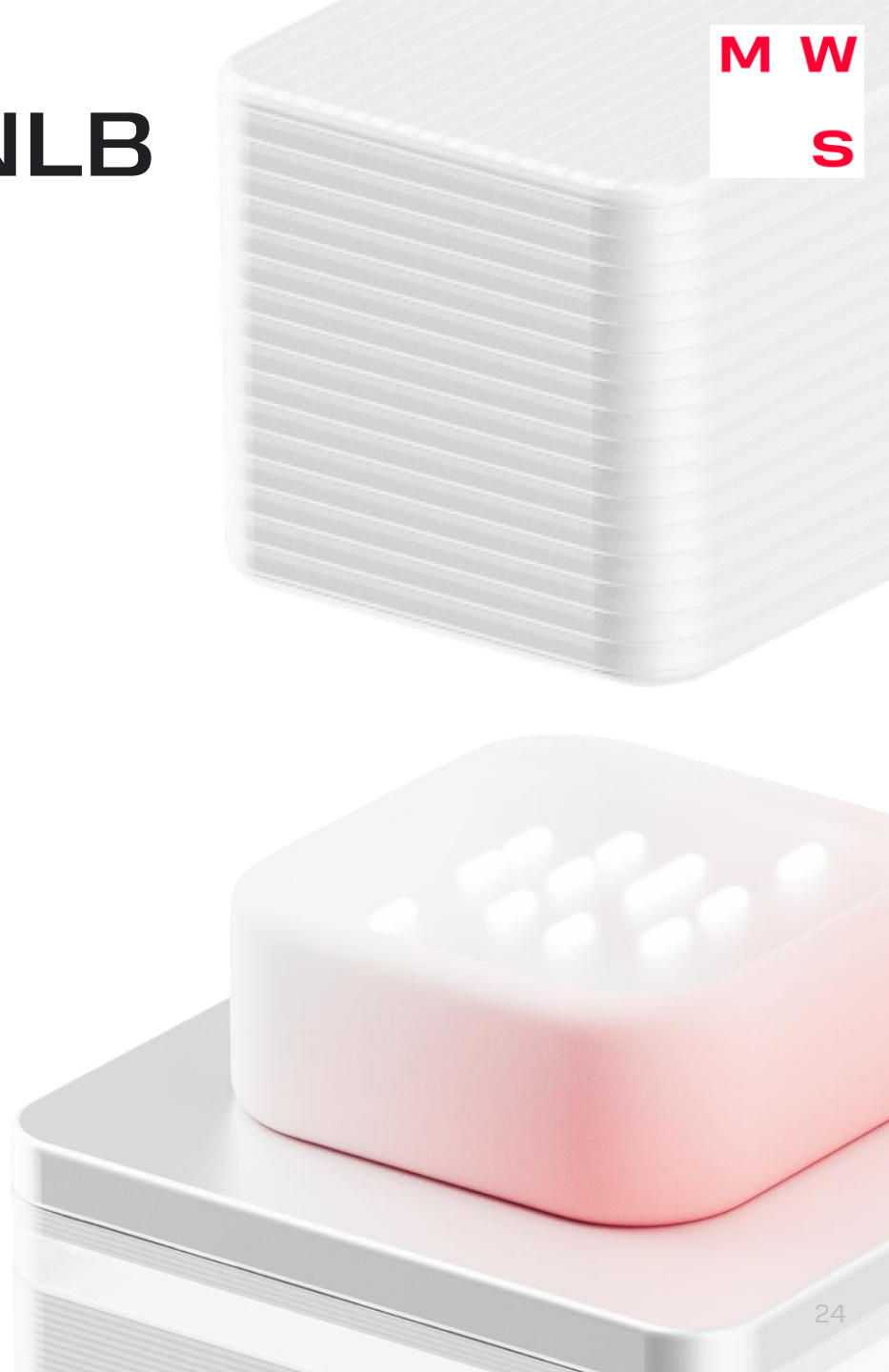
Что задело:

