# Опыты с IaC: Как мы научились запускать зоны доступности облака за пару дней

Гулаков Иван
DevOps Technical Lead

CloudMTS

# Иван Гулаков

**Техлид DevOps-команды**

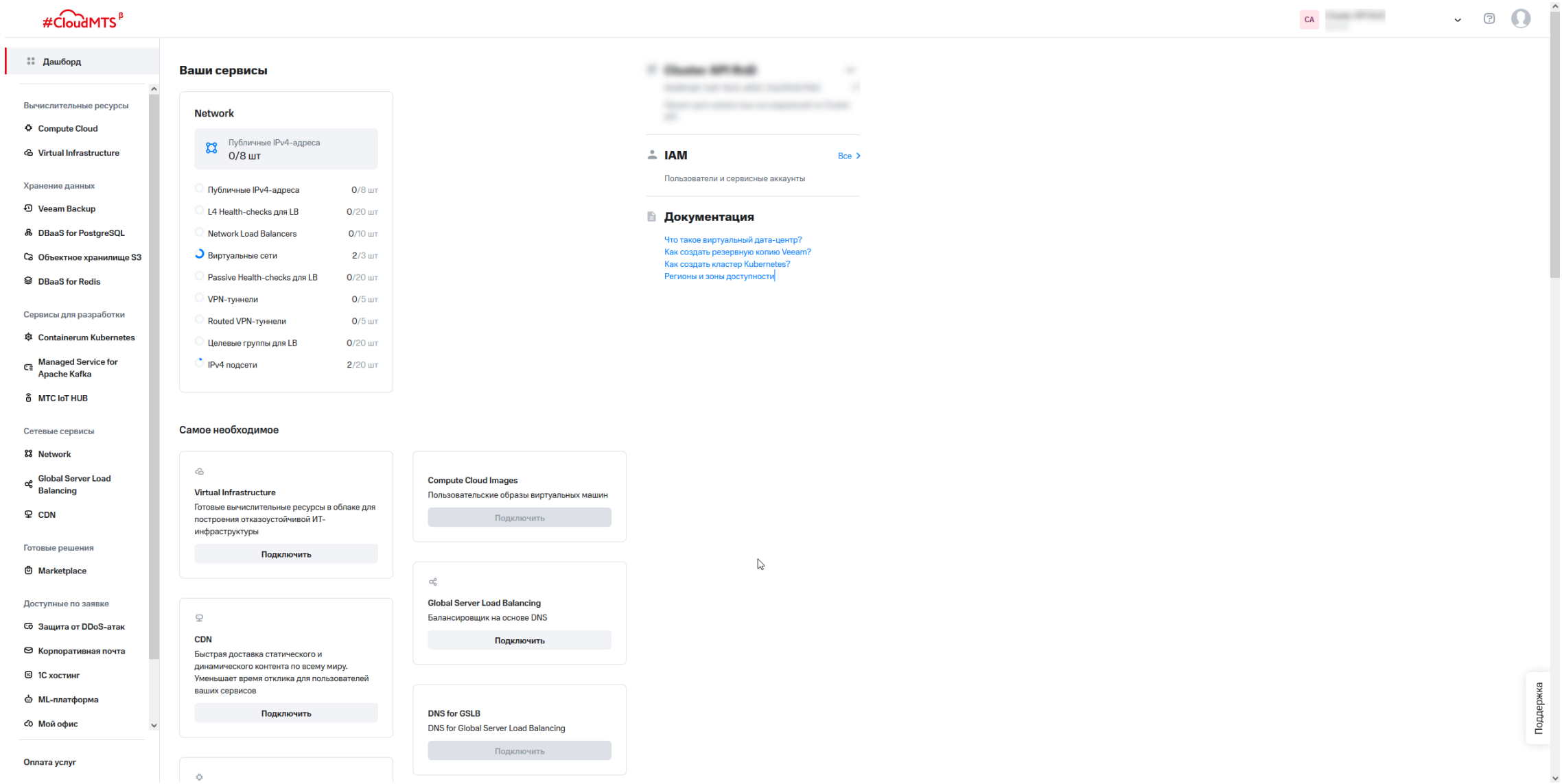
Занимаюсь развитием и поддержкой инфраструктуры для облачных сервисов.

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

Есть 3 кота, которые тоже охотно используют коробочные решения.

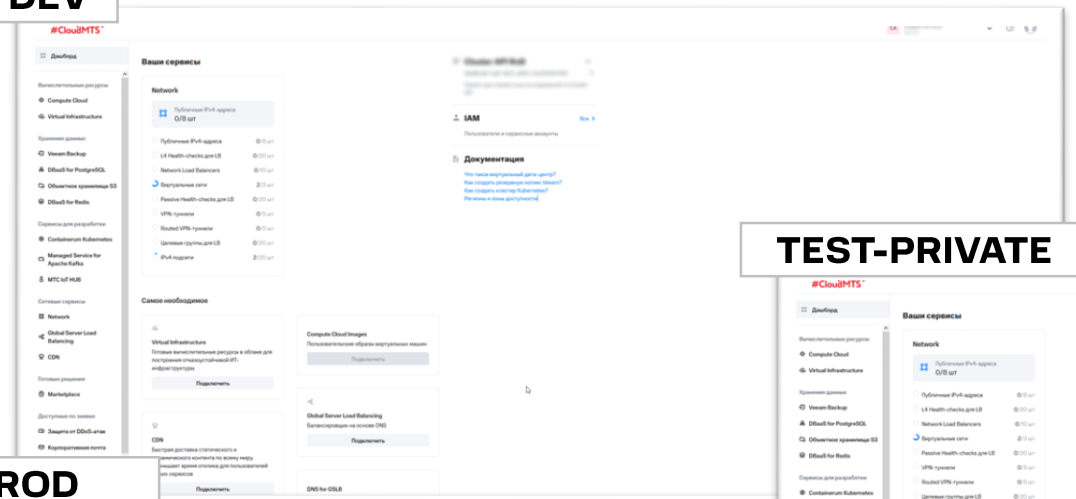
7 лет в ИТ и ещё не помер.

