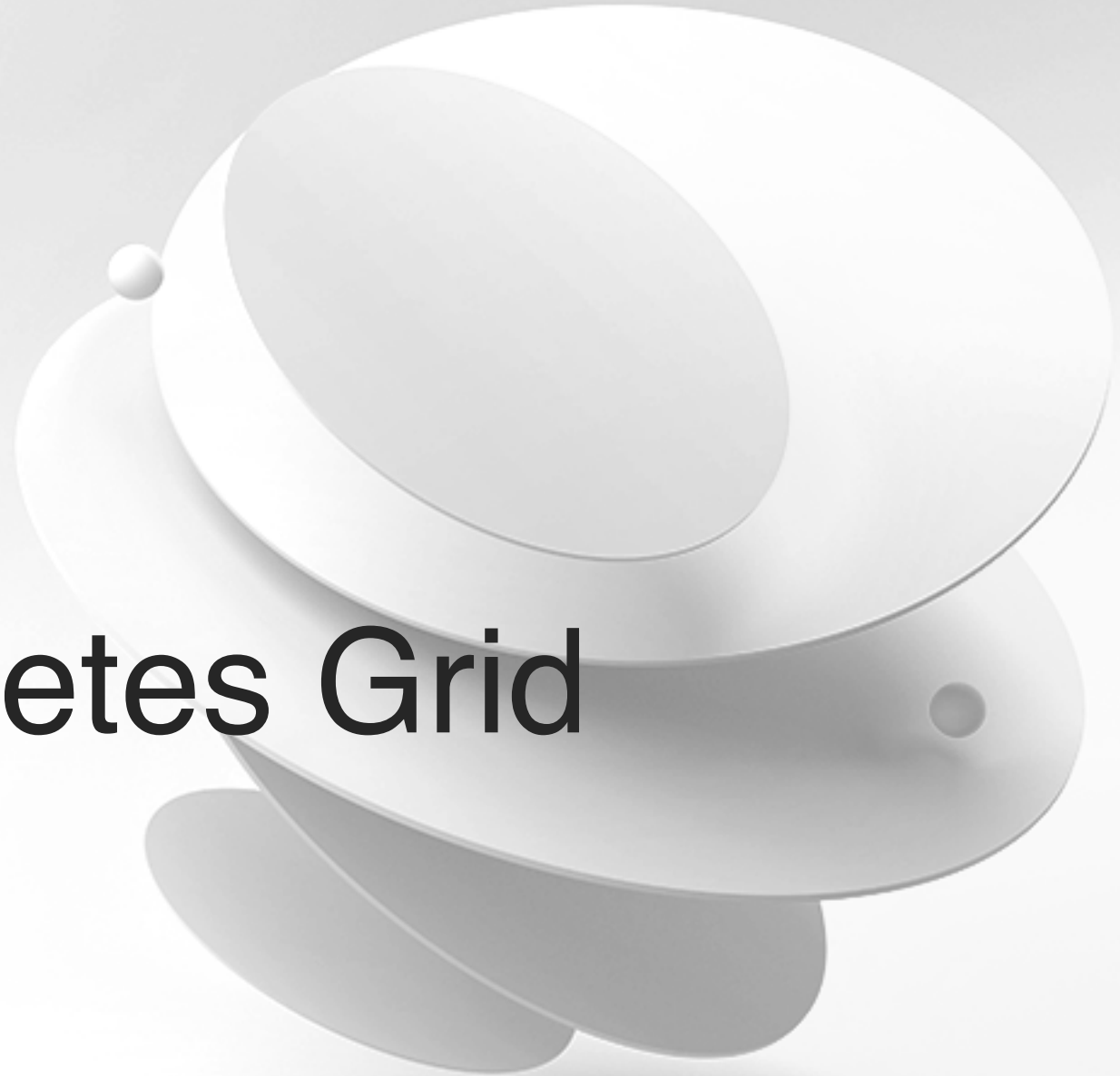
Hilbert Team



Tanzu Kubernetes Grid

Алексей Цыкунов
Co-founder & CTO at Hilbert Team

Hilbert Team

Глобальный системный интегратор, который помогает компаниям по всему миру увеличивать операционную эффективность и маржинальность бизнеса за счет миграции в облако, автоматизации IT-инфраструктуры и процессов.