01 Cilium-agent (хелсчеки)

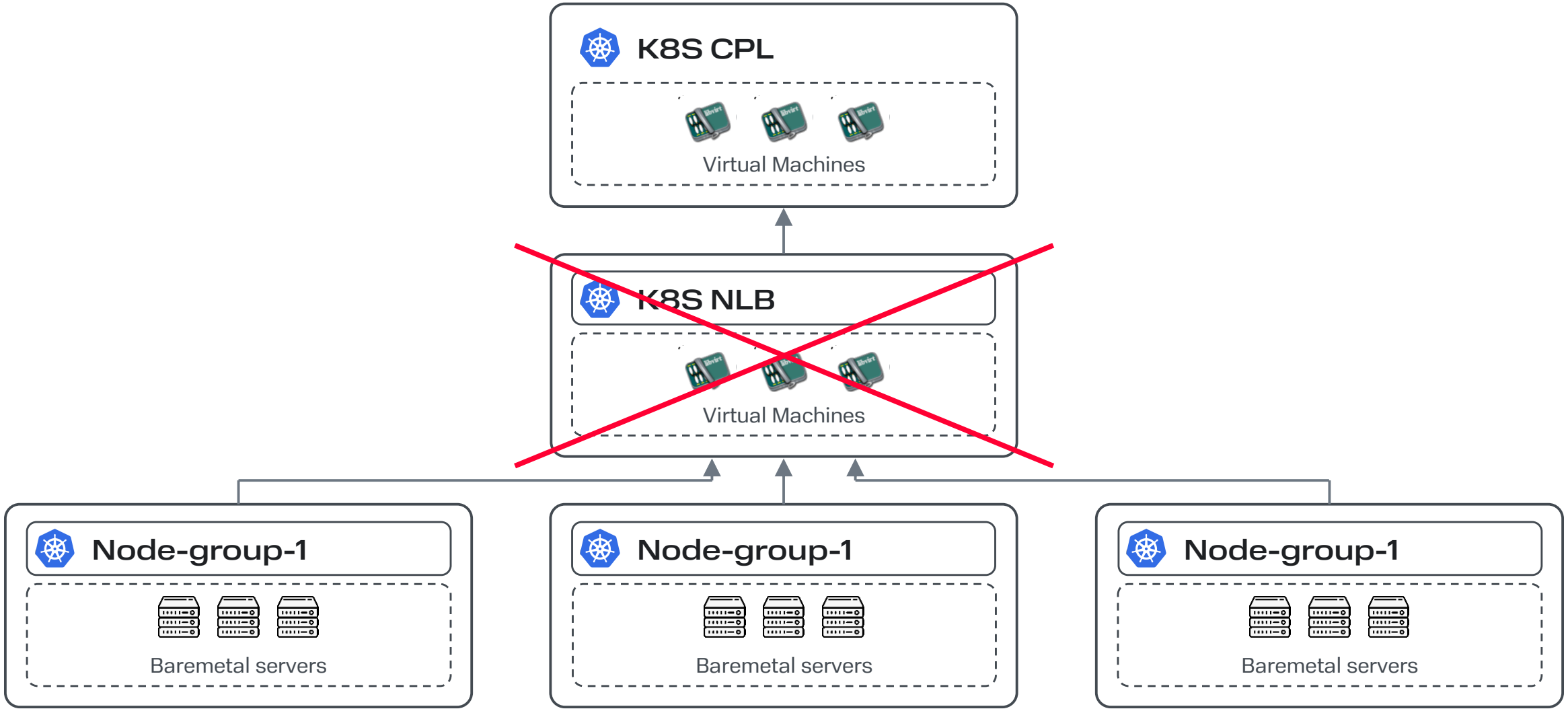
02 NotReady у k8s нод

03 Сервисы за ingress

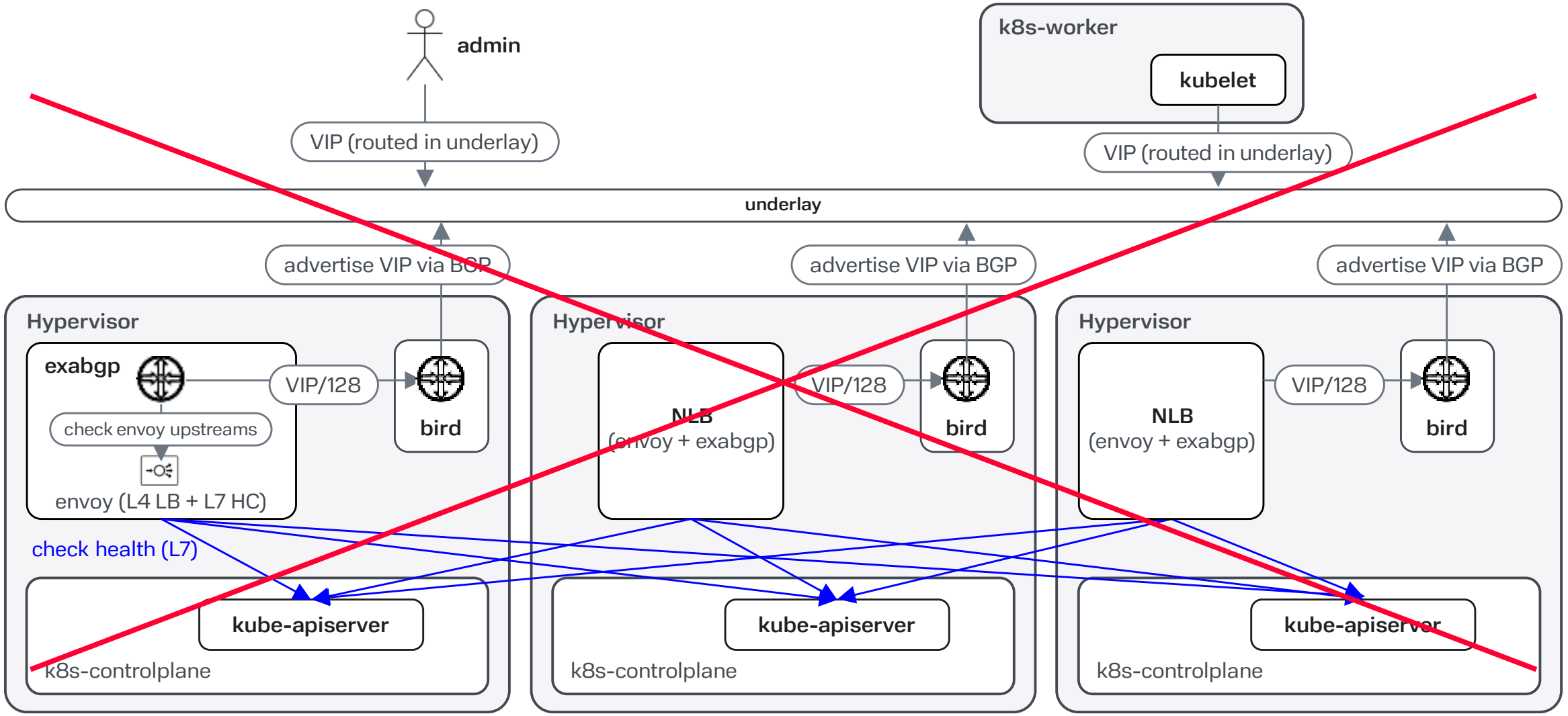
04 Сервисы под customEndpointOperator