# Как видят облако пользователи

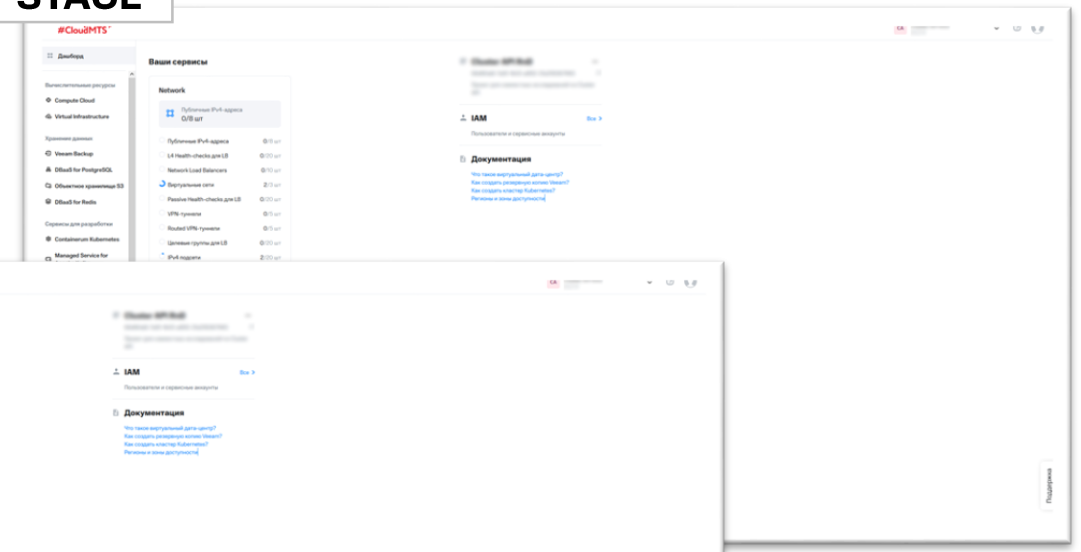


# Как видят облако разработчики

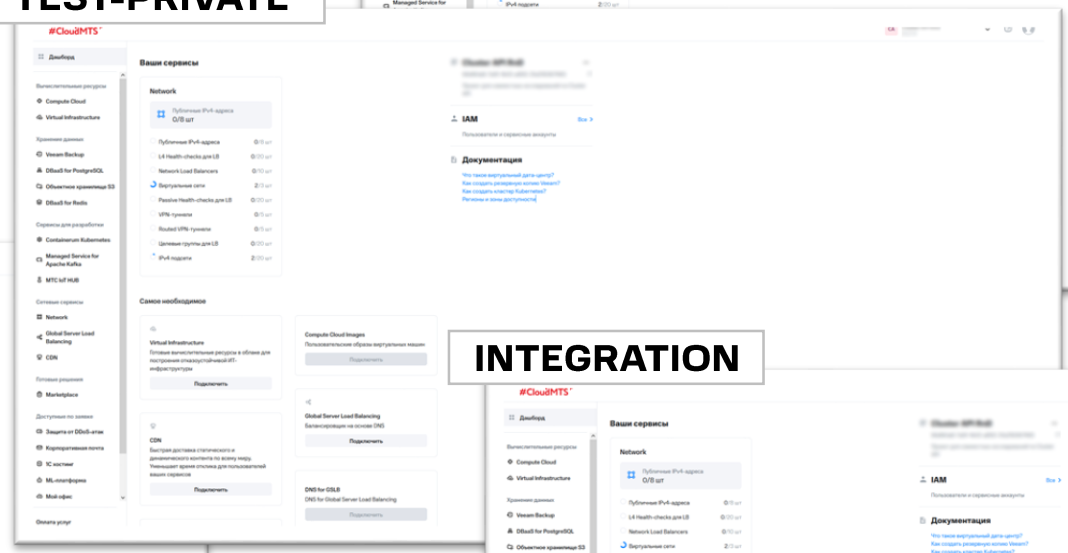
DEV



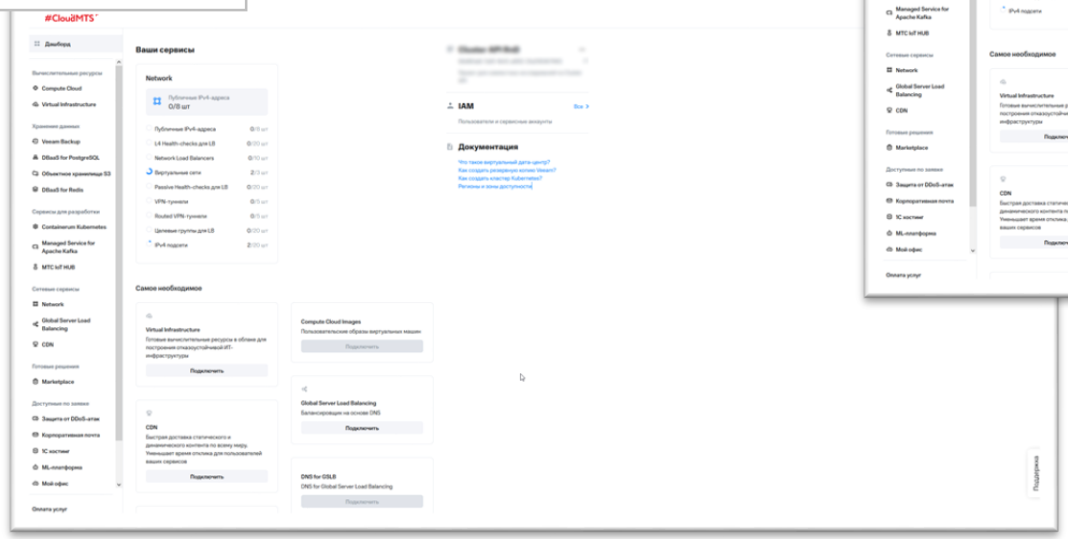
STAGE



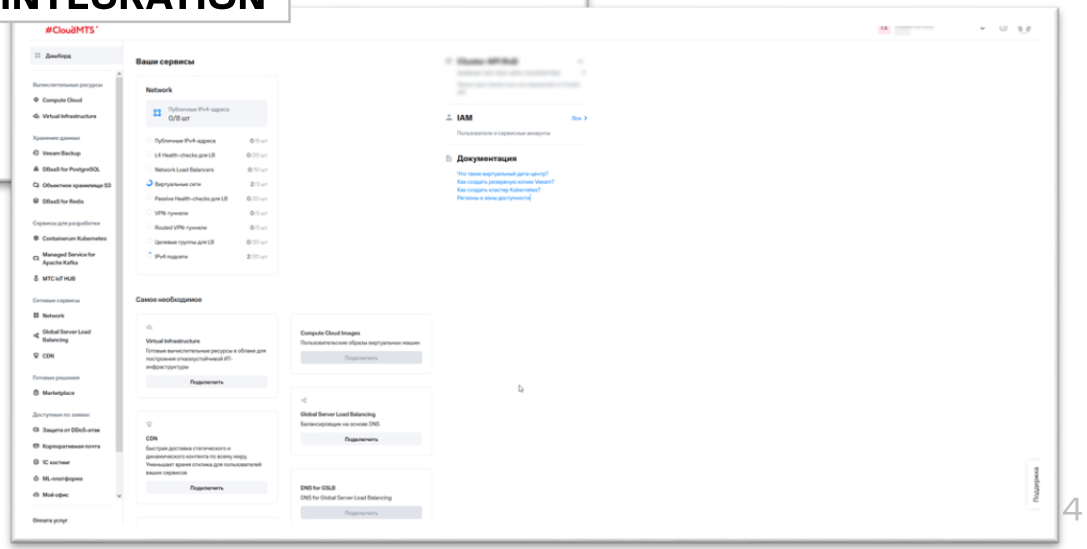
TEST-PRIVATE



PROD

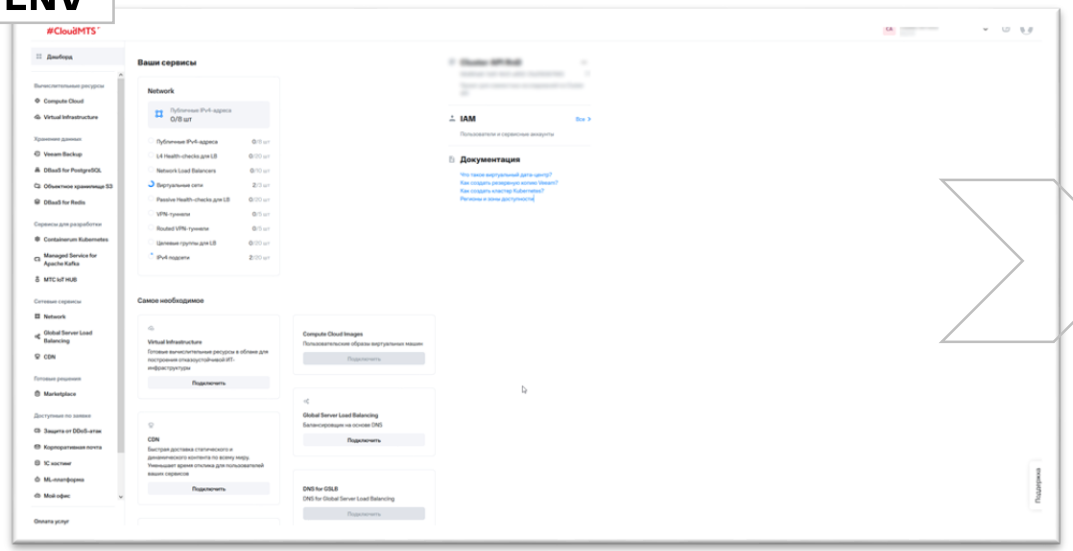


INTEGRATION



# Как видят облако SRE

**ENV**



VICTORIA METRICS

elasticsearch

fluentd

vmware NSX

kafka

vmware vSphere

mongoDB

PostgreSQL

# Этапы взросления инфраструктуры

01
Ручной привод

02
Внедрение IaC

03
Шаблонизация и структурирование IaC

04
Централизация запуска, RBAC, Аудит

to be continued....

# Проблемы при росте инфраструктуры

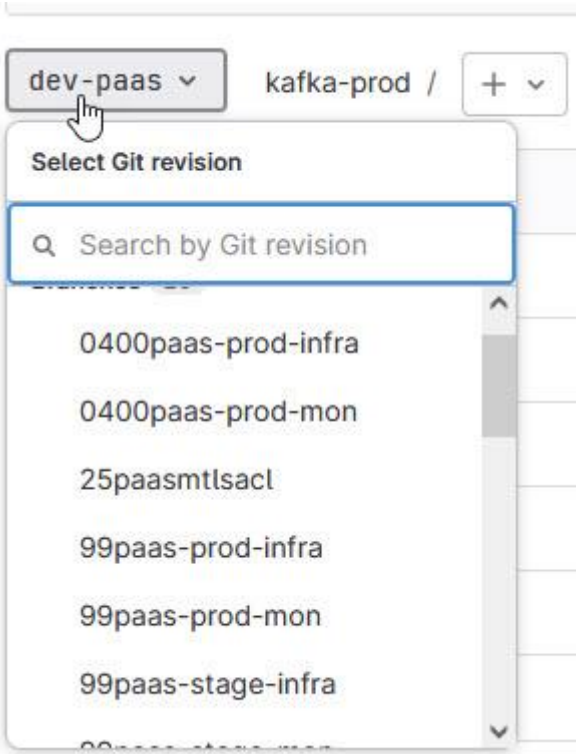
01 Бардак в git

02 Дрифт конфигов по стендам

03 Долгий и неочевидный процесс деплоя

04 Нет понимания о состоянии слоя инфраструктуры под нами

# Бардак в git




dev-paas | kafka-prod / | History | Find file | Web IDE | Clone

| Name | Last commit | Last update |
|---|---|---|
| ansible | Enabled authorizer class | 6 months ago |
| terraform | added cpu reservation | 10 months ago |
| .gitignore | refactored for paas dev | 1 year ago |
| .gitmodules | :hummer: confluent kafka как модуль | 1 year ago |
| readme.MD | cleanup | 1 year ago |
| variables.yml | added cpu reservation | 10 months ago |

**readme.MD**

### Установка kafka от confluent.

В ./terraform - опсиание виртуальных машин и генерация инветаря для ansible. в ./ansible - необходимые плейбуки.

запускать terraform-ом, в нем "обертка" для запуска ansible.