Более 30 экспертов в области Cloud, DevOps, DevSecOps, DataOps и MLOps

Сертифицированный партнёр Yandex Cloud

Обучаем DevOps-инженеров в топ-10 банках РФ с 2018 года

Hilbert Team

Обзор решения

Bootstrap и Tanzu CLI

Управление кластерами

Типы кластеров

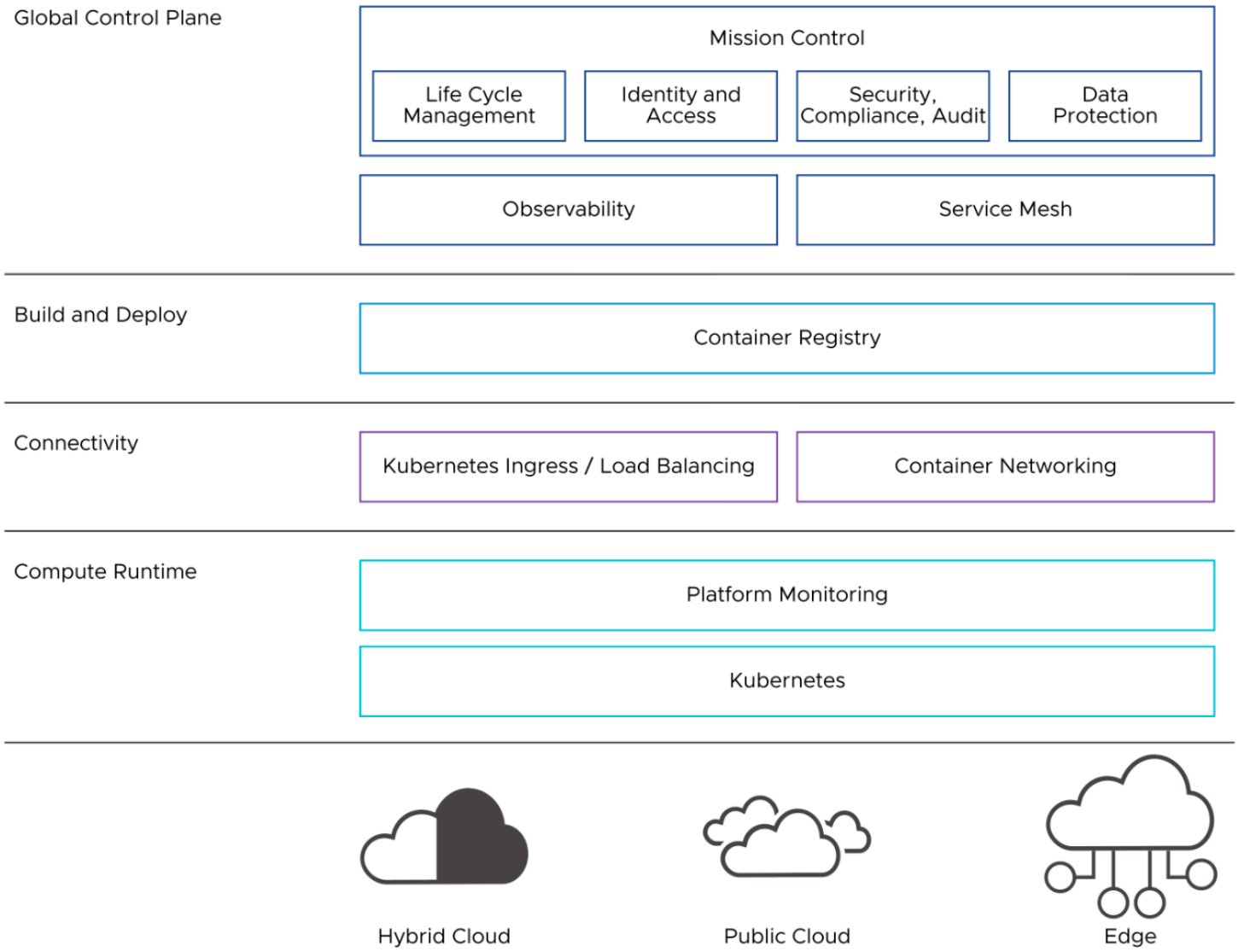
Обновление кластеров

Инфраструктурные пакеты

VMware Tanzu for Kubernetes Operations

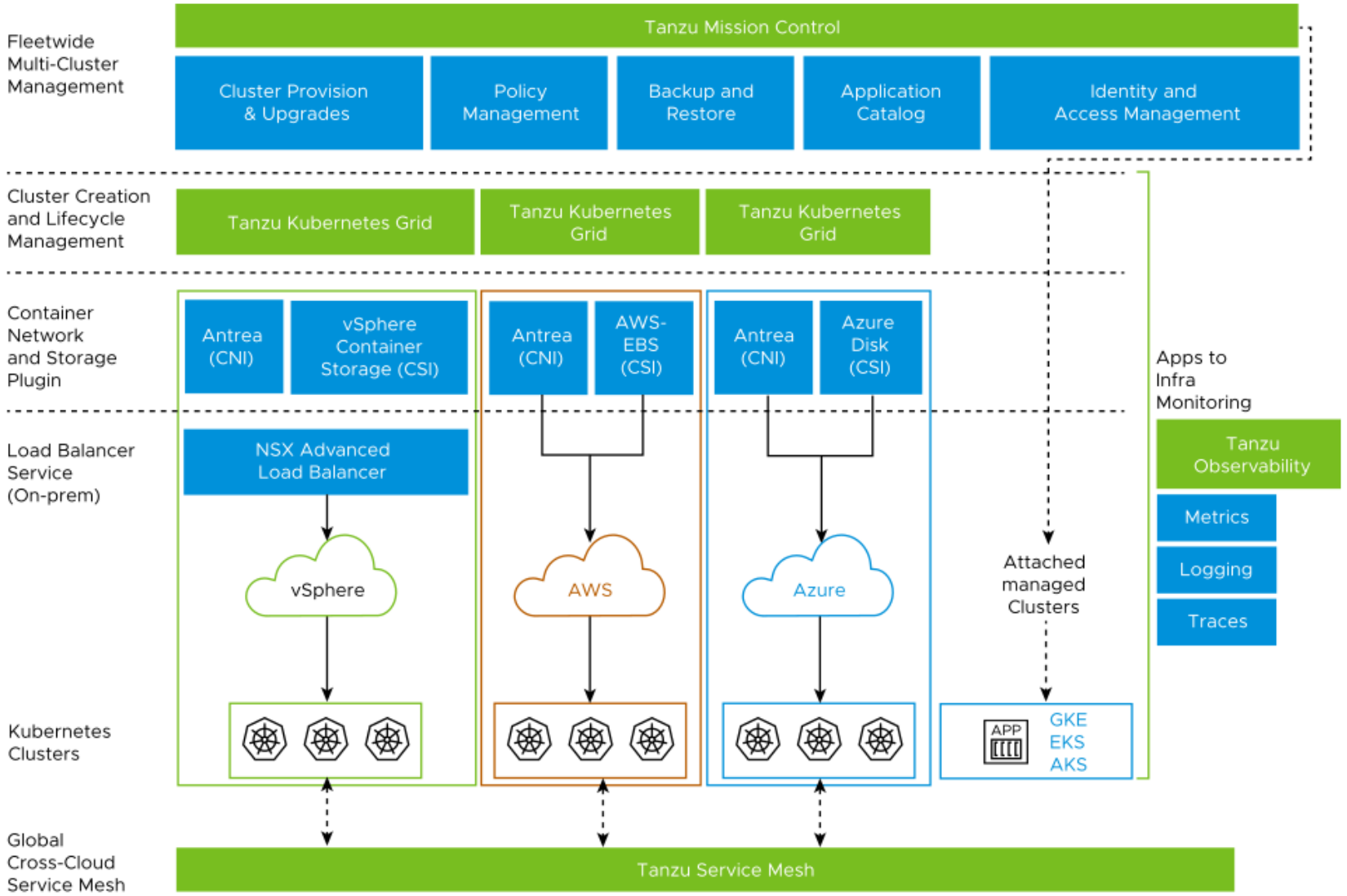
Hilbert Team

набор продуктов VMware



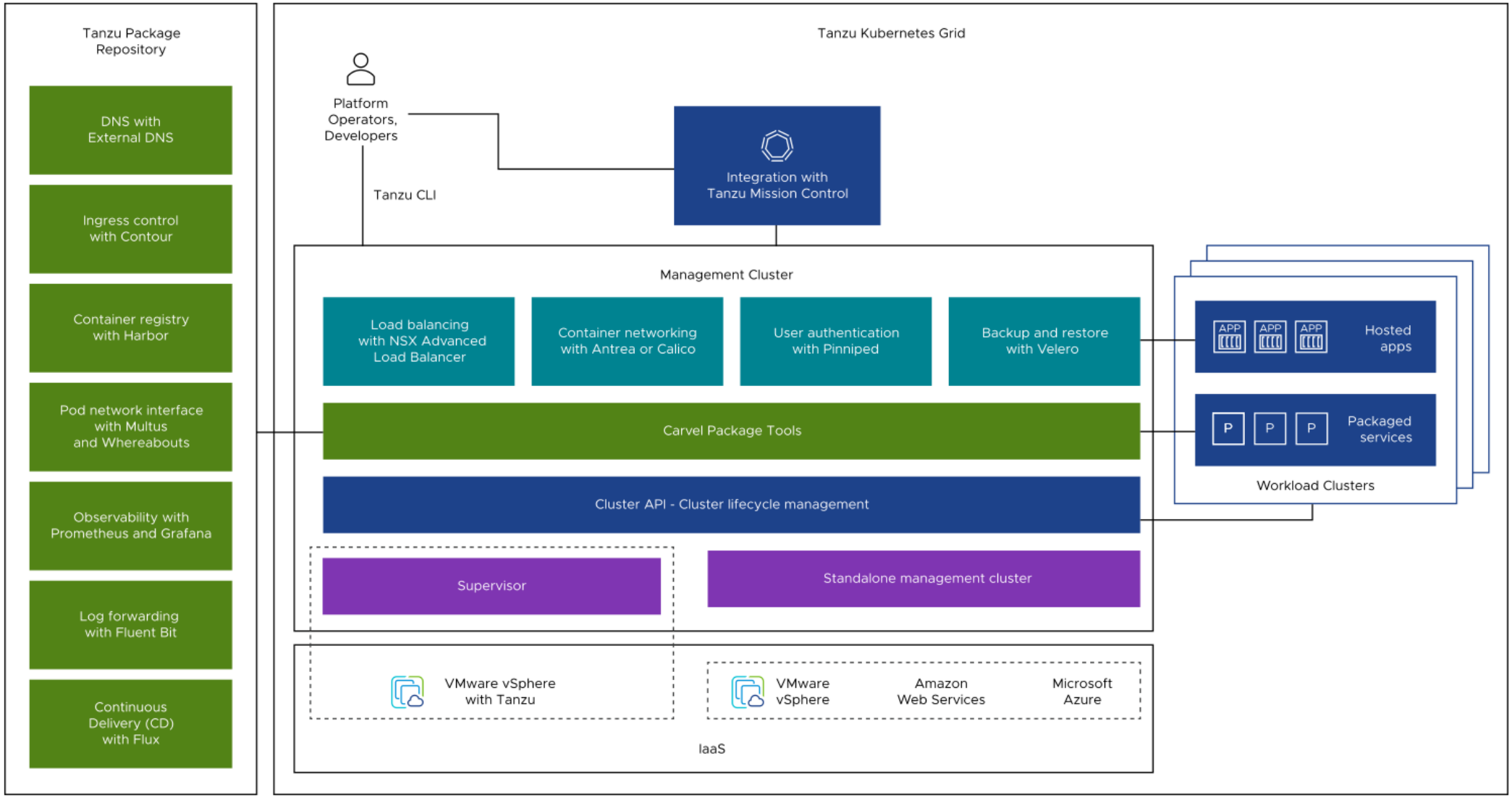
VMware Tanzu for Kubernetes Operations

набор продуктов и сервисов для управления k8s окружениями



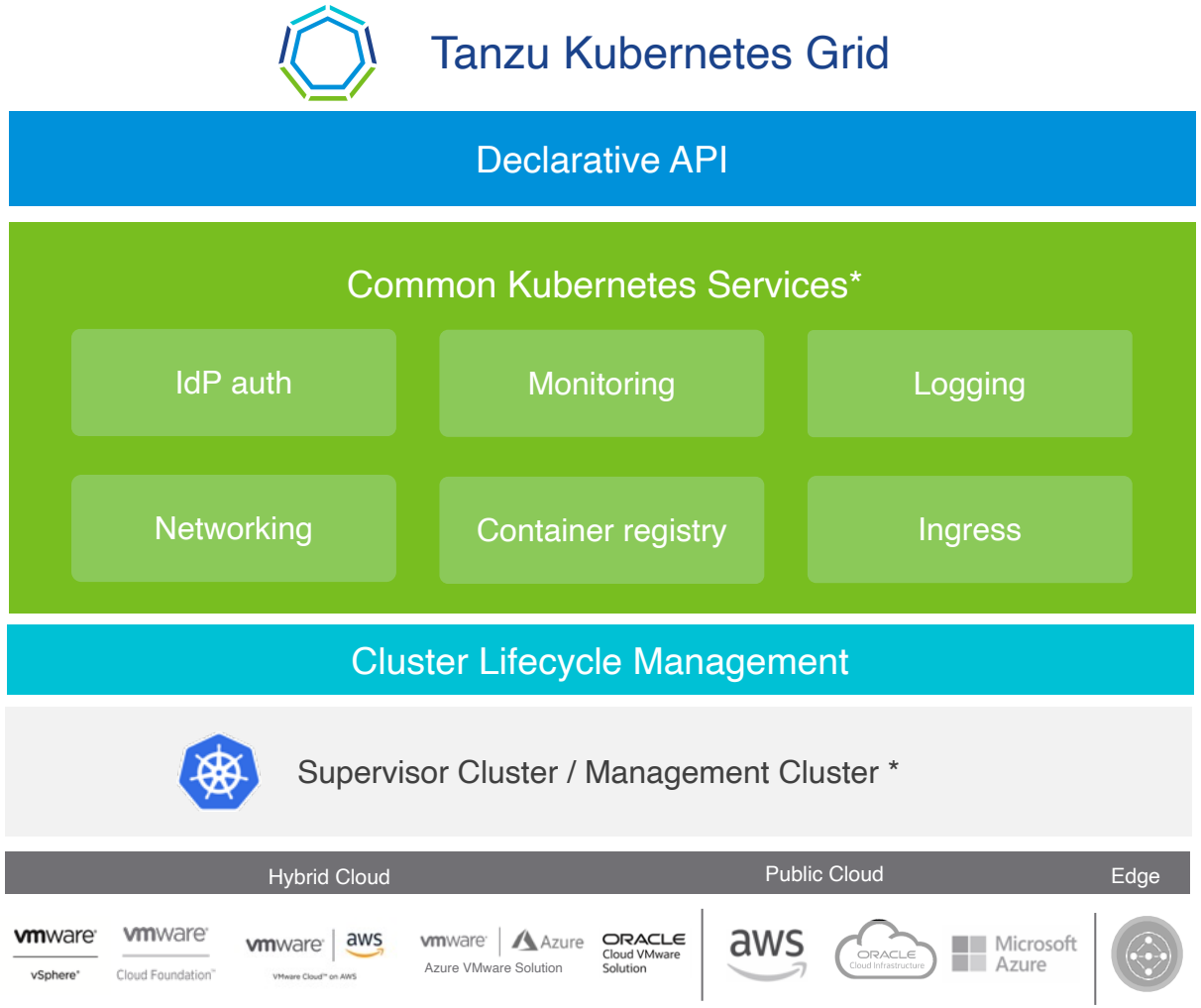
Tanzu Kubernetes Grid (TKG)

Hilbert Team



Tanzu Kubernetes Grid (TKG)

Hilbert Team



HARBOR

Cluster API

VELERO

CONTOUR

CARVEL

SONOBUOY

fluentbit

Grafana

Prometheus

ANTREA

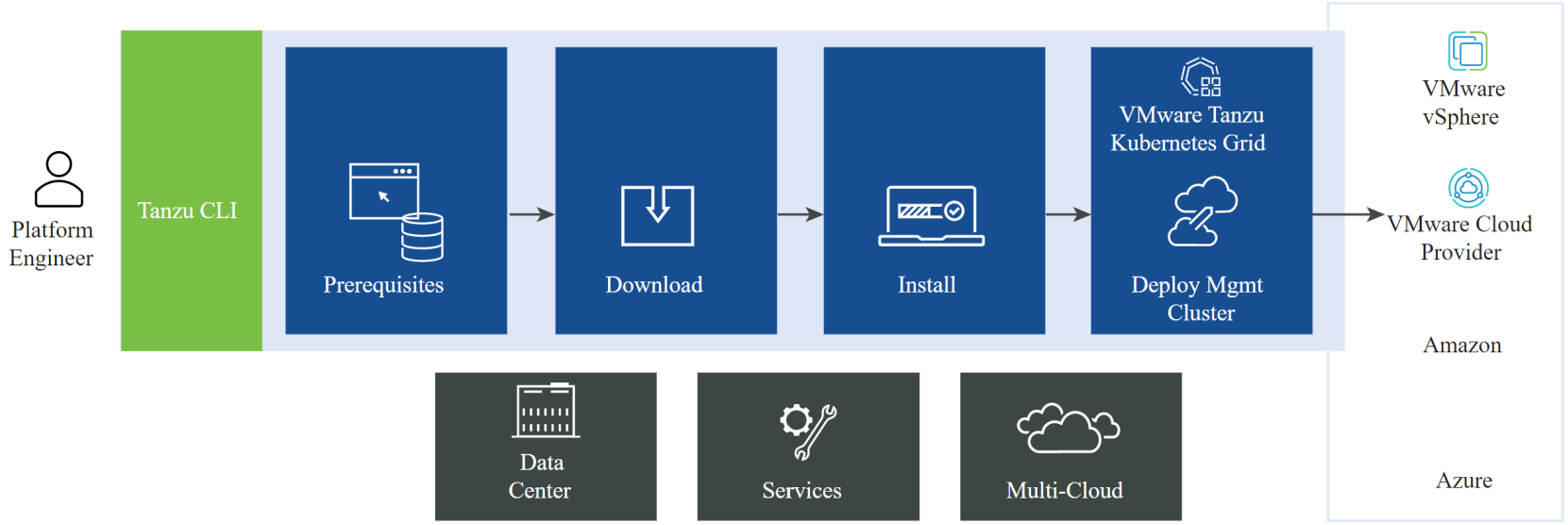
PROJECT CALICO

Bootstrap Machine и Tanzu CLI

- для начала работы вам потребуется Bootstrap VM, на которую необходимо будет установить Tanzu CLI
  - в дальнейшем ее можно использовать как машину для управления
- В случае Supervisor - это не потребуется, управление идет через VCenter

Tanzu CLI дает набор команд для:

- создания управляющих кластеров
- подключения к Supervisor кластерам
- создания, обновления и масштабирования рабочих кластеров
- установки, управления и удаления пакетов



Tanzu Kubernetes Releases (TKRs)

Hilbert Team

- Упакованные, подписанные, проверенные и поддерживаемые релизы Kubernetes от VMware.
- Используются upstream дистрибутивы и основные компоненты для обеспечения надежности и безопасности.
- Интегрированная проверка совместимости обновлений для безопасного обновления кластеров.
- Выравнивание с официальной поддержкой версий Kubernetes N-2 для обеспечения стабильности.
- Поддержка Photon OS, Ubuntu, Amazon Linux в качестве официально распространяемых образов.
- Возможность создания собственных образов с помощью инструмента image-builder, поддерживаемого сообществом Kubernetes.