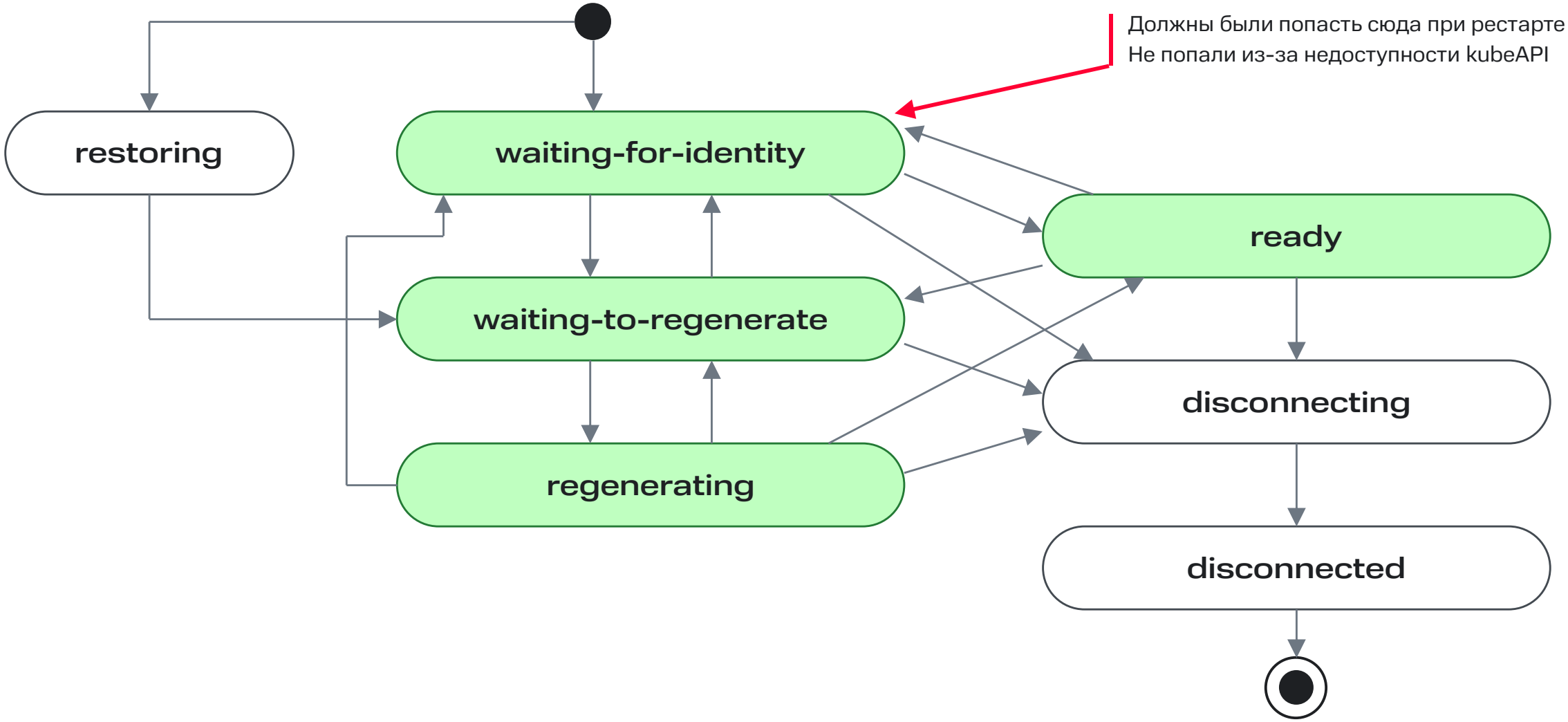
Случайно «положили» все 3 LB :)



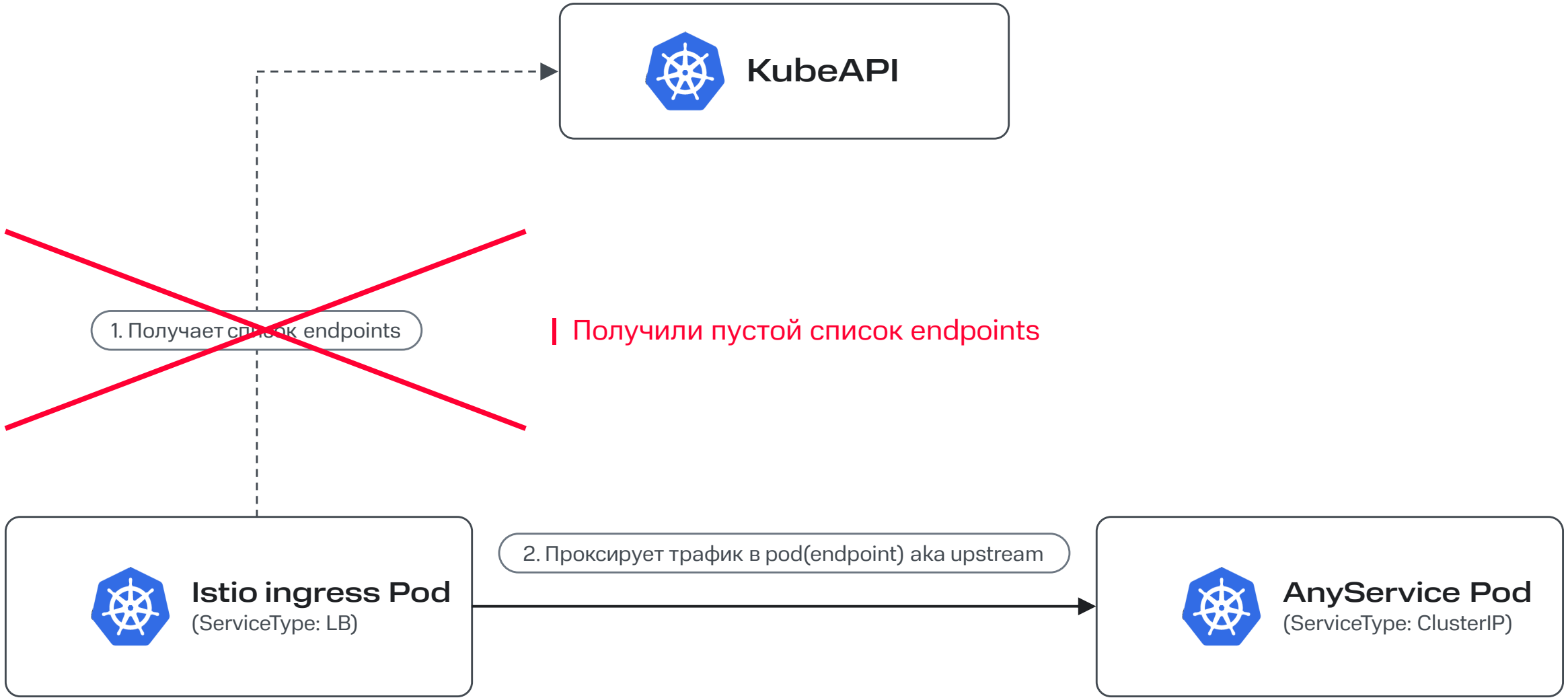
Kubelet'ы не доходят до kubeAPI -> NotReady