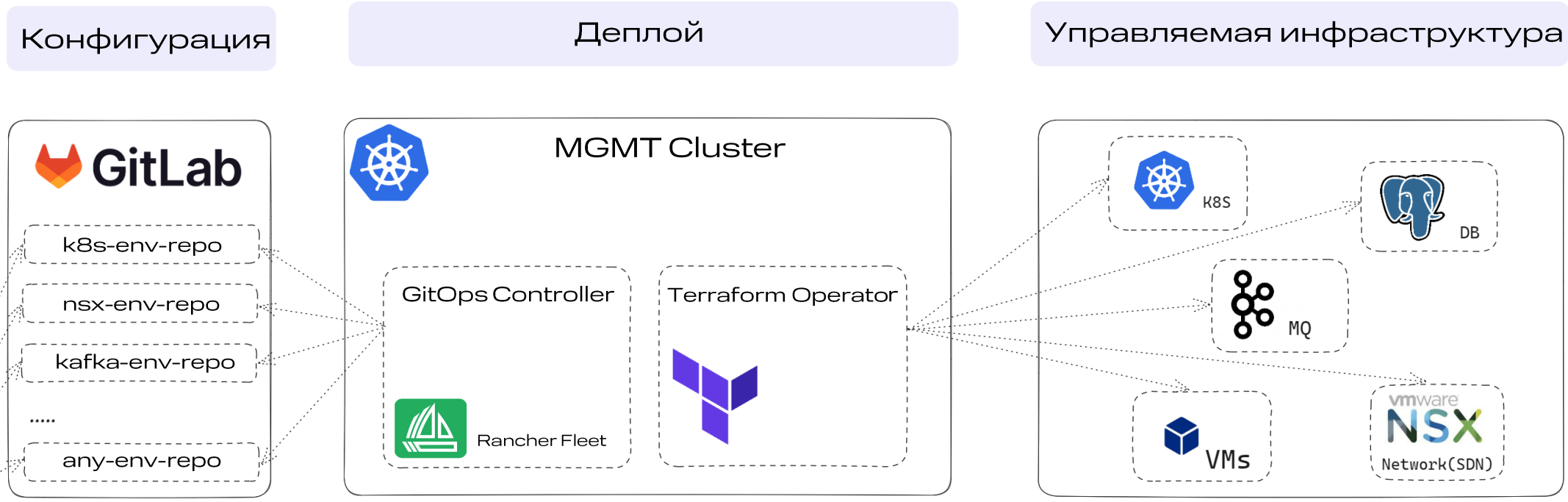
```
cd ./terraform && terraform apply
```

после создать коннетктоpы к kafka из ./ansible/configure-connectors

# Принятые конвенты

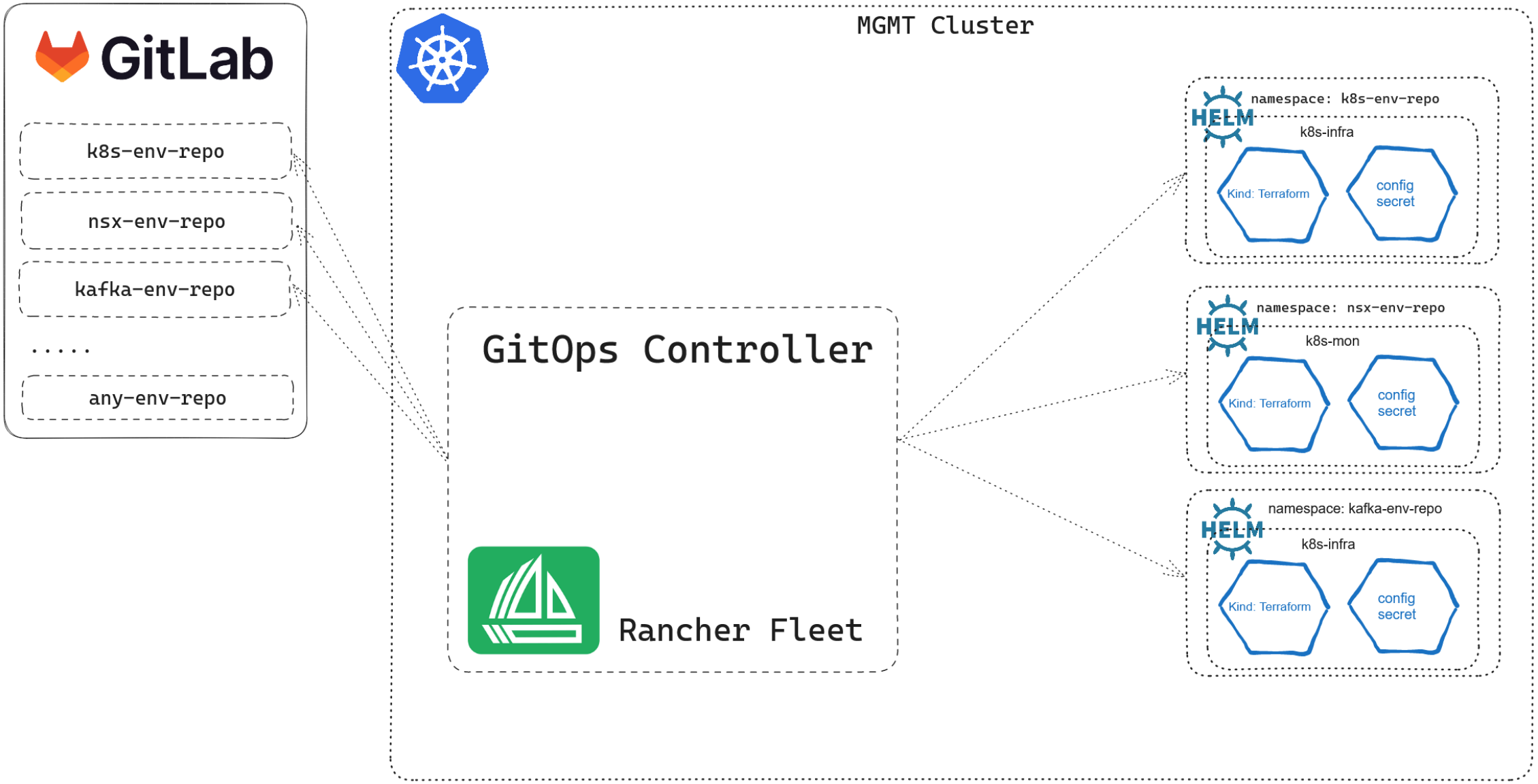
- DRY
- Общая схема деплоя для любого компонента инфраструктуры
- GitOps
- Запуск деплоя строго в 1 месте - mgmt k8s

