Security

Безопасное развёртывание контейнерных приложений

Алексей Миртов, Yandex.Cloud
Любовь Гринкевич, Yandex.Cloud

О чем доклад

- Какие есть проблемы безопасности в стандартном процессе деплоя
- Как от них защищаться, если ты devops
- Почему нельзя закрыть проблемы раз и навсегда

Введение: pipeline-разработки

Схема разработки

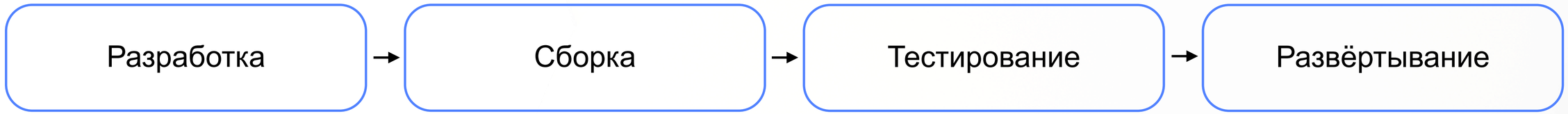


Схема контейнерной разработки

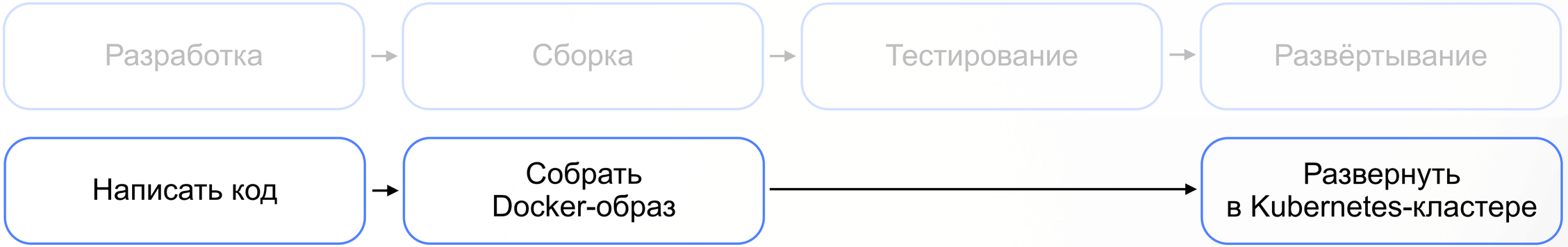