Рестарты по ХЧ cilium agents



Istio ingress: 503 UH

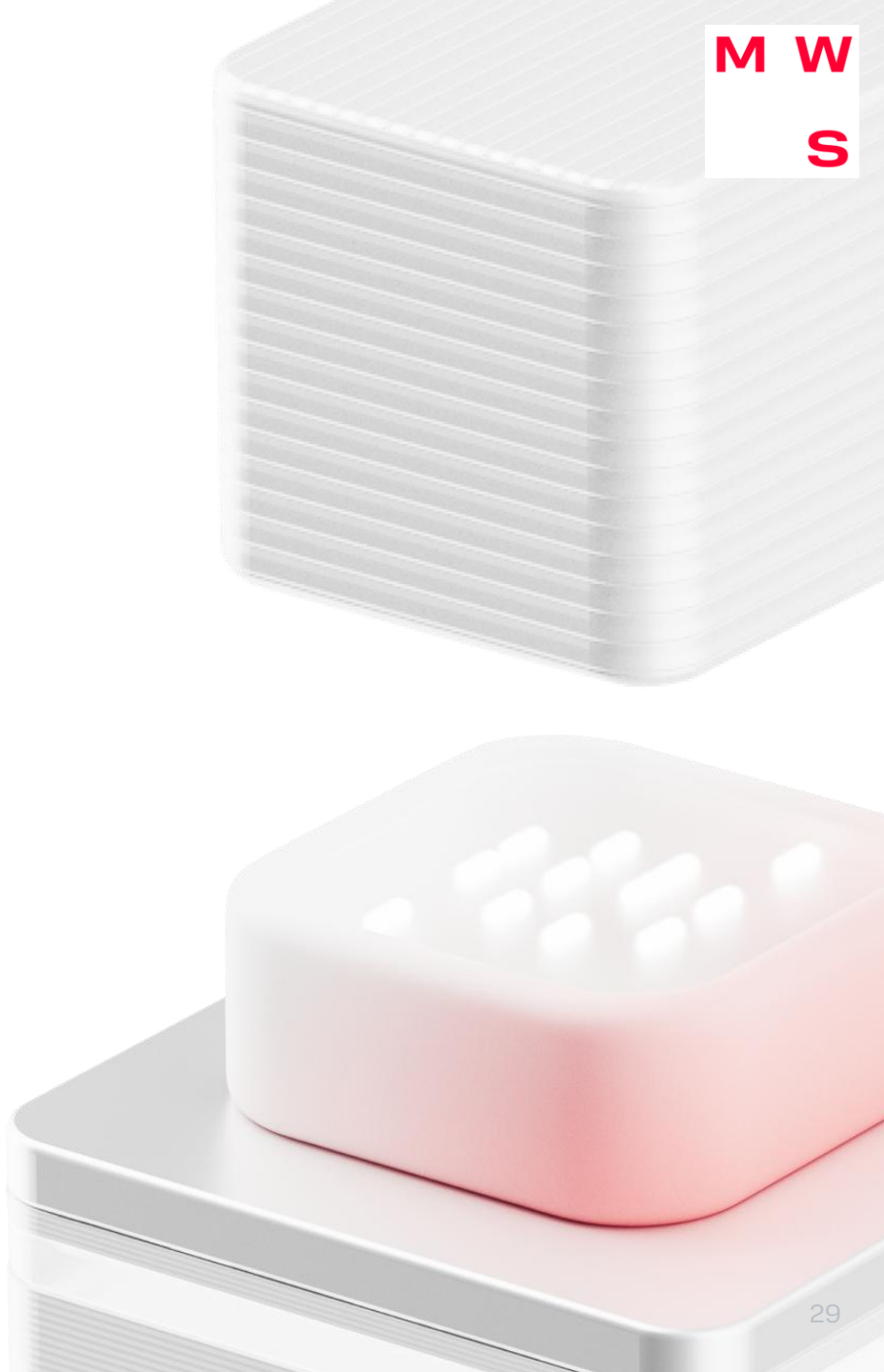


Istio ingress: 503 UH

- Kubernetes.default.svc – адреса
3 мастеров, а не VIP NLB

- Сетевая связность
от istio до мастеров есть

- Все воркер ноды NotReady =
пустые endpoints для всех clusterIP