# Платформа деплоя

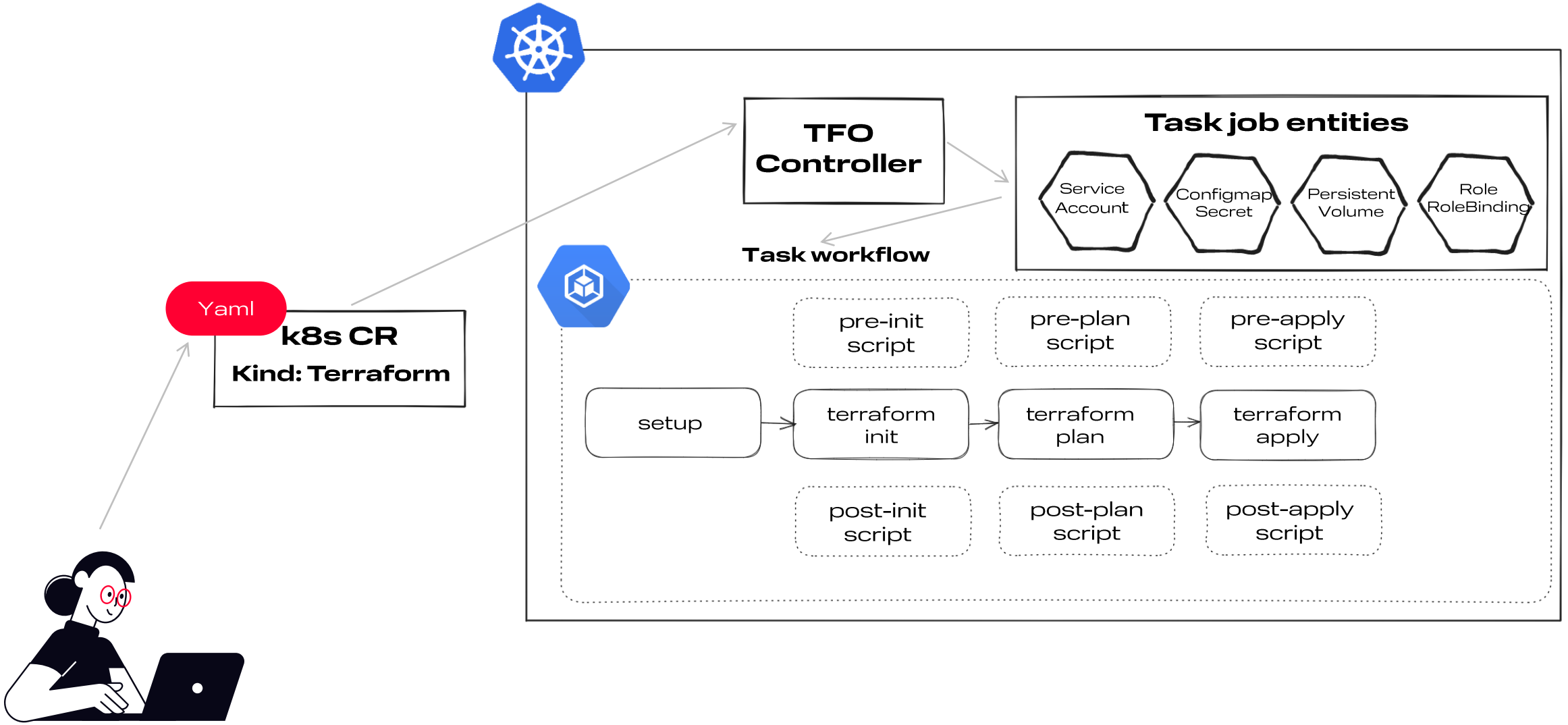



SRE
DBA
NetOps

# GitOps flow


GitLab
k8s-env-repo
nsx-env-repo
kafka-env-repo
.....
any-env-repo
MGMT Cluster
GitOps Controller
Rancher Fleet
namespace: k8s-env-repo
HELM
k8s-infra
Kind: Terraform
config
secret
namespace: nsx-env-repo
HELM
k8s-mon
Kind: Terraform
config
secret
namespace: kafka-env-repo
HELM
k8s-infra
Kind: Terraform
config
secret

# Tf-operator


TFO Controller
Task job entities
Service Account
Configmap Secret
Persistent Volume
Role RoleBinding
Task workflow
Yaml
k8s CR
Kind: Terraform
pre-init script
pre-plan script
pre-apply script
setup
terraform init
terraform plan
terraform apply
post-init script
post-plan script
post-apply script

# Env репозиторий

- Конфигурация
- Упаковка
- Доставка



k8s-environments › msk-avntg-paas-dev › msk-avg-dev-paas-mgmt

M **msk-avg-dev-paas-mgmt**

Project ID: 1680

Star 0 Fork 0

346 Commits 1 Branch 0 Tags 3 MB Project Storage

422201c7

master msk-avg-dev-paas-mgmt / Find file Web IDE Clone

README Add LICENSE Add CHANGELOG Add CONTRIBUTING Add Kubernetes cluster Set up CI/CD

Add Wiki Configure Integrations

| Name | Last commit | Last update |
|---|---|---|
| clusters | [redacted] | 50 minutes ago |
| common | victoriametrics to v1.11.21 | 3 months ago |
| core | name fix | 3 months ago |
| loadbalancers | add gloo-cr | 3 months ago |
| .gitignore | Add ext cluster | 3 months ago |
| Readme.md | Update Readme.md | 3 months ago |
| variables.yml | Update helm | 1 week ago |

**Readme.md**

[redacted]

http://tf.isaaguilar.com/docs/

- Пилотный менеджмент кластер для tf-operator
- Пререквизиты
- Инициализация управляющего кластера
- Инициализация управляемых кластеров (infra, mon, ext...)
- Удаление управляемых кластеров
- Удаление управляющего кластера
- Модификация управляемых кластеров
- FAQ

## Пререквизиты

- Готовая репа с настройкой окружения в https://git.dev.cloud.mts.ru/k8s-environments см.документацию из https://git.dev.cloud.mts.ru/infrastructure/rke-k8s-pilot/-/tree/main/docs
- Все связанное с запуском непосредственно кластера находится в https://git.dev.cloud.mts.ru/k8s-environments/msk-avntg-

# Структура env репозитория

**core**

Деплой в куб (must)

1. Istio
2. Vsphere CSI
3. OIDC Bundle
4. OPA

**clusters**

Инфраструктурные релизы

1. k8s
2. kafka
3. opendistro
4. VM's
5. ...