Схема контейнерной разработки

Application Pipeline

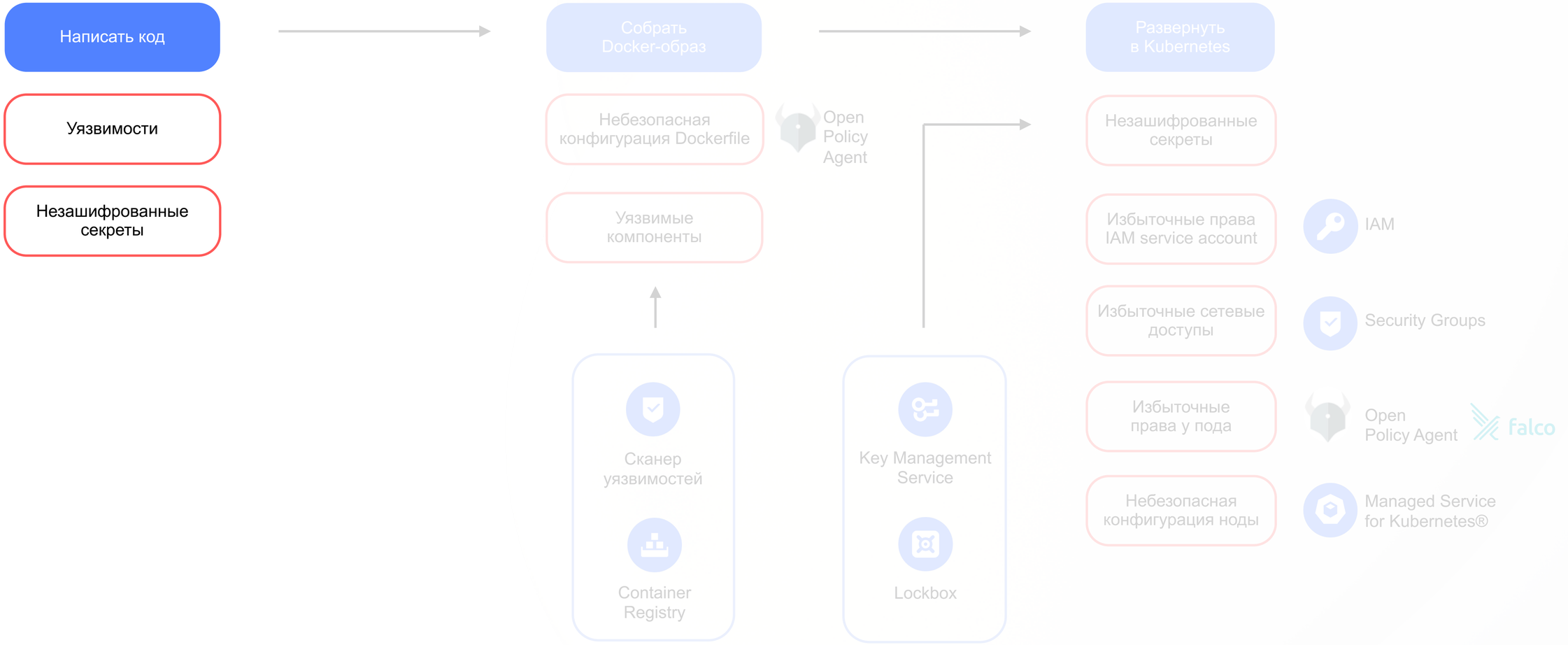


Схема контейнерной разработки

Application Pipeline

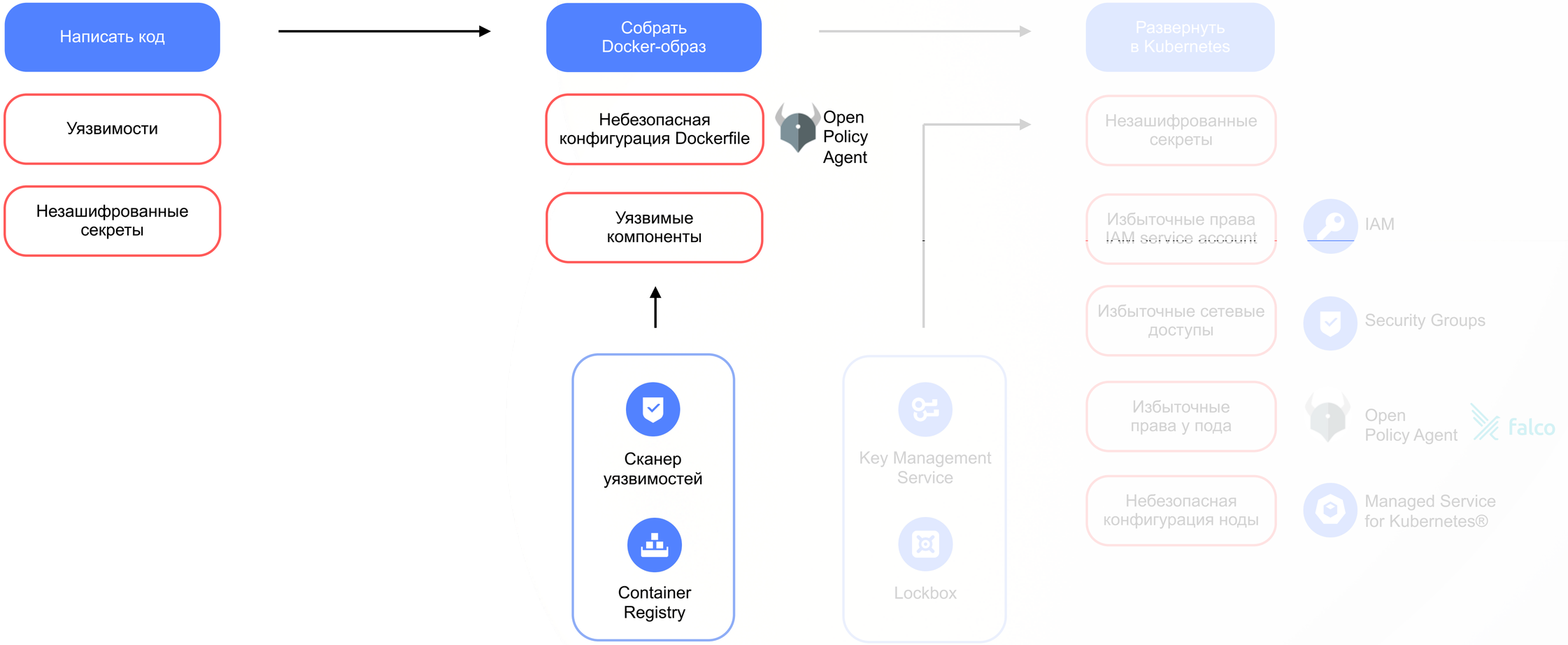
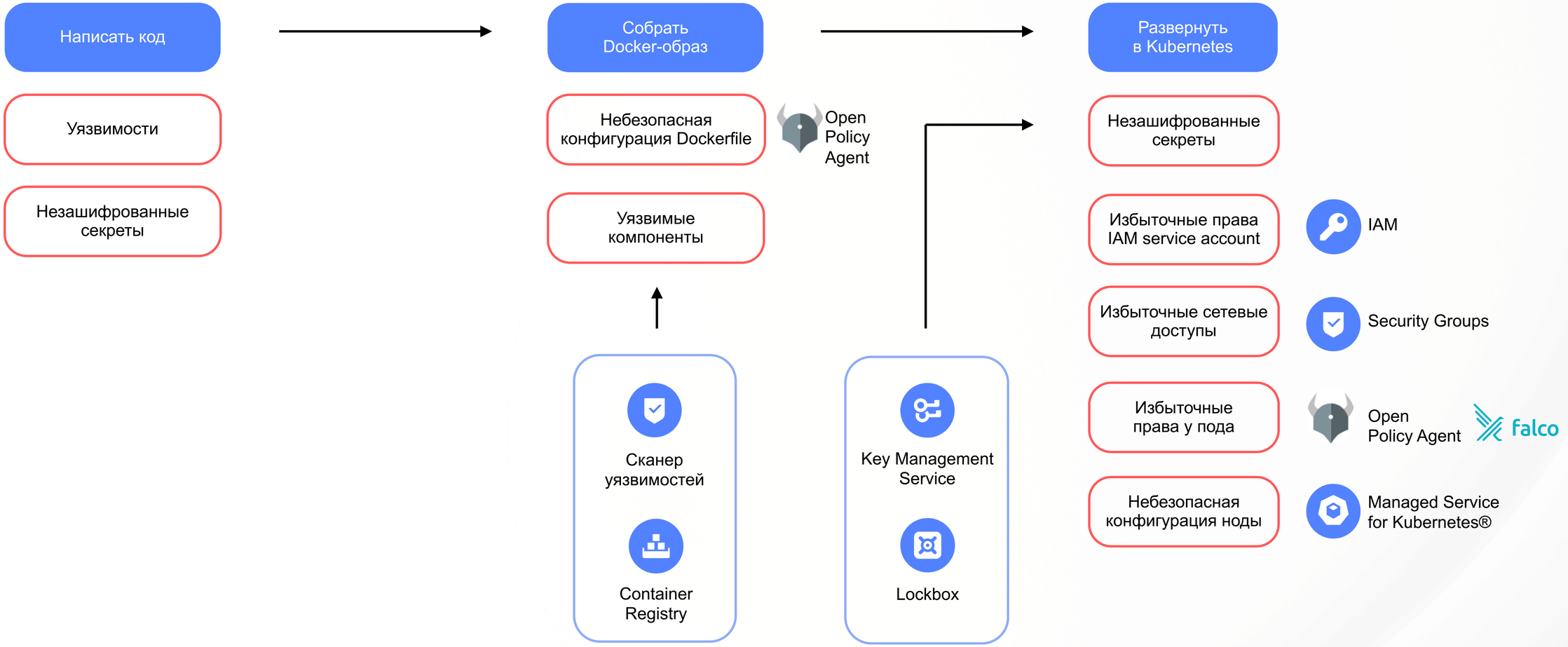