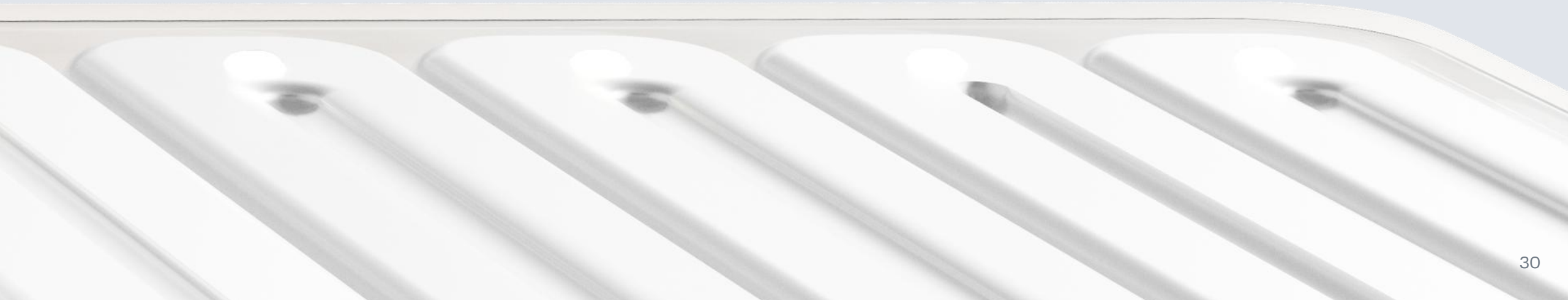


Что мы вынесли из инца

01 Починили мониторинг

02 Отключили хелсчеки cilium-agent

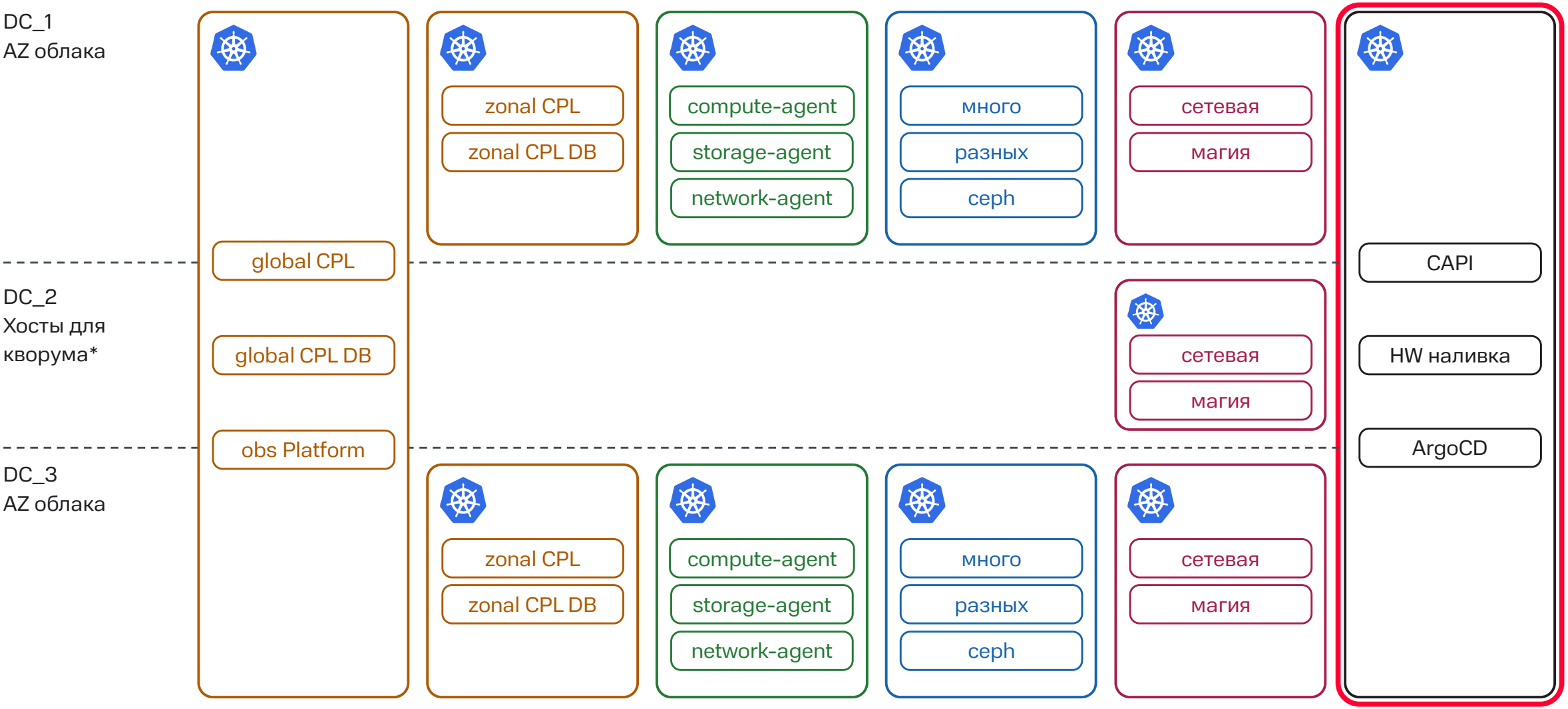
03 Kubernetes.default.svc теперь тоже за VIP



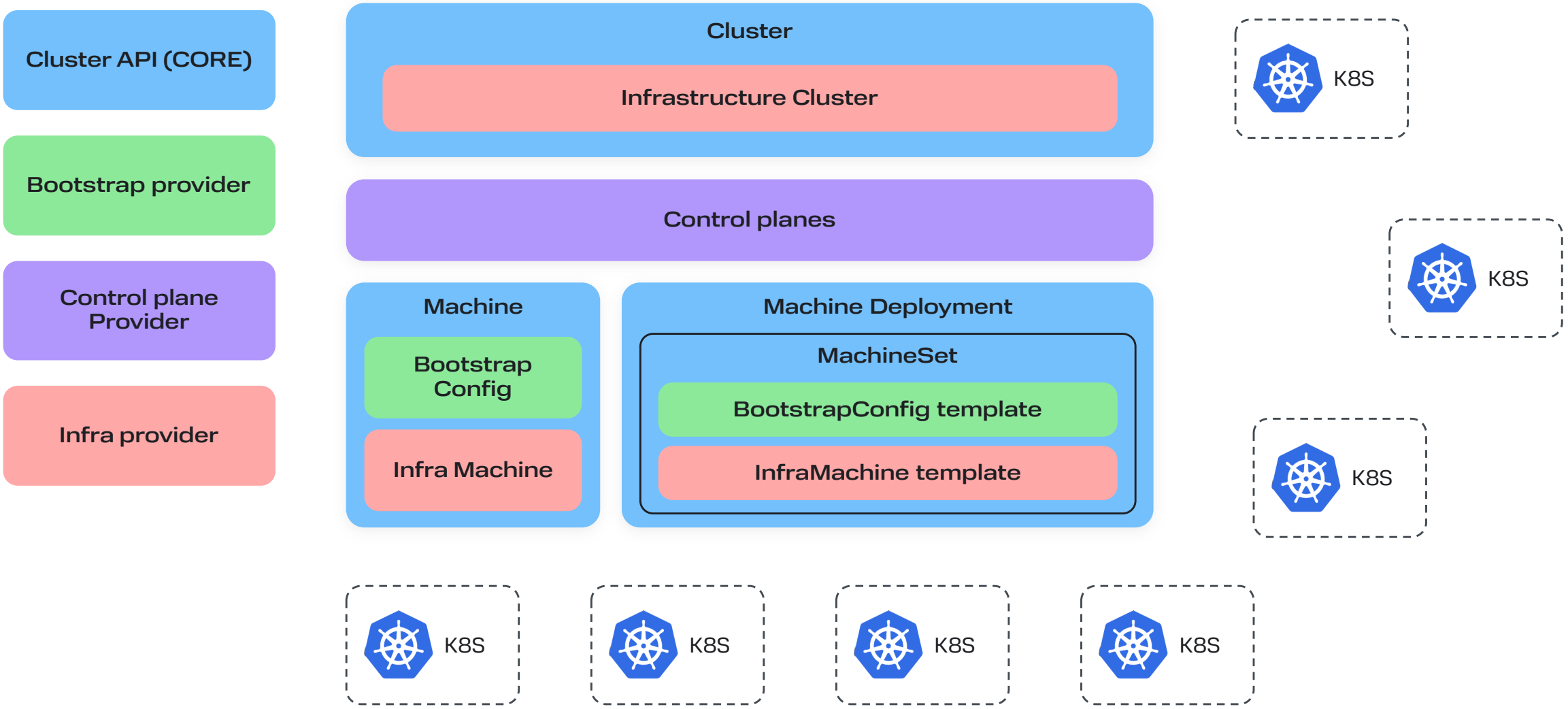
External HA в k8s: сумасшедшая автоматика