**variables.yml**

Деплой куба

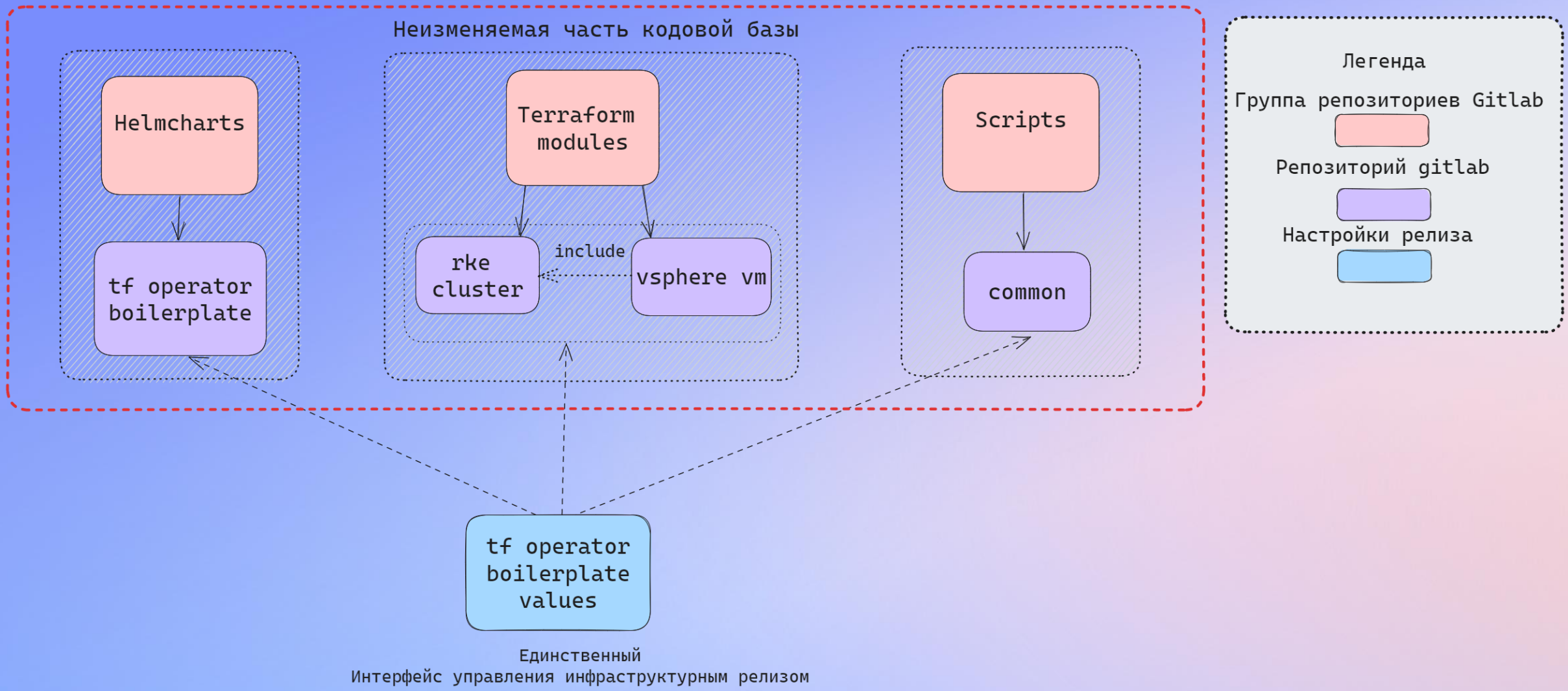
1. BM'ки
2. RKE
3. CNI
4. Fleet

**common**

Деплой в куб (may)

1. Ком-ты мониторинга
2. ком-ты логирования
3. gitlab раннеры
4. операторы
5. ....

# Устройство релиза



# Содержимое релиза

```yaml
terraformVersion: "1.4.6"

requireApproval: true
keepLatestPodsOnly: true
keepCompletedPods: false
ignoreDelete: false

terraformModule:
  source: git@git.dev.cloud.mts.ru:infrastructure/terraform/rke-cluster.git
  version: v0.1.0


backend: |-···

taskOptions:
  - for: ["setup"]
    script:
      source: "https://git.dev.cloud.mts.ru/pub/terraform-operator-tasks/-/raw/master/setup.sh"

  - for: ["preinit"]···

  - for:
      [
        "init",
        "plan",
        "apply",
        "init-delete",
        "plan-delete",
        "apply-delete",
      ]
    env:
      - name: TF_VAR_GITLAB_CLUSTER_TEMPLATE_PRJ_ID
        value: "1016"
      - name: TF_VAR_GITLAB_CLUSTER_TEMPLATE_REF
        value: "v2.0.1"
      - name: TF_VAR_GITLAB_CLUSTER_TEMPLATE_NAME
        value: "common/kube-1.21/default.yaml"
      - name: TF_VAR_GITLAB_ENVIRONMENT_VARS_PRJ_ID
        value: "1831"
      - name: TF_VAR_GITLAB_ENVIRONMENT_VARS_REF
        value: "master"
```

# TF Common

```yaml
terraformVersion: "1.4.6"

terraformModule:
  source: git@git.dev.cloud.mts.ru:infrastructure/terraform/rke-cluster.git
  version: v0.1.0


backend: |-
  terraform {
    backend "kubernetes" {
      secret_suffix    = "msk-avg-stg-paas-k8s-yktest"
      in_cluster_config  = true
      namespace = "msk-avg-stg-paas-k8s-yktest"
    }
  }
```

# Flow control

```
requireApproval: true

keepLatestPodsOnly: true

keepCompletedPods: false

ignoreDelete: false
```

# TF ENV

```
- for:
    [
      "init",
      "plan",
      "apply",
      "init-delete",
      "plan-delete",
      "apply-delete",
    ]
  env:
    - name: TF_VAR_GITLAB_CLUSTER_TEMPLATE_PRJ_ID
      value: "1016"
    - name: TF_VAR_GITLAB_CLUSTER_TEMPLATE_REF
      value: "v2.0.1"
    - name: TF_VAR_GITLAB_CLUSTER_TEMPLATE_NAME
      value: "common/kube-1.21/default.yaml"
    - name: TF_VAR_GITLAB_ENVIRONMENT_VARS_PRJ_ID
      value: "1831"
    - name: TF_VAR_GITLAB_ENVIRONMENT_VARS_REF
      value: "master"
```

# TF Hook

```
taskOptions:
  - for: ["setup"]
    script:
      source: "https://git.dev.cloud.mts.ru/pub/terraform-operator-tasks/-/raw/master/setup.sh"

  - for: ["preinit"]···

  - for:···


  - for: ["postapply"]
    script:
      inline: |-
        wget https://nexus.dev.cloud.mts.ru/repository/containerum-binaries/kubectl/kubectl-v1.24.6 -O $HOME/kubectl
        chmod +x $HOME/kubectl
        kubectl get secret tfstate-default-msk-avg-stg-paas-k8s-yktest -n msk-avg-stg-paas-k8s-yktest -o json | jq -r '.data.tfstate' | base64 -d | gzip -d > $HOME/tmpstate
        cat $HOME/tmpstate | jq -r '.outputs.rkestate.value.kube_config_yaml' > $HOME/kubeconfig
        kubectl -n msk-avg-stg-paas-k8s-yktest delete secret msk-avg-stg-paas-k8s-yktest-kubeconfig >> /dev/null || true
        kubectl -n msk-avg-stg-paas-k8s-yktest create secret generic --from-file $HOME/kubeconfig msk-avg-stg-paas-k8s-yktest-kubeconfig
```