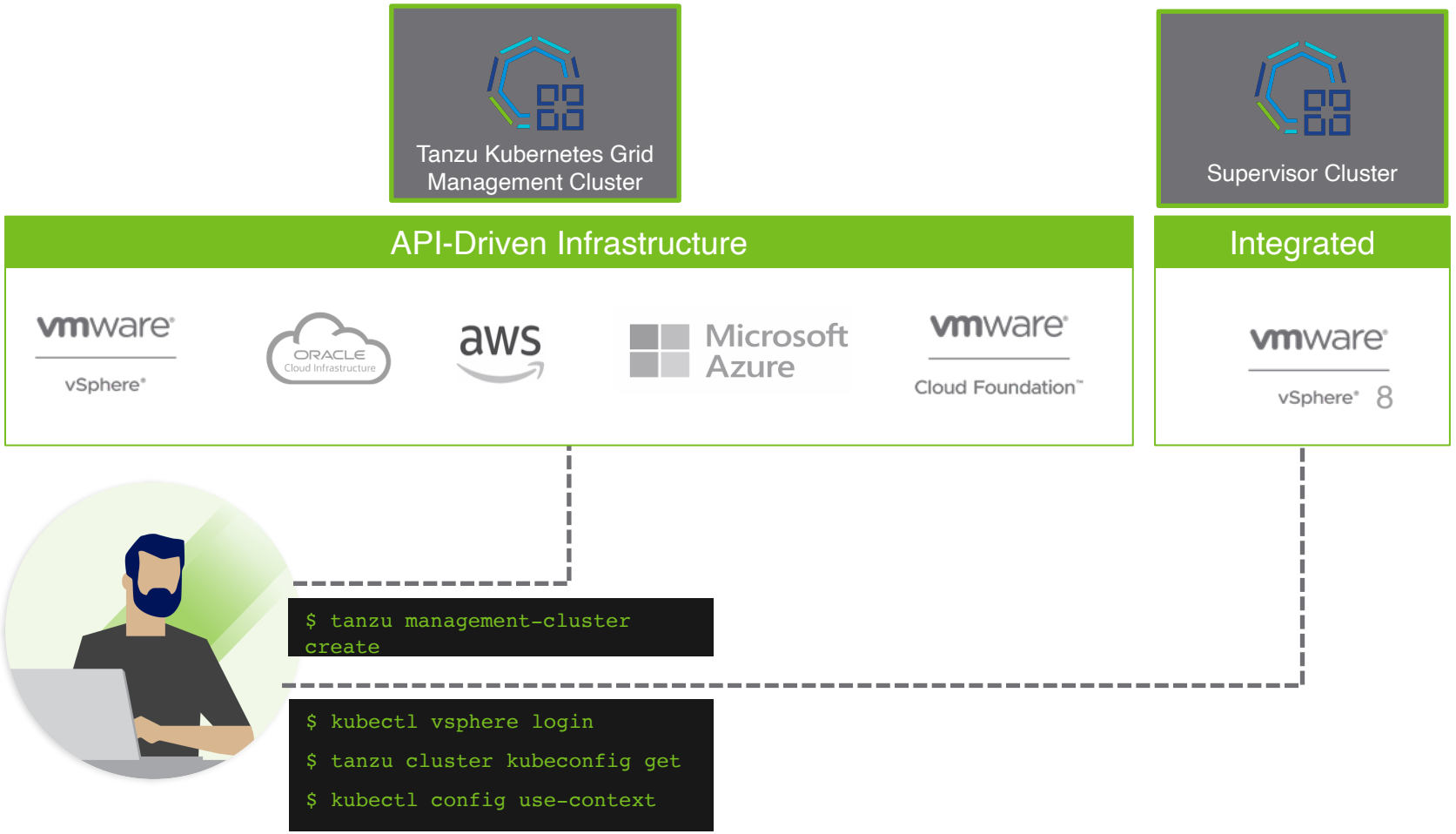
Tanzu Kubernetes Releases (TKRs)

Hilbert Team

- Релизы TKG управляются через CRD объекты
- Развертывание происходит с помощью Tanzu CLI

```
student01@dc:~$ tanzu kubernetes-release get
  NAME                                VERSION                             COMPATIBLE  ACTIVE
  v1.21.2---vmware.1-tkg.1.ee25d55    v1.21.2+vmware.1-tkg.1.ee25d55      True        True
  v1.21.6---vmware.1-tkg.1.b3d708a    v1.21.6+vmware.1-tkg.1.b3d708a      True        True
  v1.22.9---vmware.1-tkg.1.cc71bc8    v1.22.9+vmware.1-tkg.1.cc71bc8      True        True
  v1.23.8---vmware.2-tkg.2-zshippable v1.23.8+vmware.2-tkg.2-zshippable   True        True
  v1.23.8---vmware.3-tkg.1            v1.23.8+vmware.3-tkg.1              True        True
```

Management Cluster



Для централизованного управления развертыванием и жизненным циклом кластерами требуется Management кластер

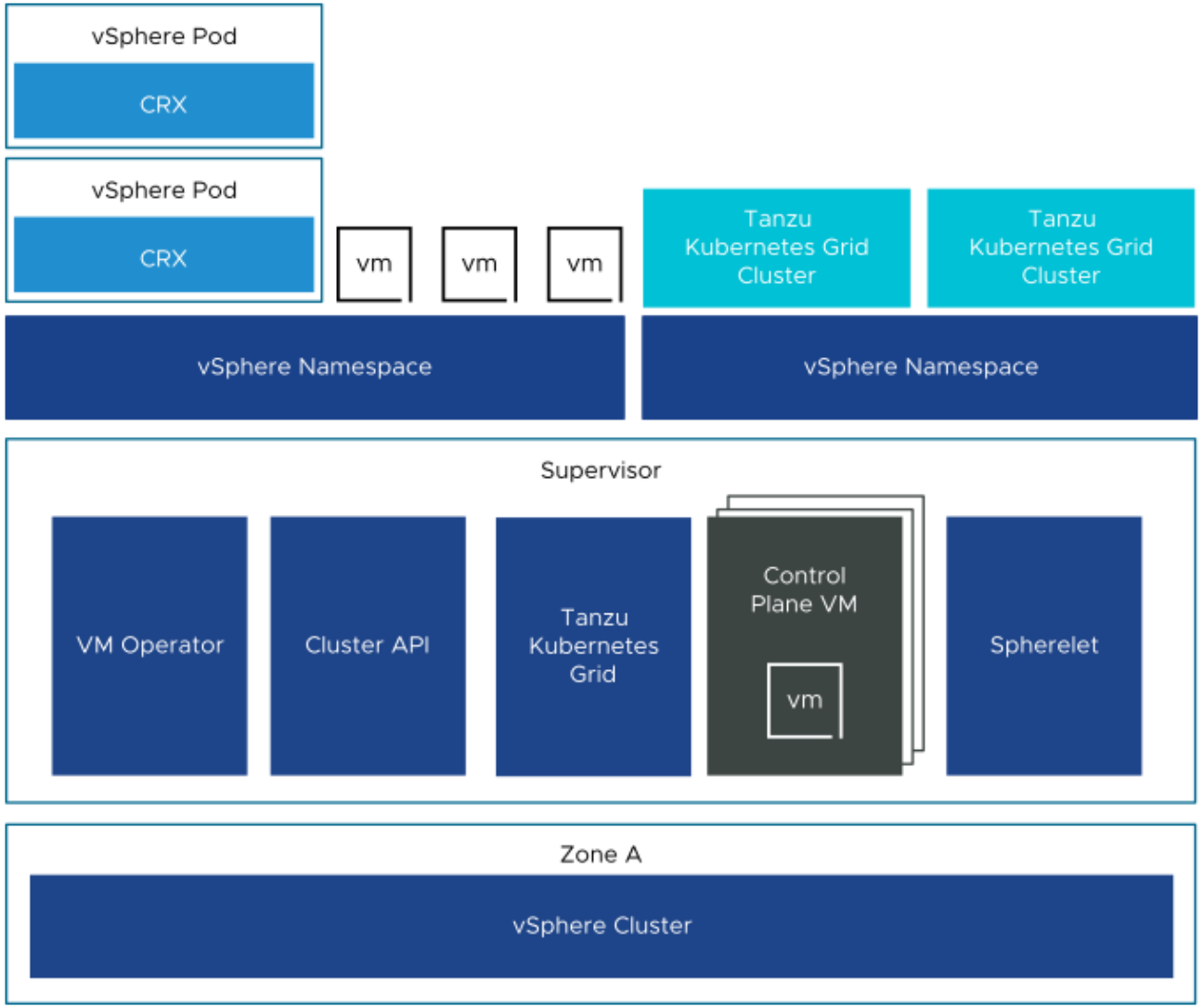
Он может быть развернут как:

- отдельностоящий управляющий кластер
  - на одной или нескольких VM
- Supervisor Cluster
  - требуется 3 ноды

vSphere with Tanzu

Hilbert Team

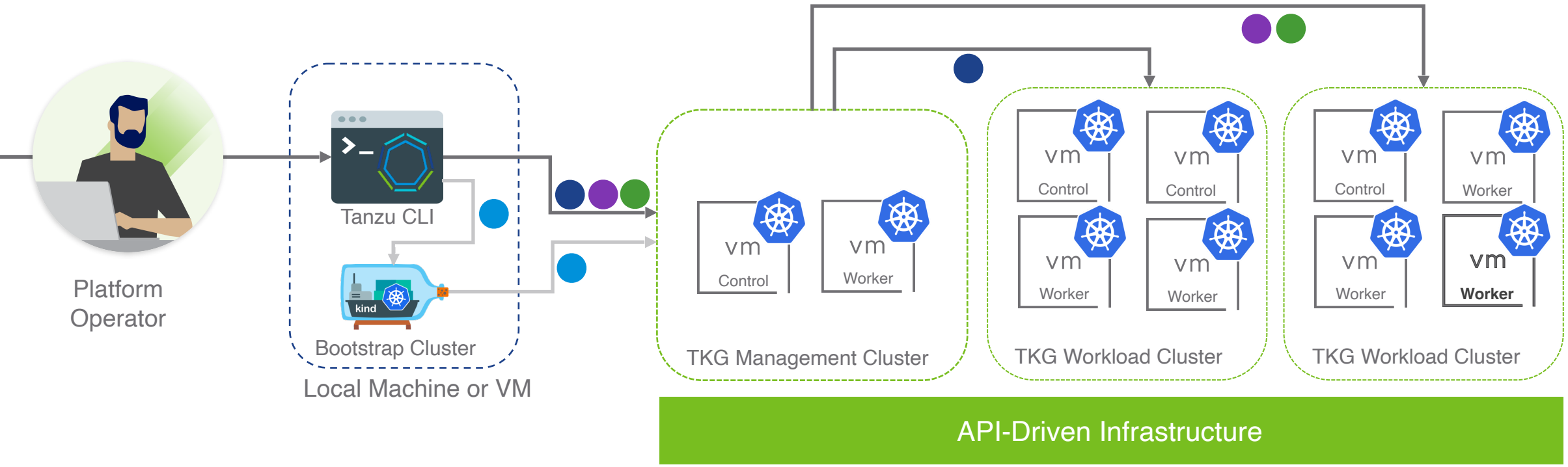
supervisor architecture



Процесс развертывания

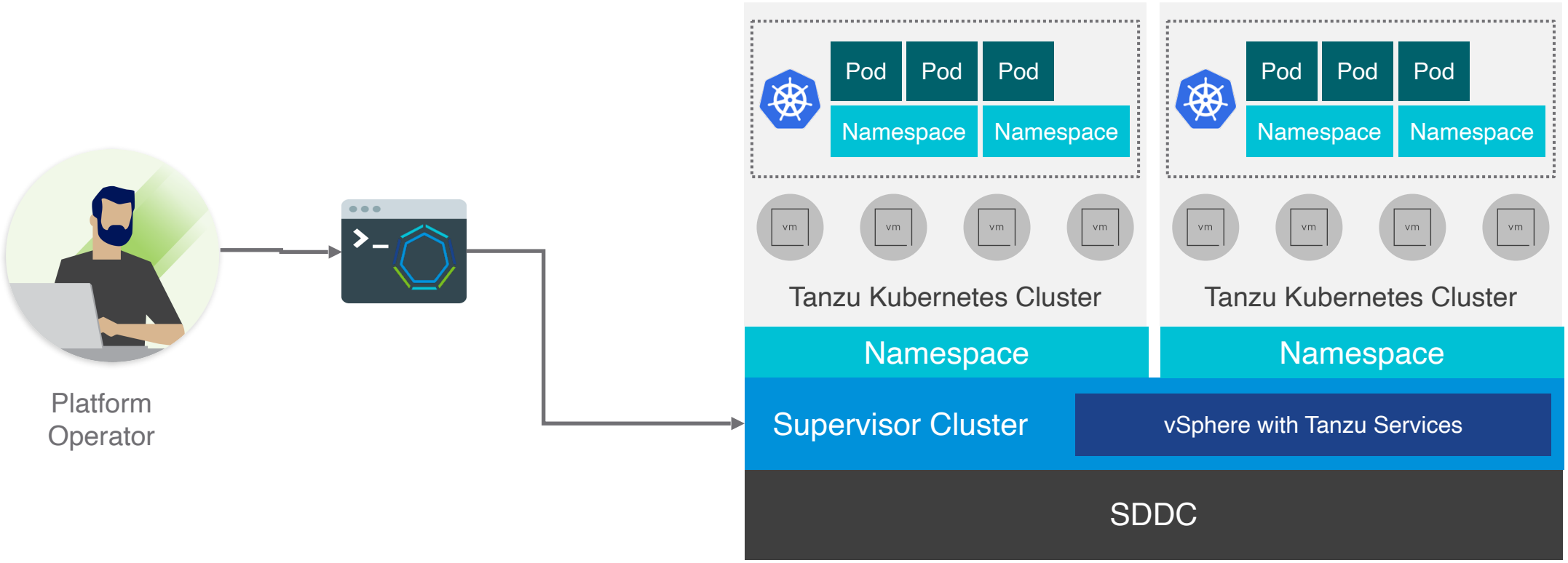
Hilbert Team

workload clusters




```
tanzu management-cluster create --ui
tanzu cluster create my-prod-k8s -f config.yaml
tanzu cluster create my-dev-k8s -f config.yaml
tanzu cluster scale my-dev-k8s -w 3
```