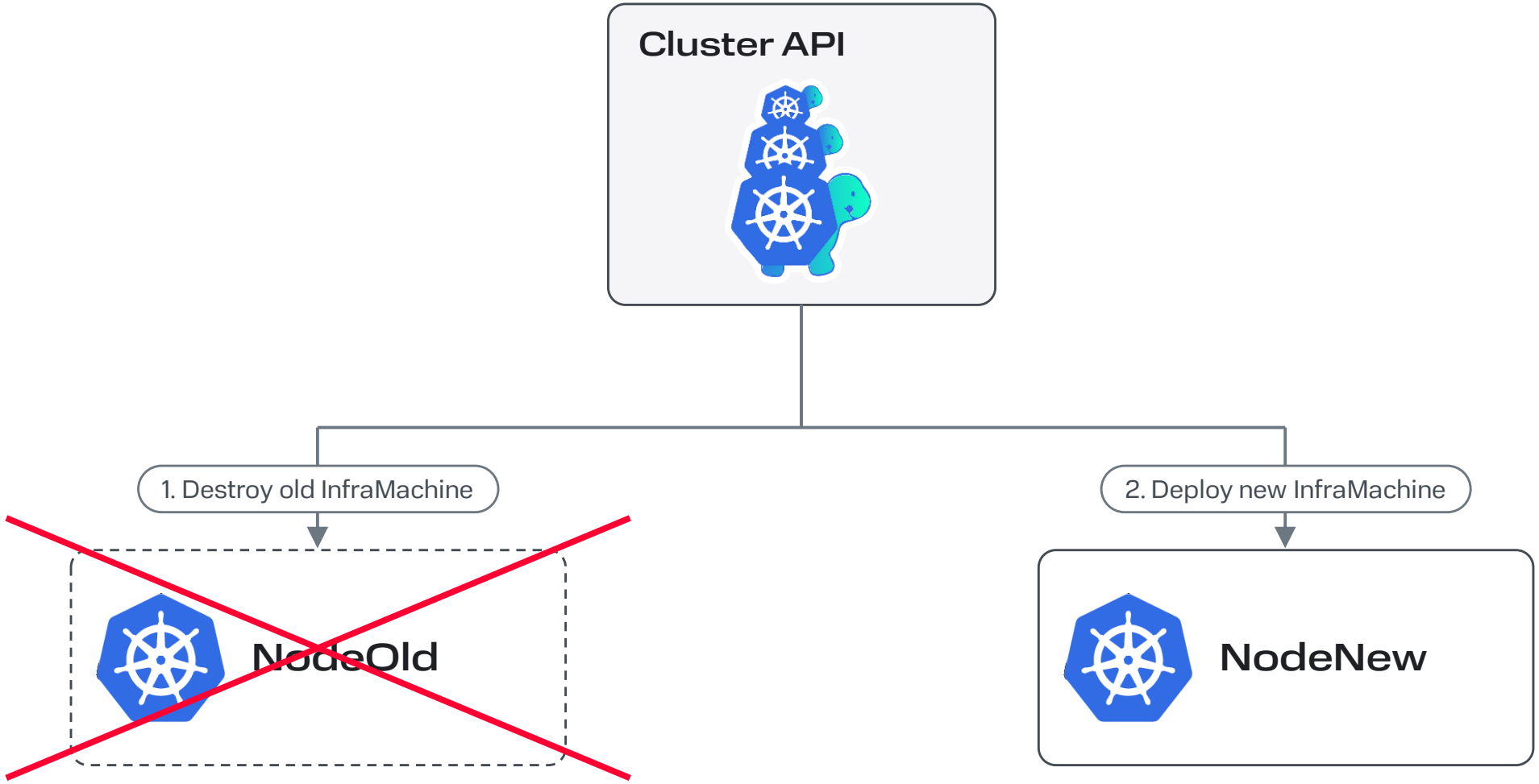
Управление парком кластеров



Cluster API

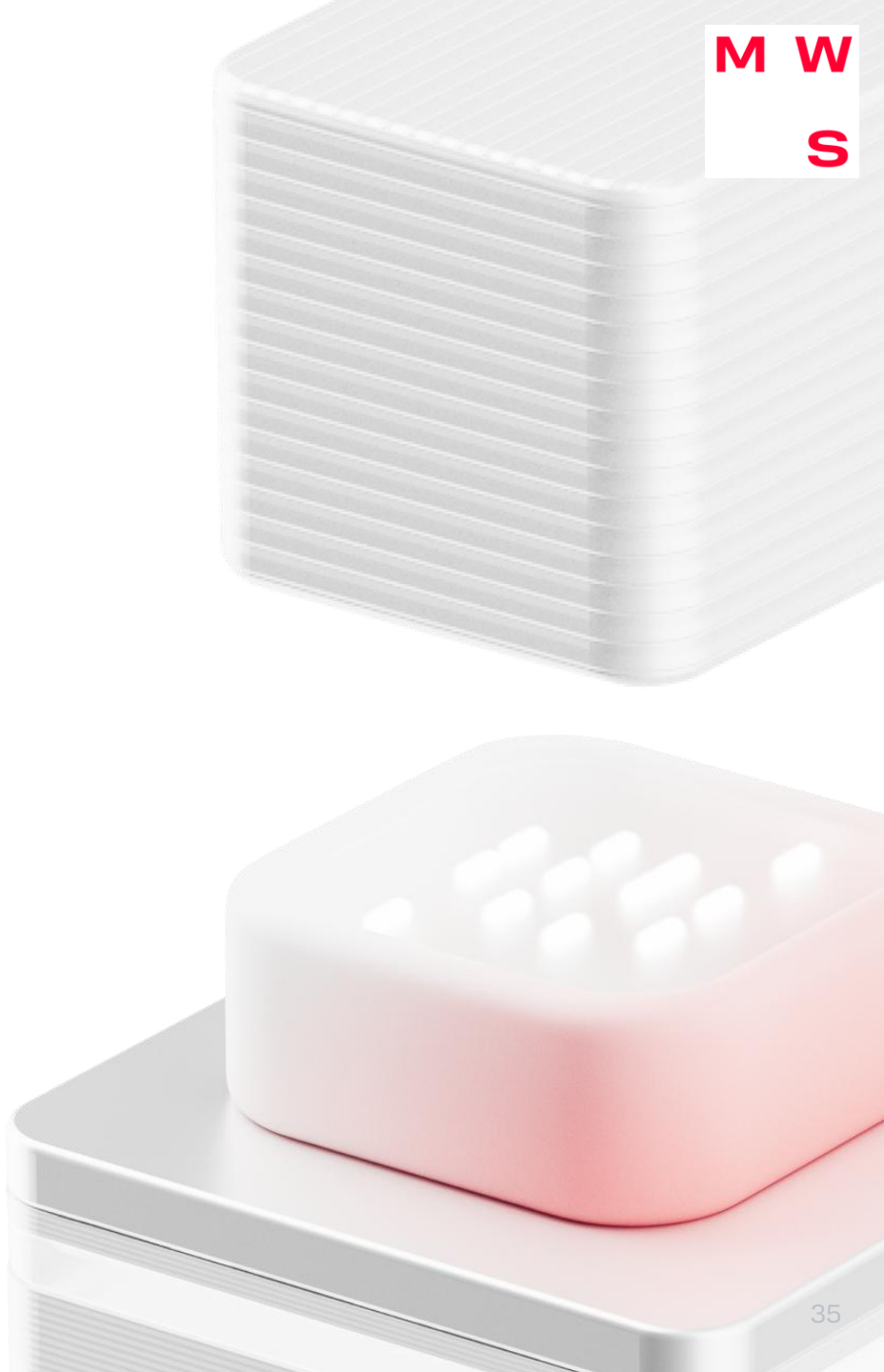

Cluster API (CORE)
Bootstrap provider
Control plane Provider
Infra provider
Cluster
Infrastructure Cluster
Control planes
Machine
Bootstrap Config
Infra Machine
Machine Deployment
MachineSet
BootstrapConfig template
InfraMachine template
K8S
K8S
K8S
K8S
K8S
K8S
K8S

Как ClusterApi обновляет дочерние k8s



От чего нужно защищаться

- Удаление ресурса Node в дочернем k8s
- Удаление контрольных ресурсов CAPI в mgmt. Кластере
- Переналивка самого хоста -_-