# Зачем нам здесь GitOps

- Единый формат релиза
- Единый flow запуска деплоя
- Единая точка управления
- Наглядная история изменений

| | | |
|---|---|---|
| msk-avg-dev-paas-es | Changed msk-avg-dev-paas-es/fleet.yaml | 1 month ago |
| msk-avg-dev-paas-k8s-capi-helm | Cldevops 818 capi | 3 weeks ago |
| msk-avg-dev-paas-k8s-capi-rke | Cldevops 818 capi | 3 weeks ago |
| msk-avg-dev-paas-k8s-ext-helm | CLDEVOPS-818 Обновление ext кластера | 3 weeks ago |
| msk-avg-dev-paas-k8s-ext-rke | CLDEVOPS-818 Обновление ext кластера | 3 weeks ago |
| msk-avg-dev-paas-k8s-infra-helm | CLDEVOPS-816 Подготовка под flatcar | 3 weeks ago |
| msk-avg-dev-paas-k8s-infra-rke | CLDEVOPS-816 Подготовка под flatcar | 3 weeks ago |
| msk-avg-dev-paas-k8s-mgmt-helm | Disable auto install | 2 months ago |
| msk-avg-dev-paas-k8s-mgmt-rke | up ver tf for mgmt | 1 month ago |
| msk-avg-dev-paas-k8s-mon-helm | update path dir | 1 month ago |
| msk-avg-dev-paas-k8s-mon-rke | Migrate mon cluster to flatcar | 1 month ago |
| msk-avg-dev-paas-k8s-yk-csi-helm | add yk k8s for csi tests | 1 week ago |
| msk-avg-dev-paas-k8s-yk-csi-rke | upd vc creds | 1 week ago |
| msk-avg-dev-paas-k8s-yk-fc-helm | upd helm | 2 weeks ago |
| msk-avg-dev-paas-k8s-yk-fc-rke | upd to 1.23 k8s | 1 week ago |
| msk-avg-dev-paas-kafka-infra | Added msk-avg-dev-paas-kafka-infra/fleet.yaml | 2 months ago |
| msk-avg-dev-paas-kafka-mon | Changed msk-avg-dev-paas-kafka-mon/fleet.yaml | 2 months ago |
| msk-avg-dev-paas-lb-internal | tf ver chg | 1 month ago |
| msk-avg-dev-paas-nsx-fw | empty commit to upd | 1 week ago |
| msk-avg-dev-paas-nsx-infra | typo fix (CLDEVOPS-851) | 1 week ago |
| msk-avg-dev-paas-nsx-inv | add sg for dbaas client backup (NETWORK-1114) | 2 days ago |
| msk-avg-dev-slkr-k8s-infra-helm | msk-avg-dev-slkr-k8s-infra-helm/fleet.yaml | 1 month ago |
| msk-avg-dev-slkr-k8s-infra-rke | Changed IPs and needs rerun tf-operator | 1 month ago |