Схема контейнерной разработки

Application Pipeline



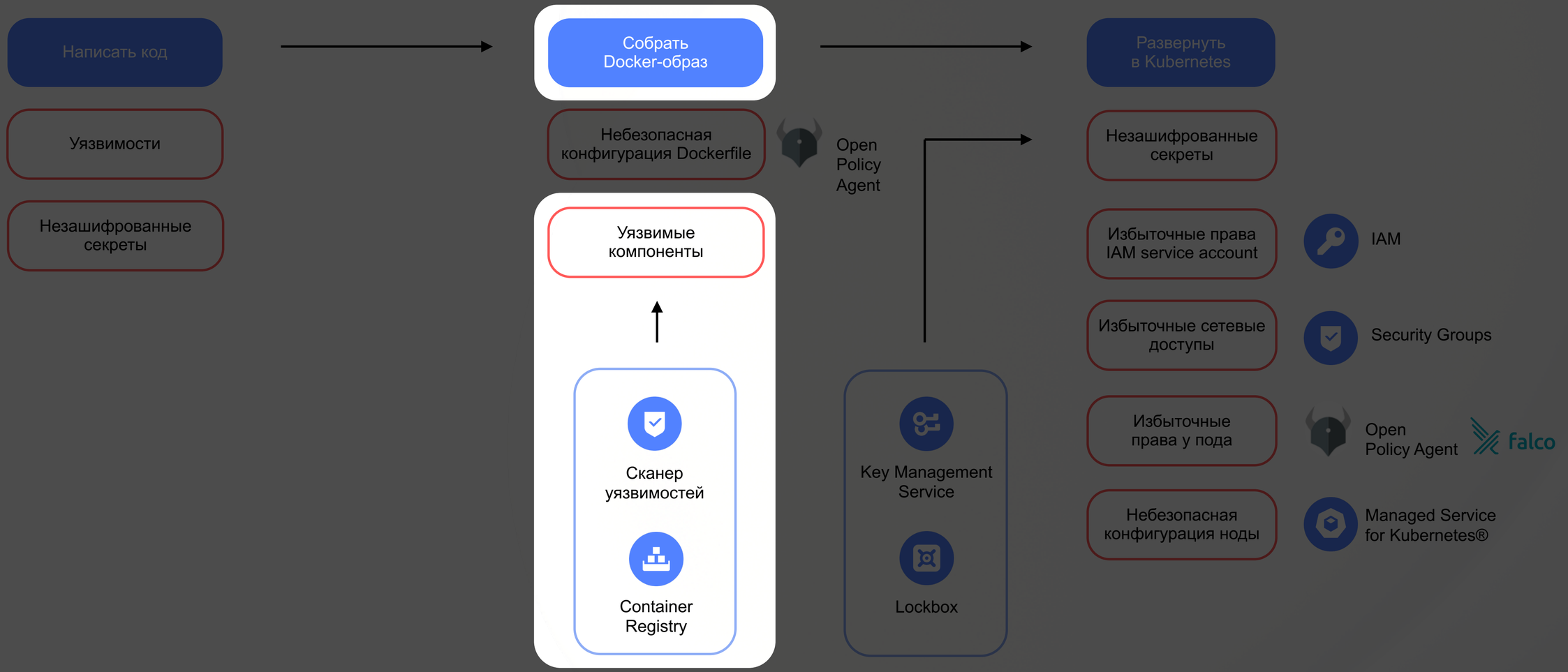
План презентации

1. Введение: pipeline-разработки
2. Уязвимые компоненты в Docker-образе
3. Небезопасная конфигурация образа
4. Kubernetes Secrets
5. Избыточные права или сетевые доступы
6. Аномальное поведение или отсутствие контроля
7. Обновления Kubernetes-нод
8. Выводы

Уязвимые компоненты в Docker-образе

Схема контейнерной разработки

Application Pipeline



Аська и Васька

Files · master · Admini | 62.84.121.121

http://130.193.55.160/root/secure-pipeline/-/tree/master

Reviews

Yandex.Cloud

Other Bookmarks

GitLab | Projects | Groups | More | Search or jump to...

S secure-pipeline

- Project overview
- Repository
  - Files
  - Commits
  - Branches
  - Tags
  - Contributors
  - Graph
  - Compare
- Issues 0
- Merge Requests 3
- CI / CD
- Operations
- Packages & Registries

Open registration is enabled on your instance.