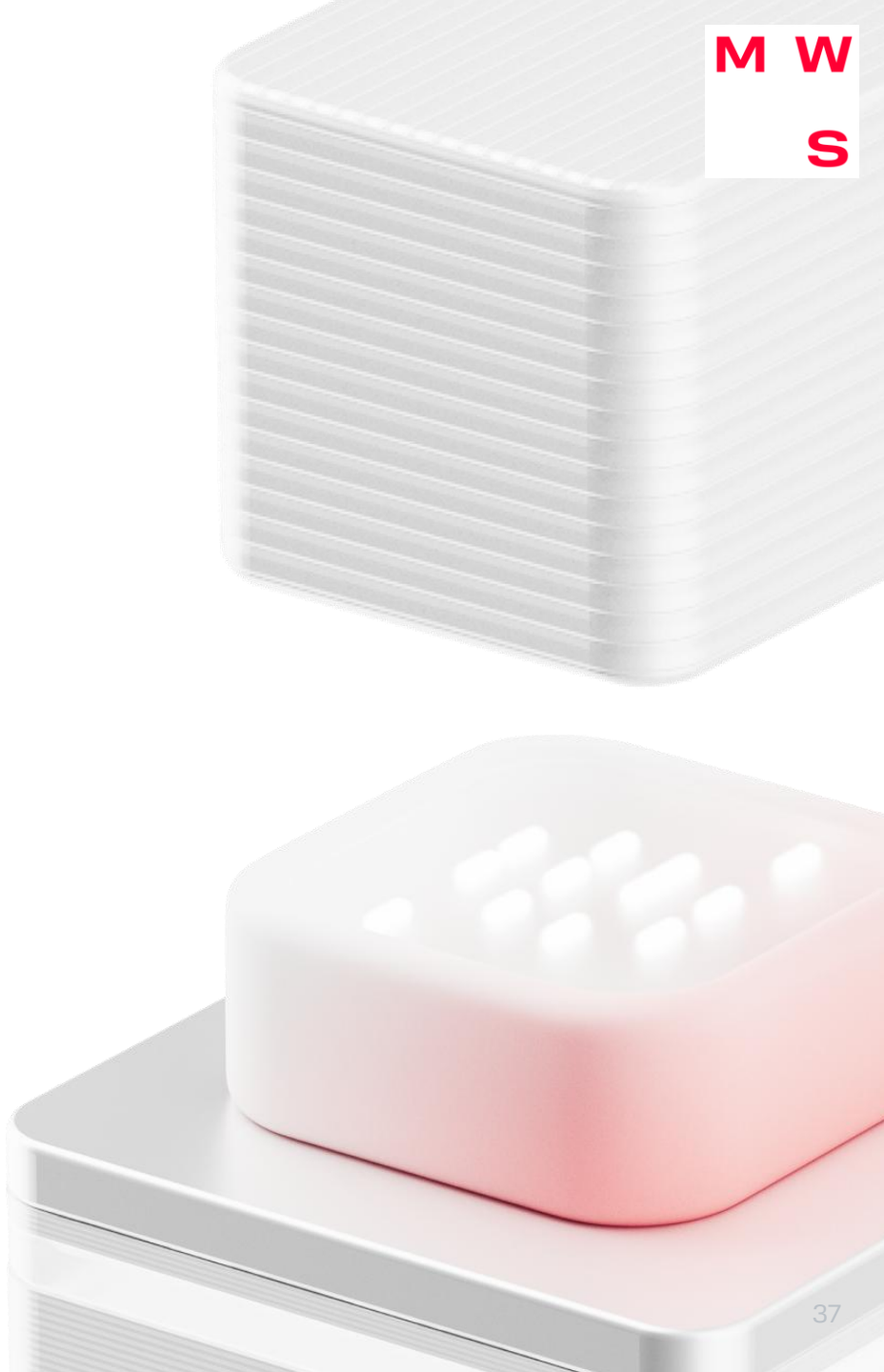
Защита удаления ресурса Node: Kyverno

block-node-deletion.yaml

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: block-node-deletion
spec:
  background: false
  rules:
    - name: require-annotation-to-delete-node
      skipBackgroundRequests: true
      match:
        resources:
          kinds: ["Node"]
          operations: ["DELETE"]
      validate:
        allowExistingViolations: true
        failureAction: Enforce
        message: Deleting a Nodes is forbidden unless it has annotation iReallyWantDeleteThis == true.
        deny:
          conditions:
            - key: "{{ request.oldObject.metadata.annotations.iReallyWantDeleteThis || 'false'}}"
              operator: NotEquals
              value: "true"
```

Защита удаления ресурсов CAPI: что защищаем

- Machine Deployment && Machines
- Ресурсы infra provider (свой кастом)
- Подконтрольные CAPI ресурсы системы наливки VOLK



Защита удаления ресурсов CAPI: custom webhooks

01

Удаление/модификация ресурсов невозможно без аннотации на поде с webhook

02

Аннотация отрабатывает однократно! После обработки запроса webhook сам снимает аннотацию с себя.



DC_1