Прямое управление Supervisor кластером

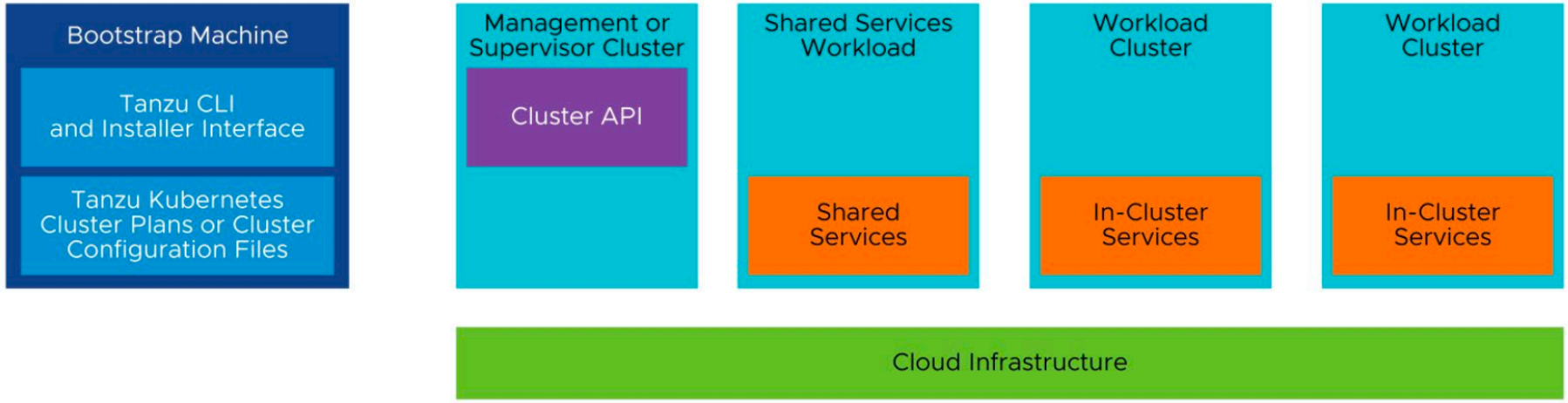



```
$ kubectl vsphere login -u administrator@vsphere.local --server=SUPERVISOR_IP
$ kubectl config use-context NAMESPACE
$ tanzu cluster kubeconfig get CLUSTER --admin -n NAMESPACE
$ kubectl config use-context CLUSTER
```

Пакеты для предоставления кластерных сервисов

Hilbert Team

- С помощью Tanzu CLI можно устанавливать пакеты с помощью для предоставления таких сервисов как:
  - *аутентификация, ingress, container registry, observability, service discovery, and logging*
- Эти пакеты собраны с помощью Carvel `imgpkg` и проверены VMware
- Они могут быть установлены:
  - внутрь каждого кластера (in-cluster service)
  - специальный инфраструктурный кластер, для предоставления сервисов для других кластеров
    - например Harbor



Install Harbor

Hilbert Team

```
tanzu package available list harbor.tanzu.vmware.com -A

# create harbor-data-values.yaml
image_url=$(kubectl -n tanzu-package-repo-global get packages harbor.tanzu.vmware.com.2.5.3+vmware.1-
tkg.1 -o \
jsonpath='{.spec.template.spec.fetch[0].imgpkgBundle.image}')

imgpkg pull -b $image_url -o /tmp/harbor-package

cp /tmp/harbor-package/config/values.yaml harbor-data-values.yaml

# edit harbor-data-values.yaml

# install package tanzu package install harbor --package harbor.tanzu.vmware.com --version
2.5.3+vmware.1-tkg.1 --values-file ./harbor-data-values.yaml \
 --namespace tanzu-system-registry

tanzu package installed get harbor --namespace tanzu-system-registry

NAME:                    harbor
PACKAGE-NAME:            harbor.tanzu.vmware.com
PACKAGE-VERSION:         2.5.3+vmware.1-tkg.1
STATUS:                  Reconcile succeeded
```

Типы кластеров

Hilbert Team

Class-based

- Для создания требуется описать манифест с kind - Cluster
- представлены в. vSphere with Tanzu 8 и TKG 2.1
- Описывают спецификацию топологии в spec.topology блоке
  - например, число и тип рабочих и управляющих нод
- Наследуют конфигурацию из spec.topology.class значения
  - Ссылается на ClusterClass объект
  - в Supervisor, по умолчанию class - это tanzukubernetescluster
  - На отдельно стоящем кластере, class формируются как tkg-INFRASTRUCTURE-default-VERSION, например, tkg-vsphere-default-v1.0.0.

Plan-based and TKC clusters (legacy)

- Для создания кластера можно использовать конфигурационный файл с переменными
- Используются имена переменных в UPPER_CASE с подчеркиванием, например CLUSTER_NAME

Plan-based and TKC clusters

Hilbert Team

```
tanzu cluster create my-cluster --plan dev
```

```
#! ---------------------------------------------------
#! Basic cluster creation configuration
#! ---------------------------------------------------

# CLUSTER_NAME:
CLUSTER_PLAN: dev
NAMESPACE: default
CNI: antrea

#! ---------------------------------------------------
#! Node configuration
#! ---------------------------------------------------

# SIZE:
# CONTROLPLANE_SIZE:
# WORKER_SIZE:
...
```

Class-based

Hilbert Team

```
tanzu cluster create my-cluster --file tkc.yaml
```

```yaml
apiVersion: cluster.x-k8s.io/v1beta1
kind: Cluster
metadata:
  name: "classy-cluster"
  namespace: demo
spec:
  clusterNetwork:
    services:
      cidrBlocks: ["198.51.100.0/12"]
    pods:
      cidrBlocks: ["192.0.2.0/16"]
    serviceDomain: "cluster.local"
  topology:
    class: tanzukubernetescluster
    version: v1.23.5+vmware.1
    controlPlane:
      replicas: 1
    workers:
      #node pools:
      machineDeployments:
        - class: node-pool
          name: node-pool-1
          replicas: 1
    variables:
      - name: vmClass
        value: best-effort-small
      - name: storageClass
        value: "global-storage-profile"
      - ntp:
        value: time.vmware.com
```

```yaml
apiVersion: cluster.x-k8s.io/v1beta1
kind: Cluster
metadata:
  name: "classy-cluster"
```

```yaml
  topology:
    class: tanzukubernetescluster
    version: v1.23.5+vmware.1
    controlPlane:
      replicas: 1
    workers:
      #node pools:
      machineDeployments:
        - class: node-pool
          name: node-pool-1
          replicas: 1
```

TKG Lifecycle with Tanzu CLI

Hilbert Team

Create

- Создание нового TKC кластера
- `tanzu create tkc-a01`

Scale

- Масштабирование кластера
- `tanzu scale tkc-a01 --controlplane-machine-count 3 --worker-machine-count 3`

Upgrade

- Обновление кластера на новую версию
- `tanzu upgrade tkc-a01 --tkr v1.23.8.vmware.1`

Delete

- Удаление TKC кластера
- `tanzu delete tkc-a01`

Бесшовное обновление версии Kubernetes

Hilbert Team

CLI

- обновите и затем проверьте корректность версии Tanzu CLI
- `tanzu version`

OVAs

- скачайте и задеплойте последние версии Tanzu Kubernetes Grid OVAs для OS и Kubernetes

MGMT Cluster

- Обновите управляющий кластер
- `tanzu management-cluster upgrade`

Workload Cluster

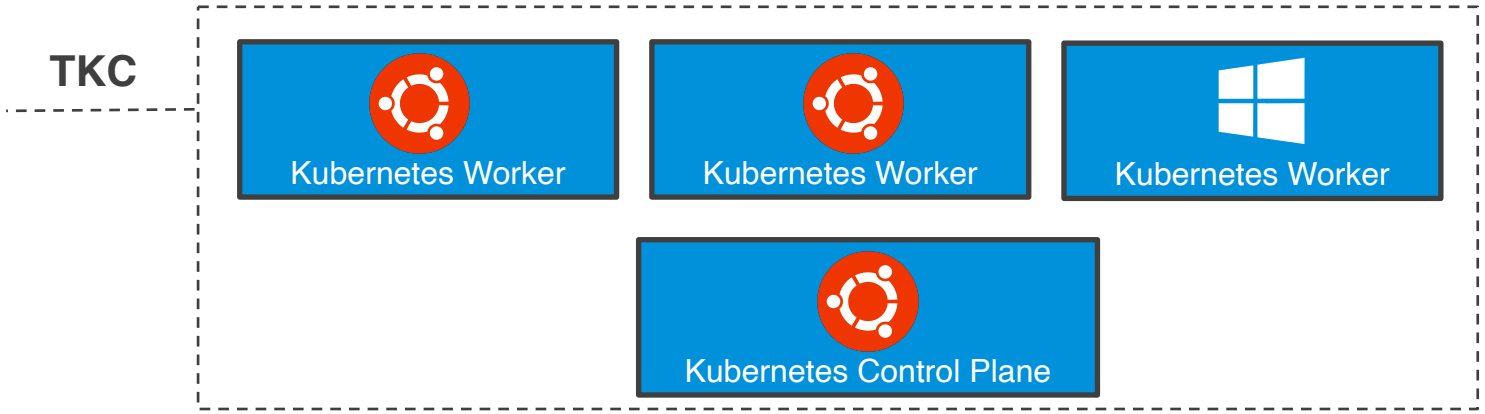
- Обновите рабочие кластера по мере необходимости
- `tanzu cluster upgrade my-cluster`

полная поддержка Windows контейнеров

Hilbert Team

Можно включить поддержку Windows контейнеров в конфигурационном файле и создать новый кластер. Потребуется загрузить дополнительные ISO

```
IS_WINDOWS_WORKLOAD_CLUSTER: "true"
VSPHERE_WINDOWS_TEMPLATE: windows-2019-kube-v1.23.8
ENABLE_MHC: "false"
```



Запускайте .NET и нативные Windows приложения в контейнерах в Kubernetes

Управляйте Windows нодами в кластере вместе с Linux нодами

Можно создавать свои Windows темплейты для деплоя новых нод

Kubernetes Image Builder

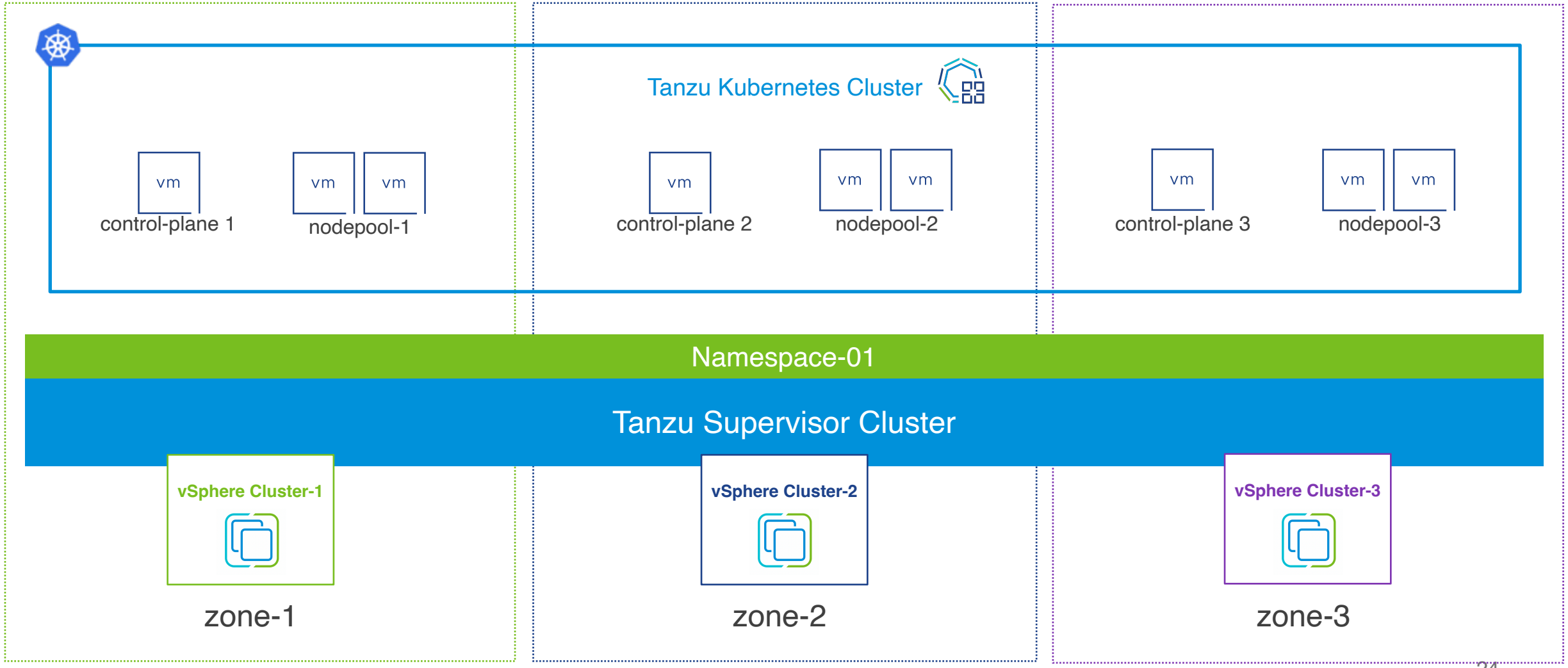
Hilbert Team

- Для сборки собственных CAPI образов рекомендуется использовать image-builder
  - https://github.com/kubernetes-sigs/image-builder