Learn more about how you can customize / disable registration on your instance.

View setting

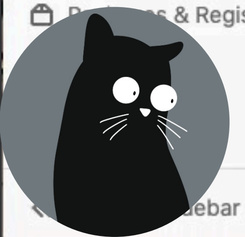
Administrator › secure-pipeline › **Repository**

master | secure-pipeline / | History | Find file | Web IDE | Clone

fix
Administrator authored 6 days ago

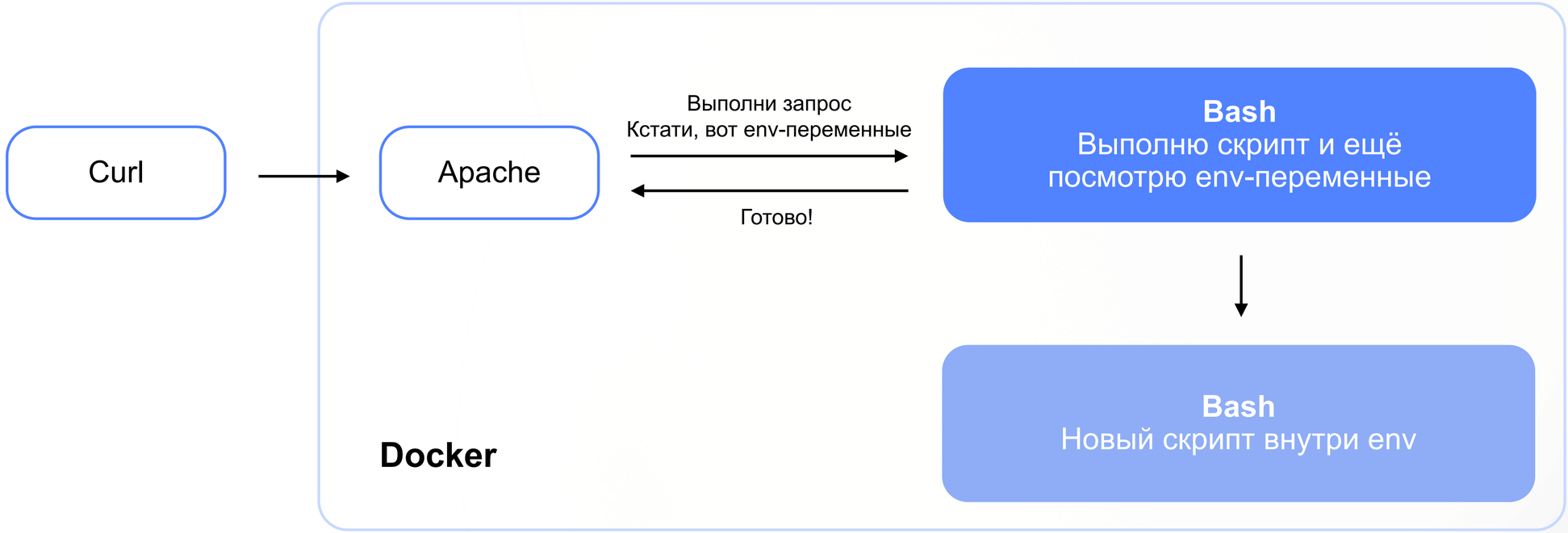
b6f46032

Name	Last commit	Last update
.gitlab-ci.yml	fix	6 days ago
Dockerfile	Build and deploy server	1 week ago
gitlabStepDockerfile	Build and deploy server	1 week ago
index.html	Build and deploy server	1 week ago
k8s.yaml	Update k8s.yaml by real image	6 days ago
my-very-important-script.sh	Build and deploy server	1 week ago
virtual-host.conf	Build and deploy server	1 week ago



Уязвимые компоненты в Docker-образе

Shellshock



Merge Requests · Adm

http://130.193.55.160/root/secure-pipeline/-/merge_requests

Reviews

Yandex.Cloud

Other Bookmarks

GitLab Projects Groups More Search or jump to...

S secure-pipeline

- Project overview
- Repository
- Issues 0
- Merge Requests 3
- CI / CD
- Operations
- Packages & Registries
- Analytics
- Wiki
- Snippets
- Members
- Settings

Open registration is enabled on your instance.