AZ облака

DC_2
Хосты для
кворума*

DC_3
AZ облака

global CPL

global CPL DB

obs Platform

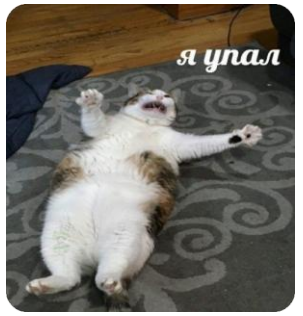
zonal CPL

zonal CPL DB

compute-agent

storage-agent

network-agent



сетевая

магия

сетевая

магия

CAPI

HW наливка

ArgoCD

zonal CPL

zonal CPL DB

compute-agent

storage-agent

network-agent

много

разных

ceph

сетевая

магия

Инцидент 2: ноды storage кластера ушли в переналивку

Что задело:

01

Несколько worker нод кластера

02

Машины не успели переналиться и застряли в live-cd



Инцидент 2: TLDR что случилось?

01

Непредвиденный rollout ресурсов был несколько месяцев заблокирован на webhook

02

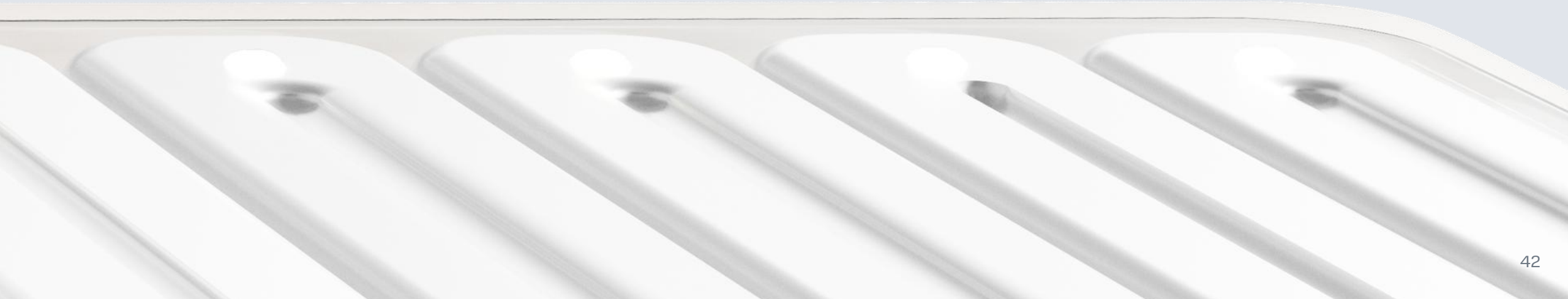
В ходе плановых работ и аннотирования пода случайно его разблокировали



Что мы вынесли из инца

01 Стали более внимательно обновлять ядро CAPI

02 Начали писать свою реализацию контроллера для Machine*

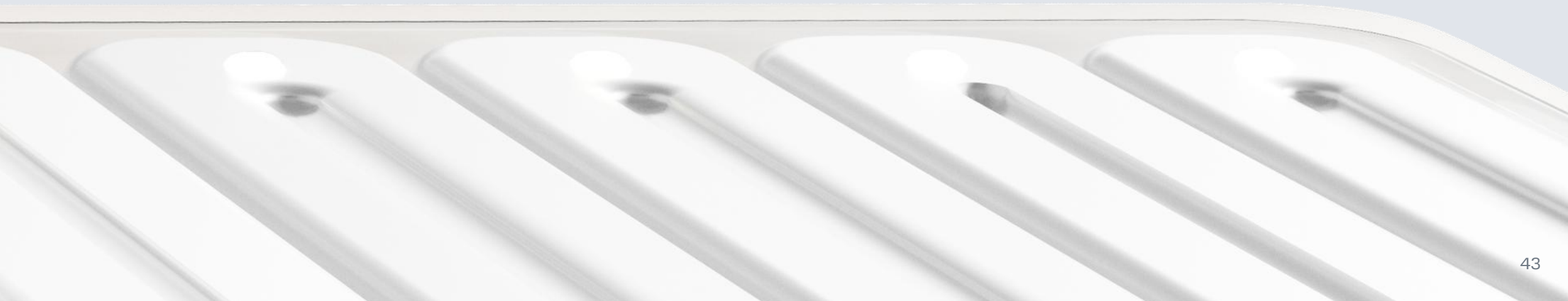


Выводы

01 Стремитесь к полностью автономному DPL k8s

02 Не используйте асинхронные пути для internal и external трафика k8s

03 Не доверяйте своей автоматике и стройте заборы



СПАСИБО ЗА ВНИМАНИЕ

@KEPIUKIK



Иван Гулаков

https://t.me/kepiukik