# Полный flow деплоя

01
Создать env репозиторий

02
Сконфигурировать в env репе variables.yml
Gitops манифесты

03
Добавить fleet.yml в mgmt. Репозиторий x2

04
Tf-operator запускает деплой в mgmt кластере

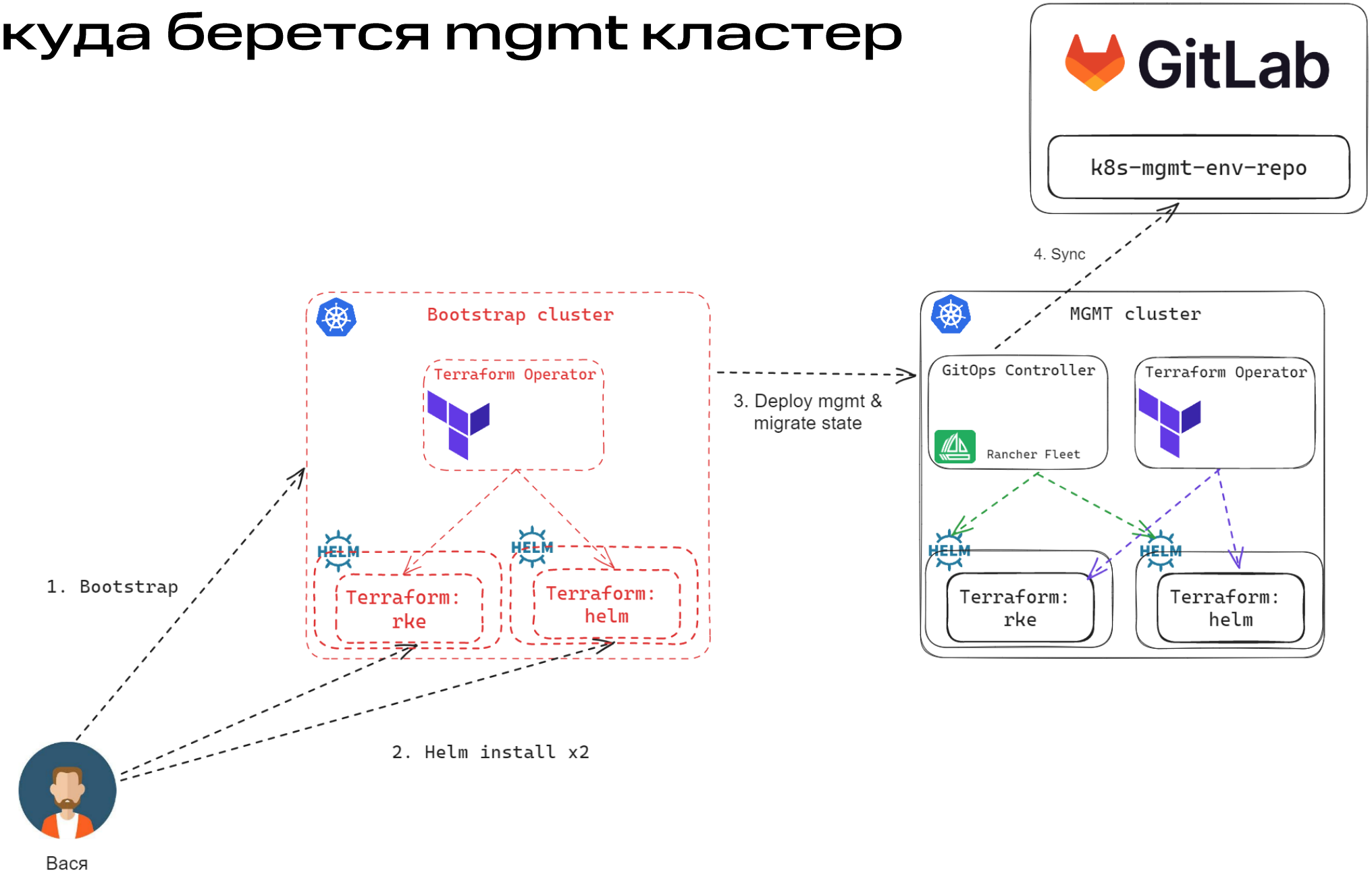
05
Постинициализация BM через Ignition

06
Деплой куба через rke

07
Деплой fleet контроллера в развернутый кластер

08
Деплой helm чартов

# Откуда берется mgmt кластер

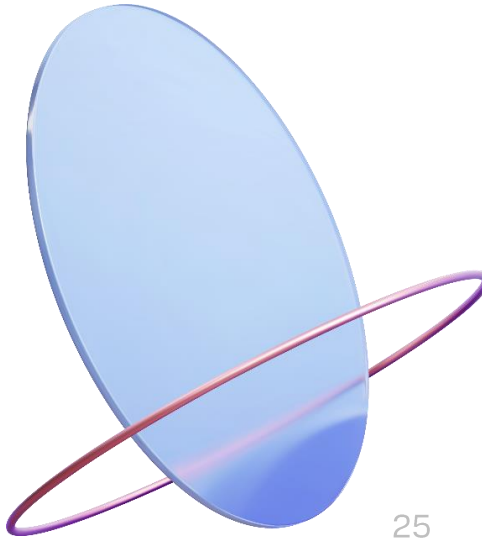


# Защищаем mgmt кластер

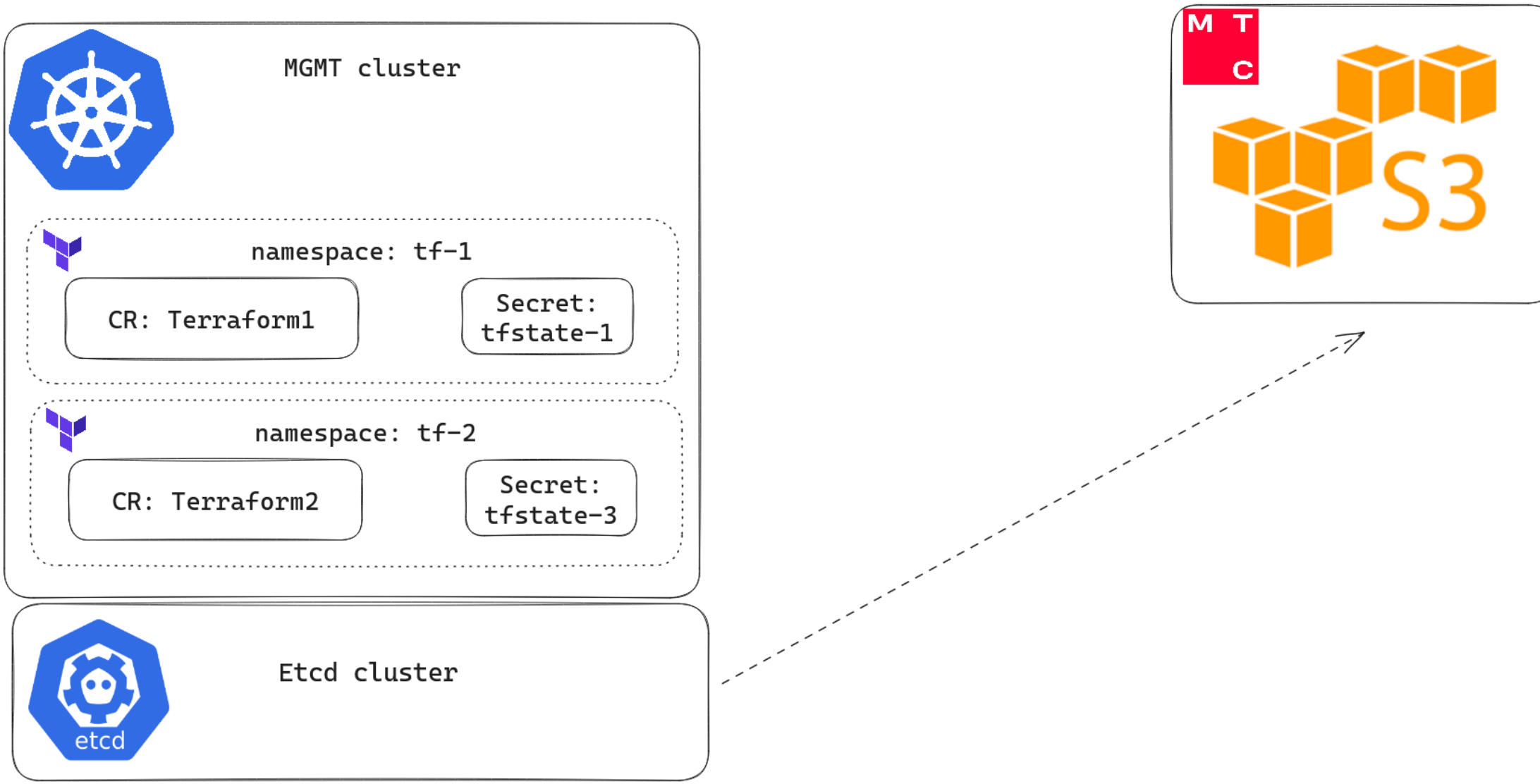
- Блокировка удаления ключевых CR через Open Policy Agent
- Дополнительная защита от дурака на terraform ресурсах (ignoreDelete, блокировки на уровне state, запуск строго через requireApproval)
- Дополнительные DR планы

# DR

- Ресурсы в mgmt k8s целы, ресурсы на виртуализации утеряны
- Утеряны ресурсы в mgmt k8s
- Утерян mgmt k8s



# Бекап mgmt


MGMT cluster
namespace: tf-1
CR: Terraform1
Secret: tfstate-1
namespace: tf-2
CR: Terraform2
Secret: tfstate-3
Etcd cluster
etcd
S3

# Что в итоге получили

- Структурируемое хранение тела IaC
- Ускорение TtM инфраструктуры
- Наглядность
- Единый стандарт и инструмент для управления инфрой для всех команд
- Единая точка правды и управления всей инфраструктурой региона

# Недостатки

- Много врапперов = сложнее дебаг
- Относительно высокий порог входа
- Довольно сильная завязка на terraform

# Планы по развитию

- CLI
- Деплой на baremetal
- Интеграция с Cluster API
- Интеграция с Crossplane

# СПАСИБО ЗА ВНИМНАИЕ

ИВАН ГУЛАКОВ
https://t.me/kepiukik