Learn more about how you can customize / disable registration on your instance.

View setting

Administrator › secure-pipeline › Merge Requests

Open 3 Merged 0 Closed 1 All 4

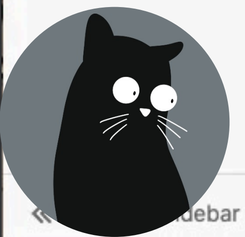
Edit merge requests New merge request

Recent searches Search or filter results... Created date

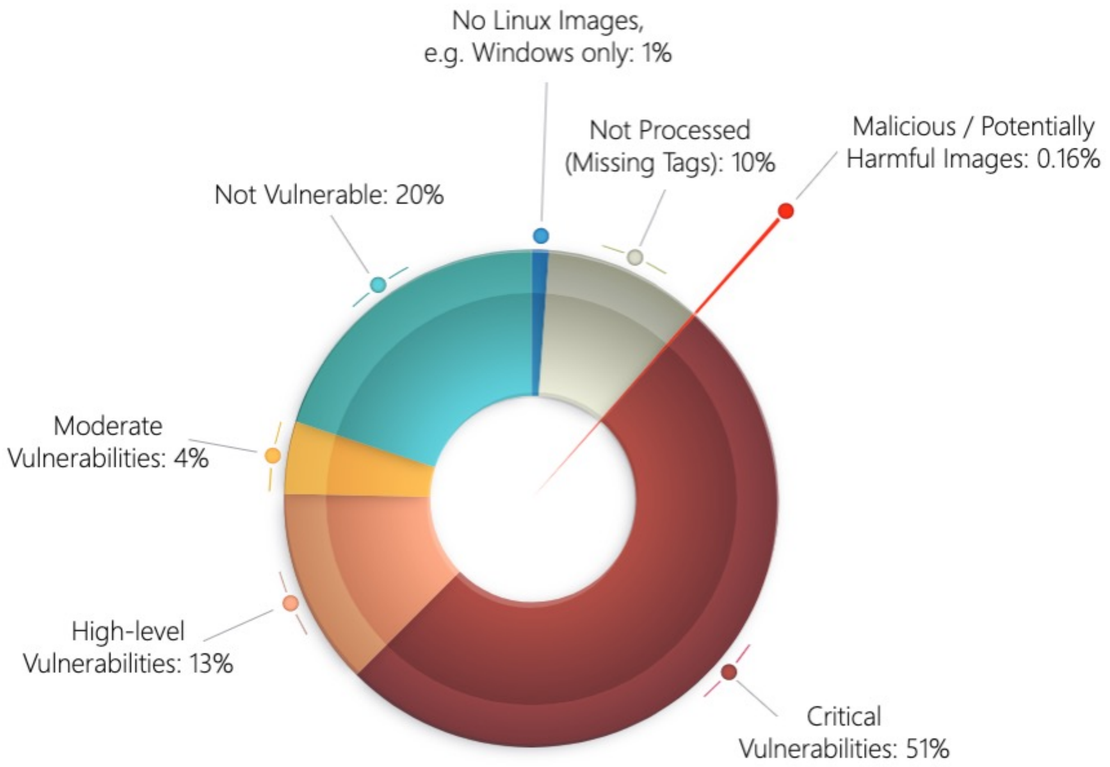
Check dockerfiles before build
!4 · opened 1 week ago by Administrator `fix-vulns`
0 updated 1 week ago

Fix vulnerabilities by updating packages
!3 · opened 1 week ago by Administrator `scan-image`
0 updated 1 week ago

Scan image before deploy
!2 · opened 1 week ago by Administrator
0 updated 1 week ago



Безопасность базовых образов



Prevasio Pty Ltd | https://prevasio.com | Copyright © 2020 All Rights Reserved

Статистика уязвимостей в 4M образах с Docker Hub на 2020 год по версии компании Prevasio

https://clck.ru/YcCN2

Защита Docker-образа: сканирование

On-premise

- Aqua Security
- Clair
- Anchore
- JFrog Xray

Managed

- Snyk (docker image scan)
- Qualys
- GCP
- Yandex.Cloud
- Azure (Qualys)
- AWS (Clair)