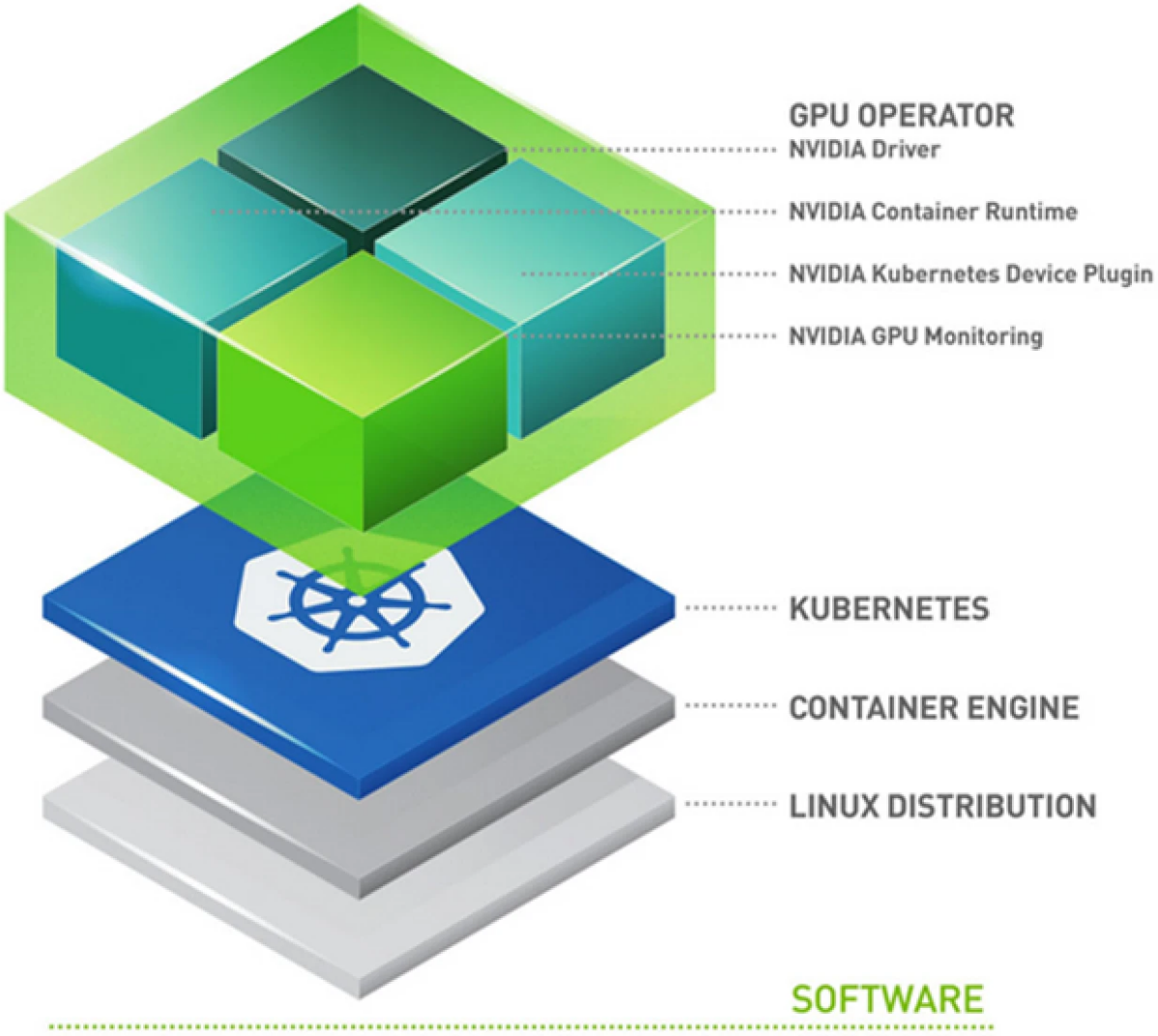
```
git clone git@github.com:kubernetes-sigs/image-builder.git
cd image-builder/images/capi
```

- С помощью него можно собирать образы для
  - AWS
  - Azure
  - vSphere
    - Open Virtualization Archive (OVA)
    - полученные образы импортируете в vSphere, делаете снэпшот и помечаете как vm template

Повышение устойчивости работы кластеров TKG с помощью распределения по зонам vSphere



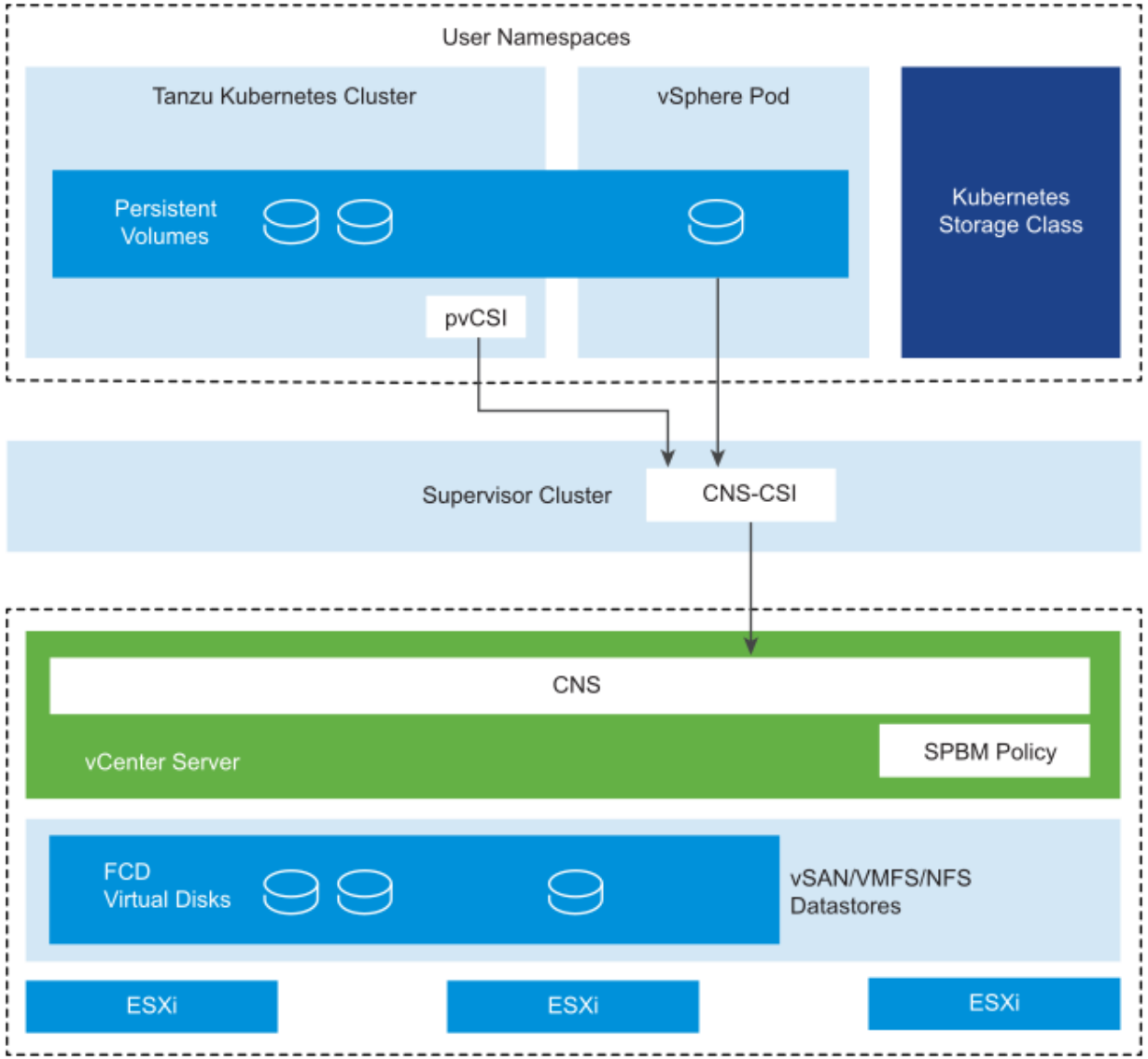
Использование GPU узлов для задач AI/ML



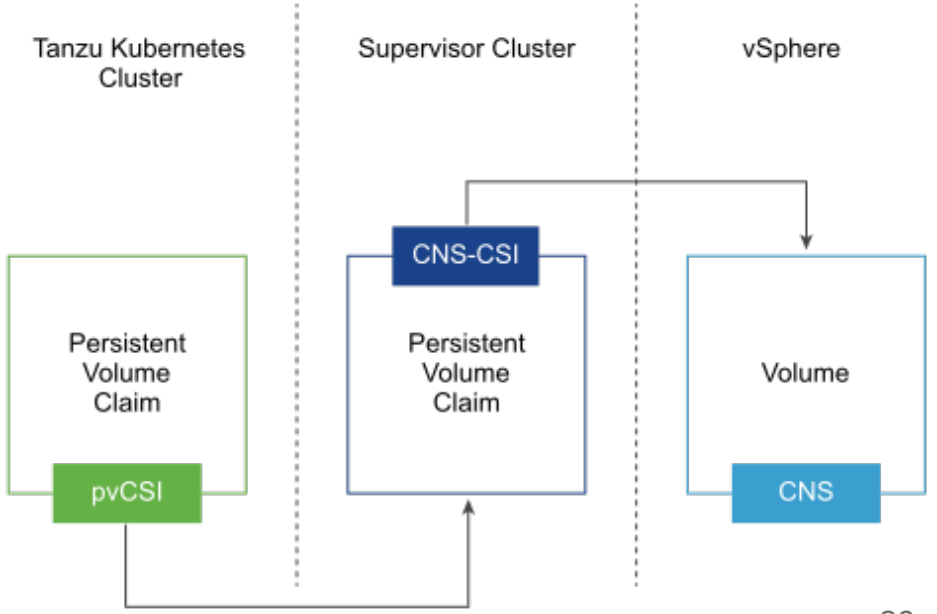
GPU operator реализован в виде helm чарта с помощью которого устанавливаются компоненты, которые позволяют запускать приложения с использованием GPU:

- GPU Feature Discovery размечает ноды с спецификацией GPU
- The NVIDIA AI Enterprise Guest Driver.
- Kubernetes Device Plugin для объявления GPU планировщику
- NVIDIA Container Toolkit для сборки и запуска контейнеров с поддержкой GPU
- DCGM Monitoring