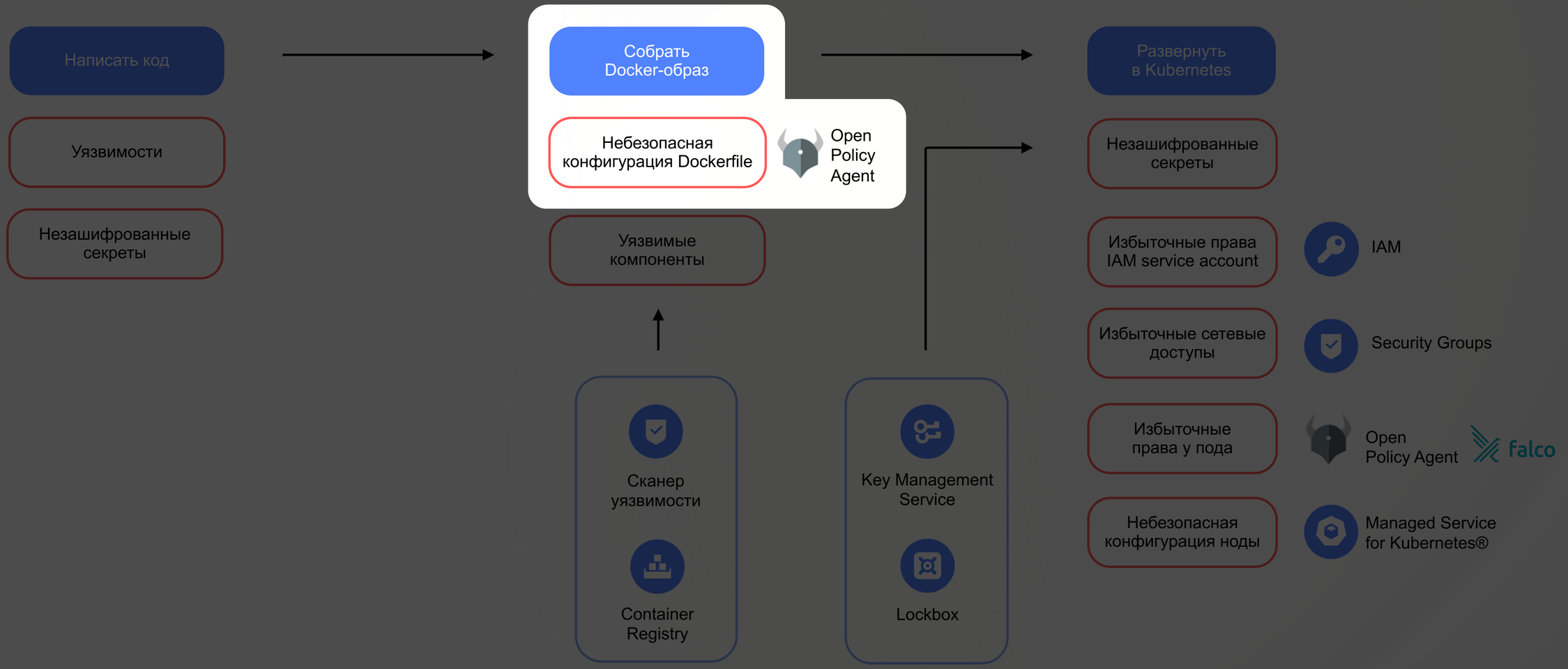
Защита Docker-образа

- Доверенные базовые образы
- Обновления пакетов
- Сканирование уязвимостей

Небезопасная конфигурация образа

Схема контейнерной разработки

Application Pipeline



Защита Docker-образа: конфигурирование

Open Policy Agent —
инструмент создания политик

Conftest —
CLI для OPA над конфигами

Merge Requests · Adm

http://130.193.55.160/root/secure-pipeline/-/merge_requests

Reviews

Yandex.Cloud

Other Bookmarks

GitLab Projects Groups More Search or jump to...

S secure-pipeline

- Project overview
- Repository
- Issues 0
- Merge Requests 3
- CI / CD
- Operations
- Packages & Registries
- Analytics
- Wiki
- Snippets
- Members
- Settings

Open registration is enabled on your instance.

Learn more about how you can customize / disable registration on your instance.