CNS CSI

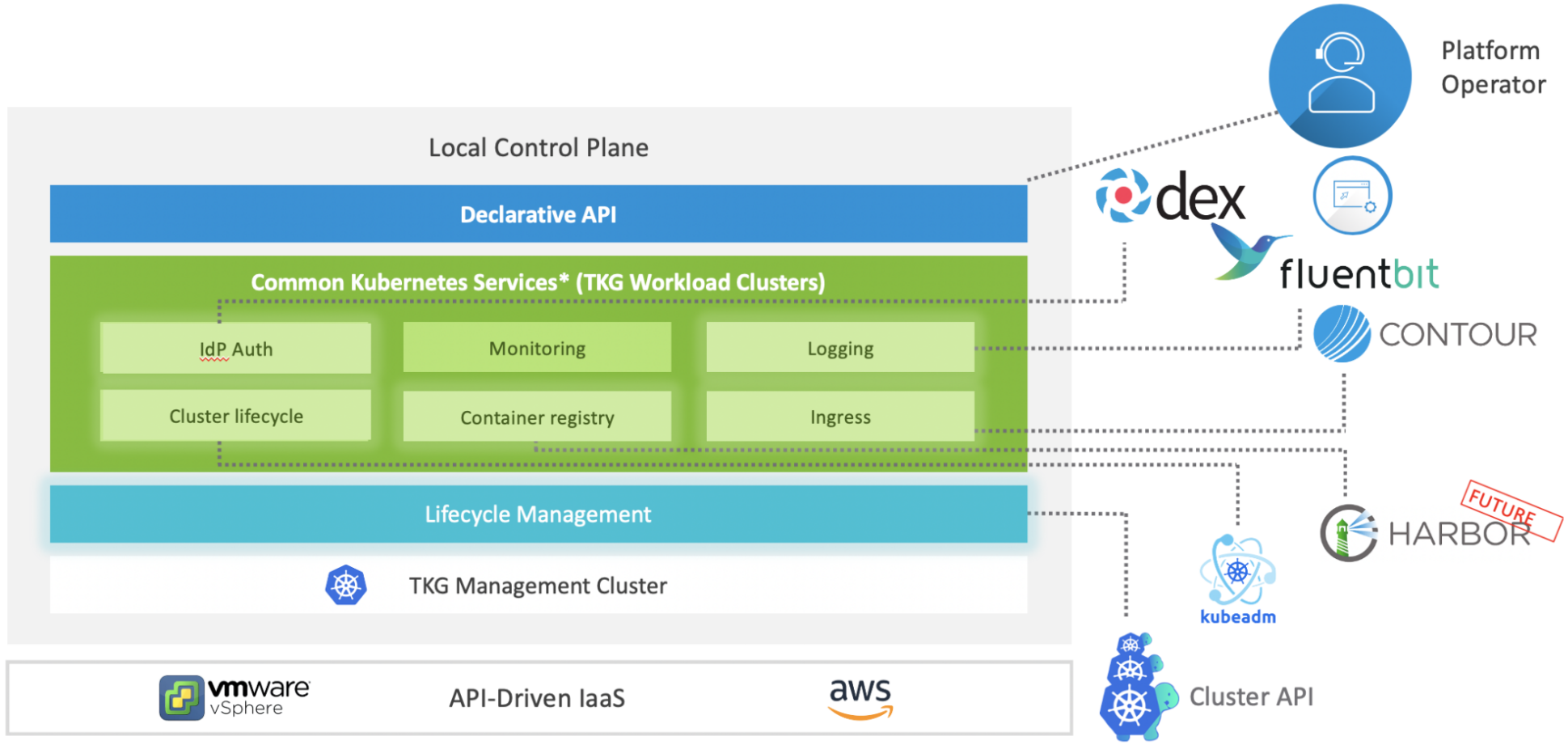



```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: default
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.vsphere.vmware.com
parameters:
  storagePolicyName: optional
```

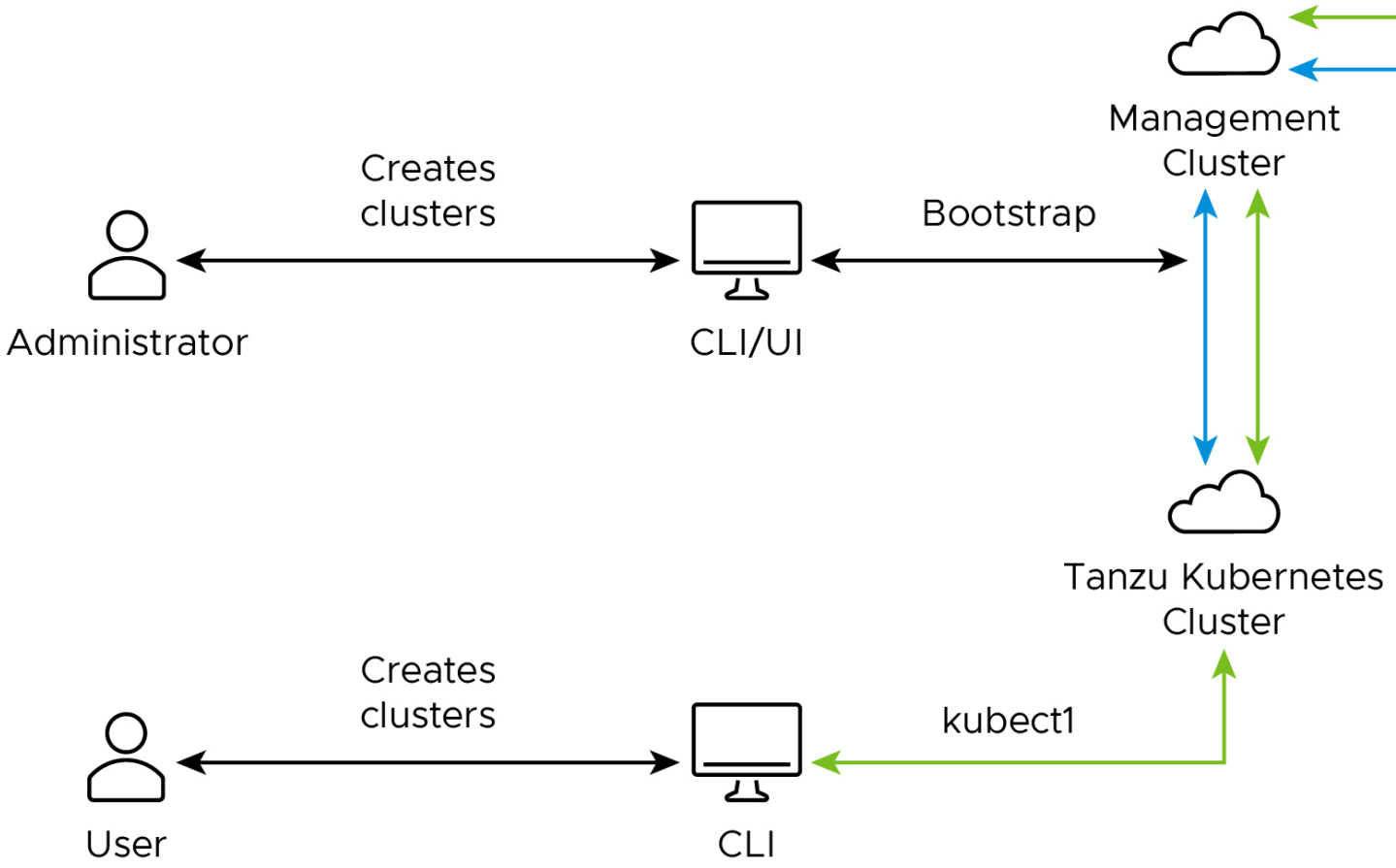


Инфраструктурные сервисы

Hilbert Team



Identity and Access Management



Используется Pinniped

- позволяет подключать OpenID Connect (OIDC) или LDAP провайдеров (IdP) в рабочие кластера
- для LDAP используется Dex
- для OIDC внутренние ендпоинты
- администратор настраивает IAM в управляющем кластере
- при создании рабочего кластера конфигурация наследуется
- процесс аутентификации идет через управляющий кластер

Пример настройки RBAC для рабочего кластера

Hilbert Team

- С помощью Tanzu CLI получим не админский конфиг для рабочего кластера
  - `tanzu cluster kubeconfig get my-cluster --export-file /tmp/my-cluster-kubeconfig`
- Выполним простую операцию, она перекинет на Login страницу (понадобится браузер)
  - `kubectl get pods -A --kubeconfig /tmp/my-cluster-kubeconfig`
- После аутентификации мы получим ошибку, т.к. прав не хватает
- Получим админский конфиг
  - `tanzu cluster kubeconfig get my-cluster --admin`
- Переключим контекст
  - `kubectl config use-context my-cluster-admin@my-cluster`
- Создадим ClusterRoleBinding
  - `kubectl create clusterrolebinding workload-test-rb --clusterrole cluster-admin --user user@example.com`
- Теперь если выполним повторно нашу операцию то все пройдет успешно
  - `kubectl get pods -A --kubeconfig /tmp/my-cluster-kubeconfig`

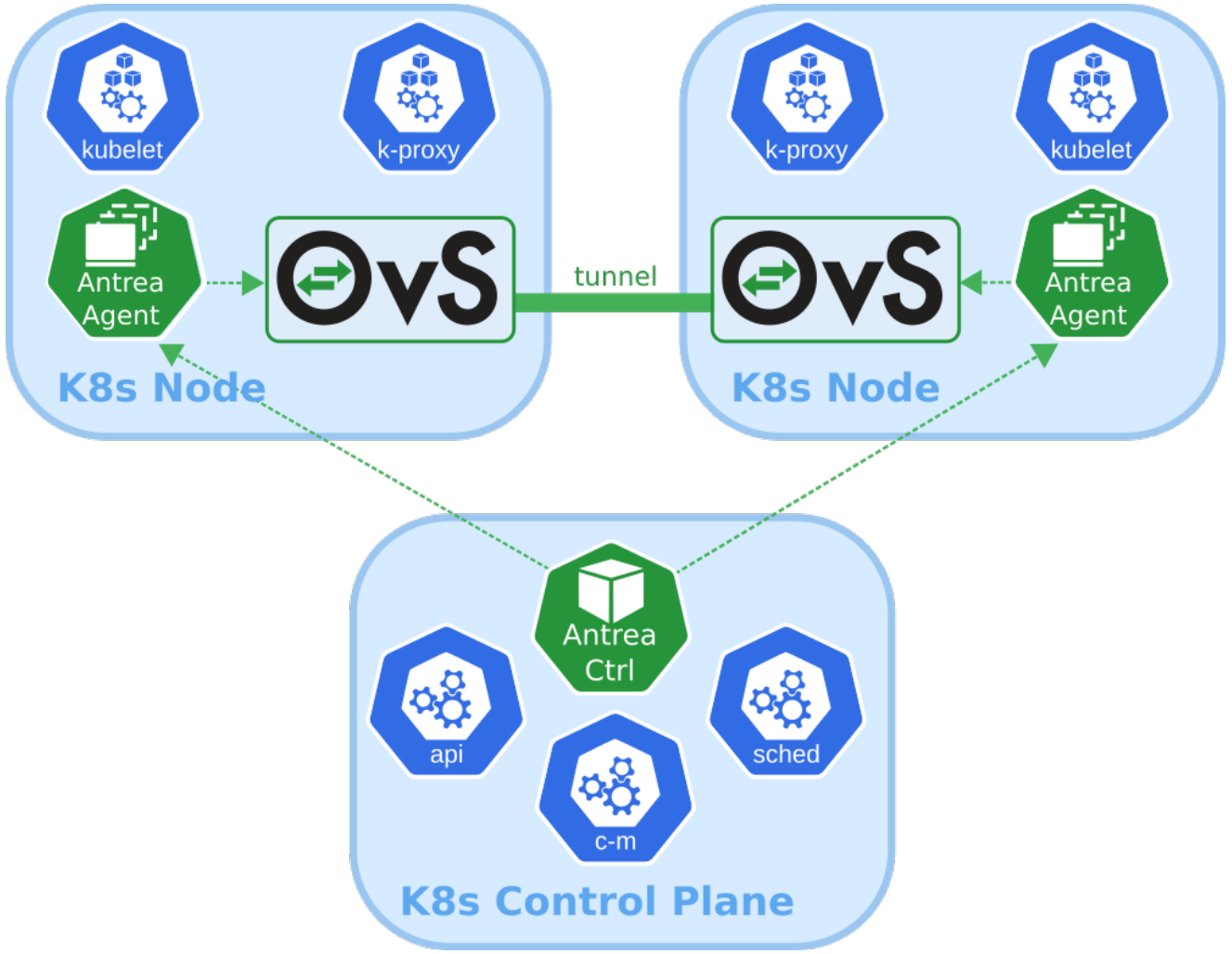
TKG Networking

Hilbert Team

Endpoint	Provider
Pod connectivity	Antrea or Calico
Service type: ClusterIP	Antrea or Calico
Service type: NodePort	Antrea or Calico
Service type: LoadBalancer	NSX-T load balancer, NSX Advanced Load Balancer, HAProxy
Cluster ingress	Third-party ingress controller
Network policy	Antrea or Calico

CNI: Antrea

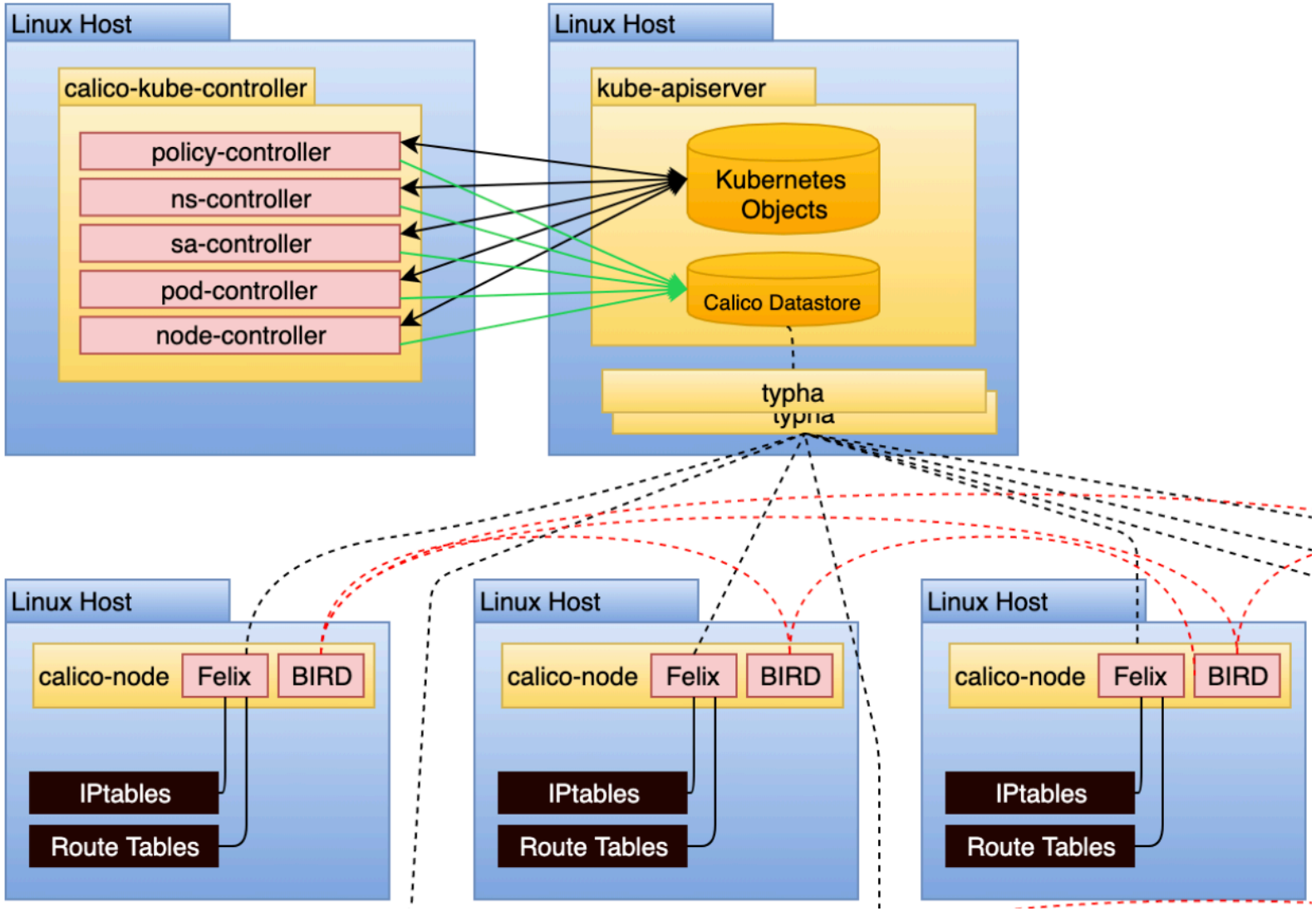
Hilbert Team



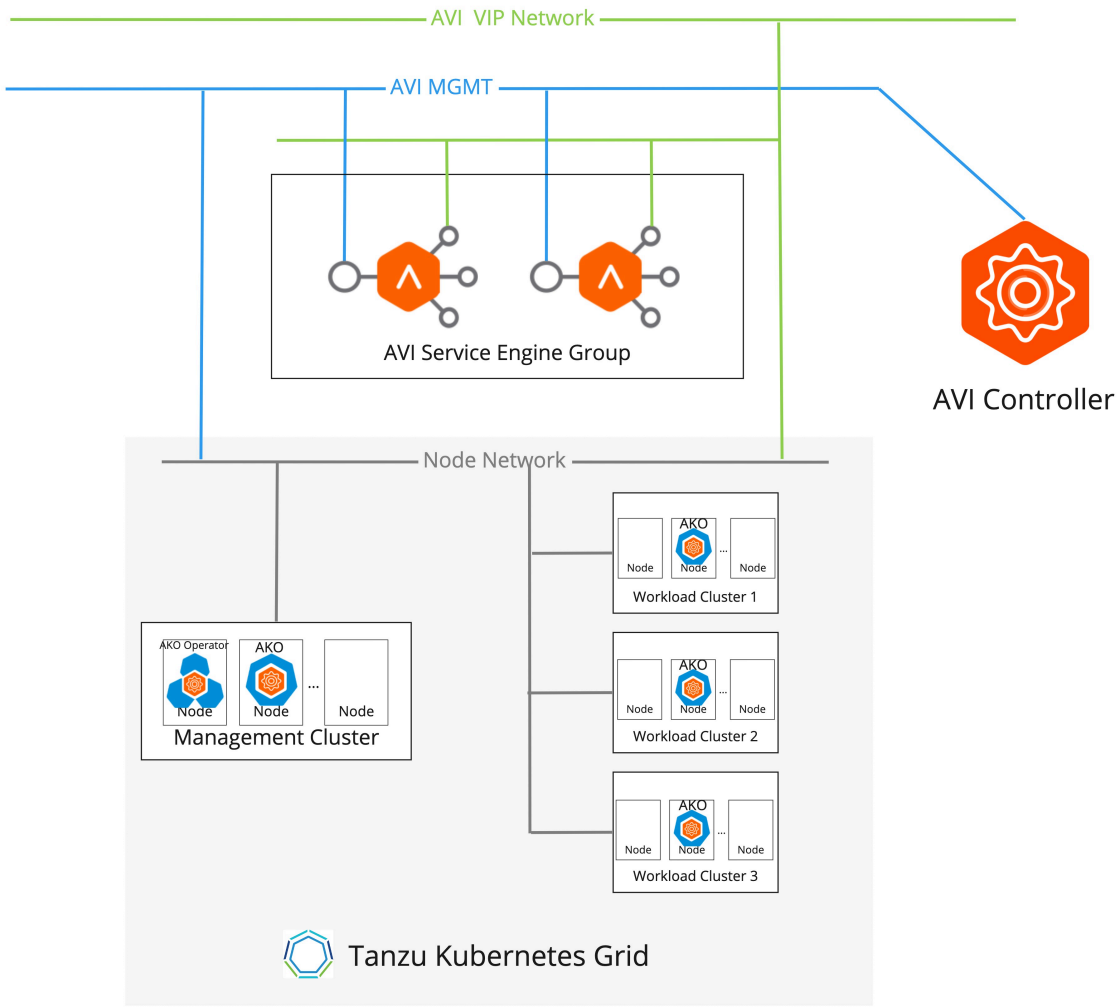
- Используется по умолчанию
- Kubernetes-native
- Powered by Open vSwitch
- Run everywhere
- Comprehensive policy model
- Windows Node support
- Troubleshooting and monitoring tools
- Network observability and analytics
- Network Policies for virtual machines
- Encryption
- Easy deployment

CNI: Calico

Hilbert Team



NSX Advanced Load Balancer



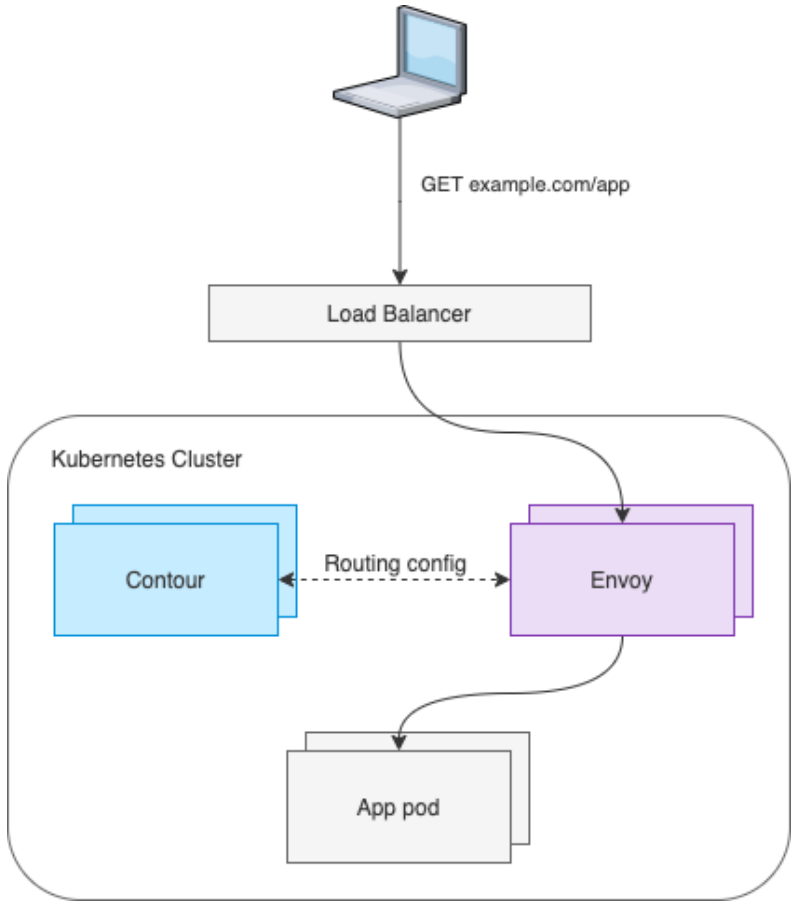
- L4 Load Balancer Implementation
- L7 ingress controller
- Cluster endpoint VIP and control plane load balancing provider

Основные компоненты

- **Avi Kubernetes Operator (AKO)**
- **AKO Operator** i
- **Service Engines (SE)**
- **Service Engine Groups**
- **Avi Controller**

Secure Ingress Routing

Hilbert Team



CONTOUR

```
cat <<EOF | kubectl apply --filename -
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: nginx
  annotations:
    ingress.kubernetes.io/force-ssl-redirect: "true"
    kubernetes.io/ingress.class: contour
spec:
  tls:
  - secretName: nginx-tls
    hosts:
    - nginx.mytanzu.com
  rules:
  - host: nginx.mytanzu.com
    http:
      paths:
      - pathType: Prefix
        path: "/"
        backend:
          service:
            name: nginx
            port:
              number: 80
EOF
```

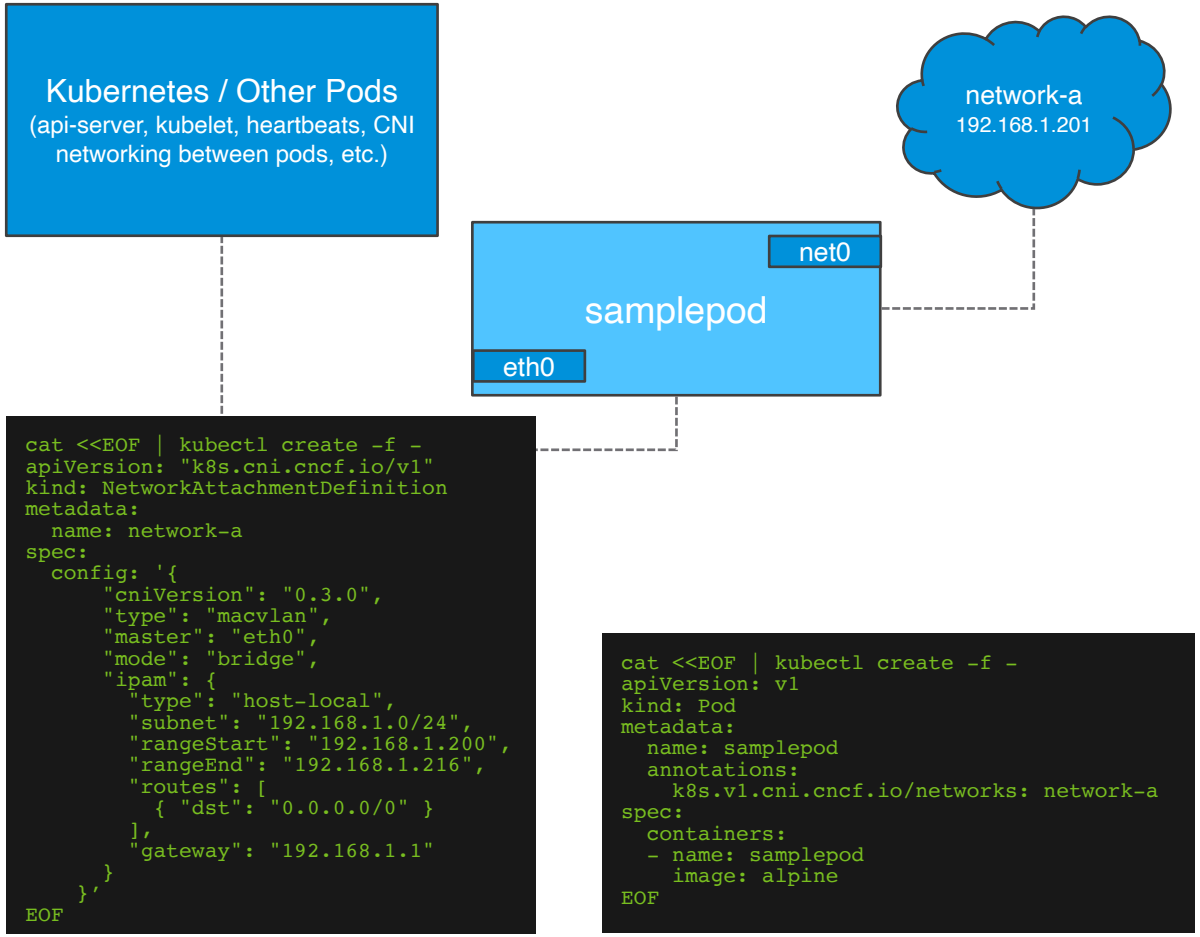
Customize your app for network connectivity

Hilbert Team

MULTUS

Multus CNI - плагин позволяющий подключить к подам несколько сетевых интерфейсов

Может вызывать любой дополнительный CNI установленный в кластере



Make Kubernetes Resources Discoverable

Hilbert Team

С помощью сервиса ExternalDNS возможно автоматически анонсировать сервисы внутри TKG.

```yaml
apiVersion: v1
kind: Service
metadata:
  name: nginx
  annotations:
    external-dns.alpha.kubernetes.io/hostname: nginx.external-dns-test.my-org.com
spec:
  type: LoadBalancer
  ports:
  - port: 80
    name: http
    targetPort: 80
  selector:
    app: nginx
```

Protecting Kubernetes Data

Hilbert Team

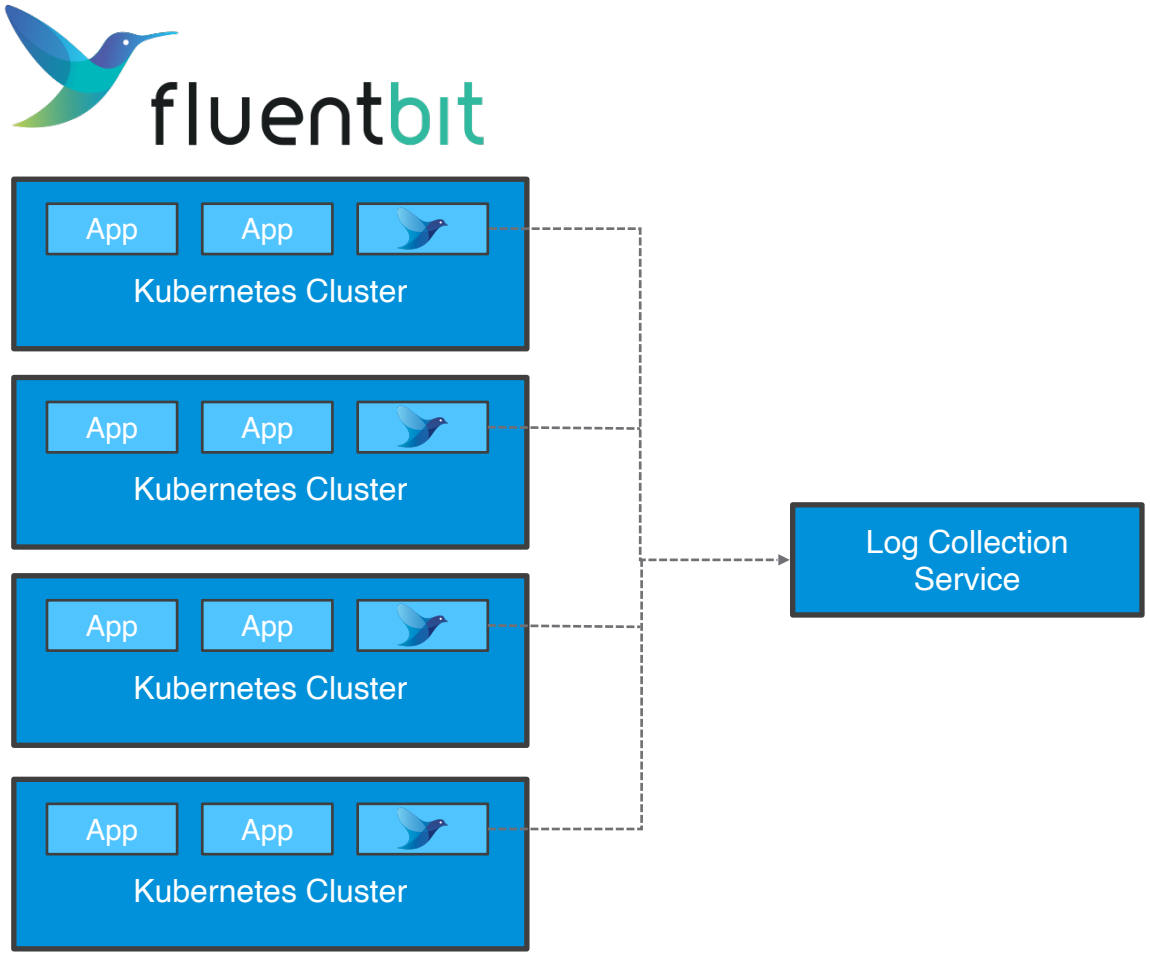
open-source решение для безопасного резервирования, восстановления и миграции Kubernetes кластеров и persistent volumes.

Подходит для миграции ресурсов между кластерами

VELERO

Kubernetes Logging and Processing

Hilbert Team



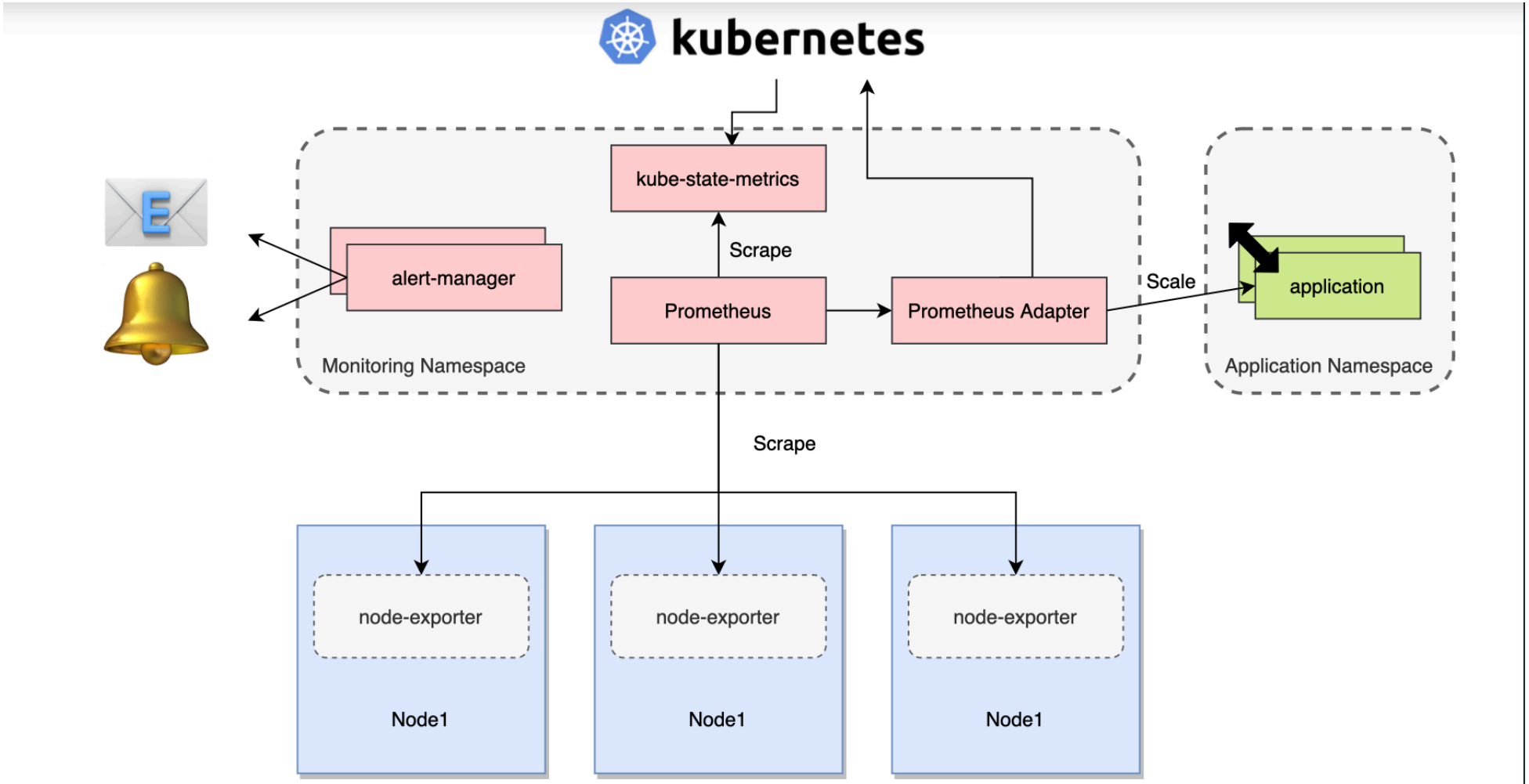
VMware Aria™

elasticsearch

splunk>

Мониторинг

Hilbert Team

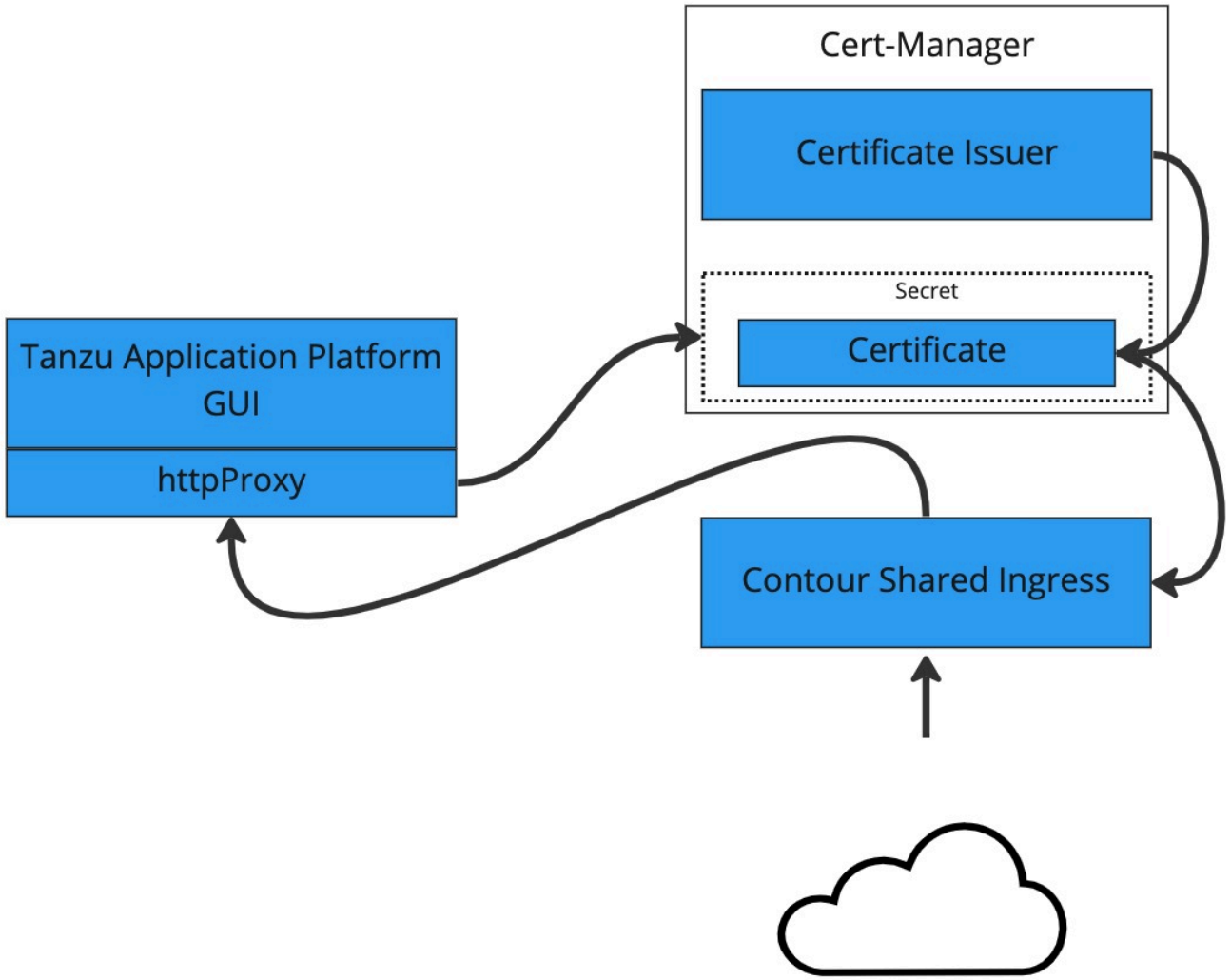


Prometheus

Grafana

Cloud Native Certificate Management For Apps

Hilbert Team



Спасибо за внимание

Ваши вопросы

Оставьте заявку
на аудит вашего бизнеса

Hilbert Team

Алексей
Цыкунов

hilbertteam.com @hilbertteam

@erlong15