View setting

Administrator › secure-pipeline › Merge Requests

Open 3 Merged 0 Closed 1 All 4

Edit merge requests New merge request

Recent searches Search or filter results... Created date

Check dockerfiles before build
!4 · opened 1 week ago by Administrator `fix-vulns`
0 updated 1 week ago

Fix vulnerabilities by updating packages
!3 · opened 1 week ago by Administrator `scan-image`
0 updated 1 week ago

Scan image before deploy
!2 · opened 1 week ago by Administrator
0 updated 1 week ago

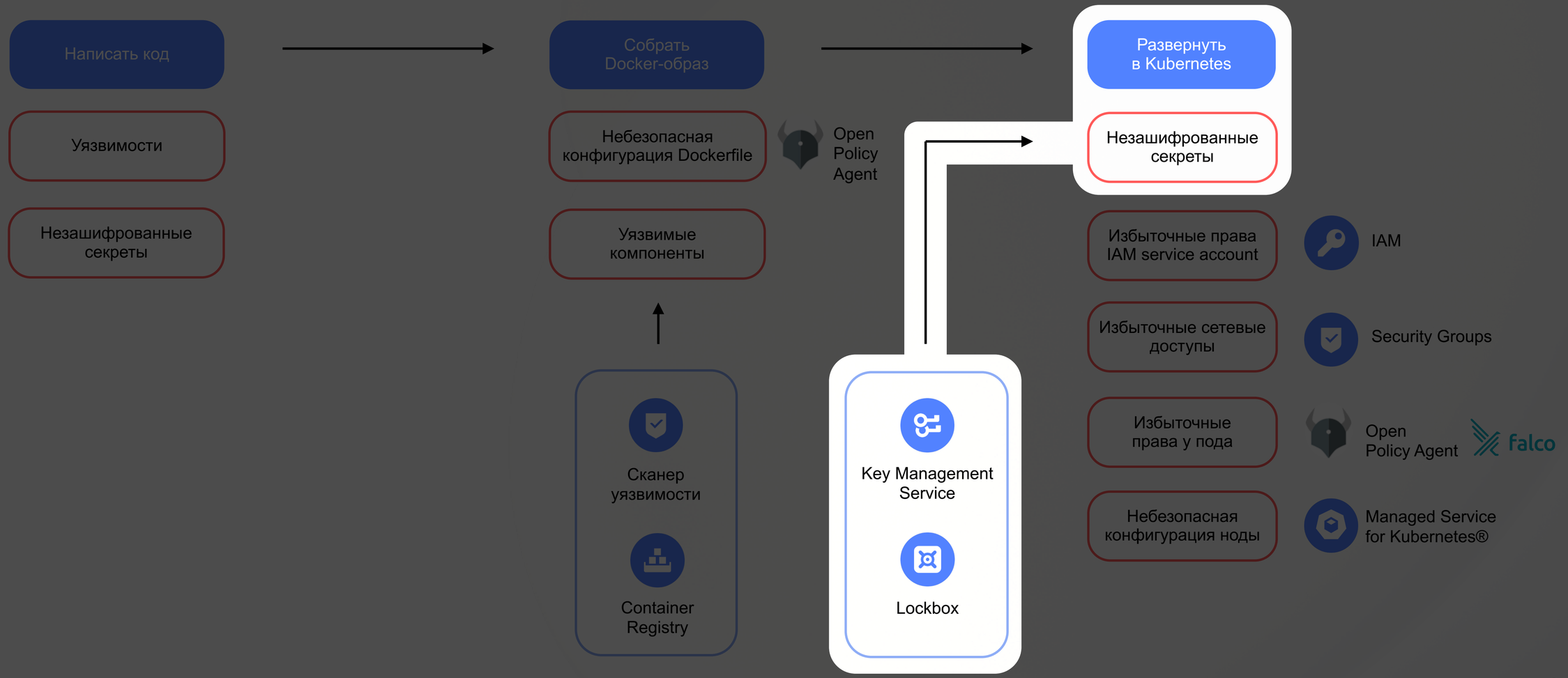
Проблемы безопасности в примере

- Образ, развернутый в хостовой сети
- Доступ к сервису метаданных кластера
- Расширенные права у сервисного аккаунта кластера

Kubernetes Secrets

Схема контейнерной разработки

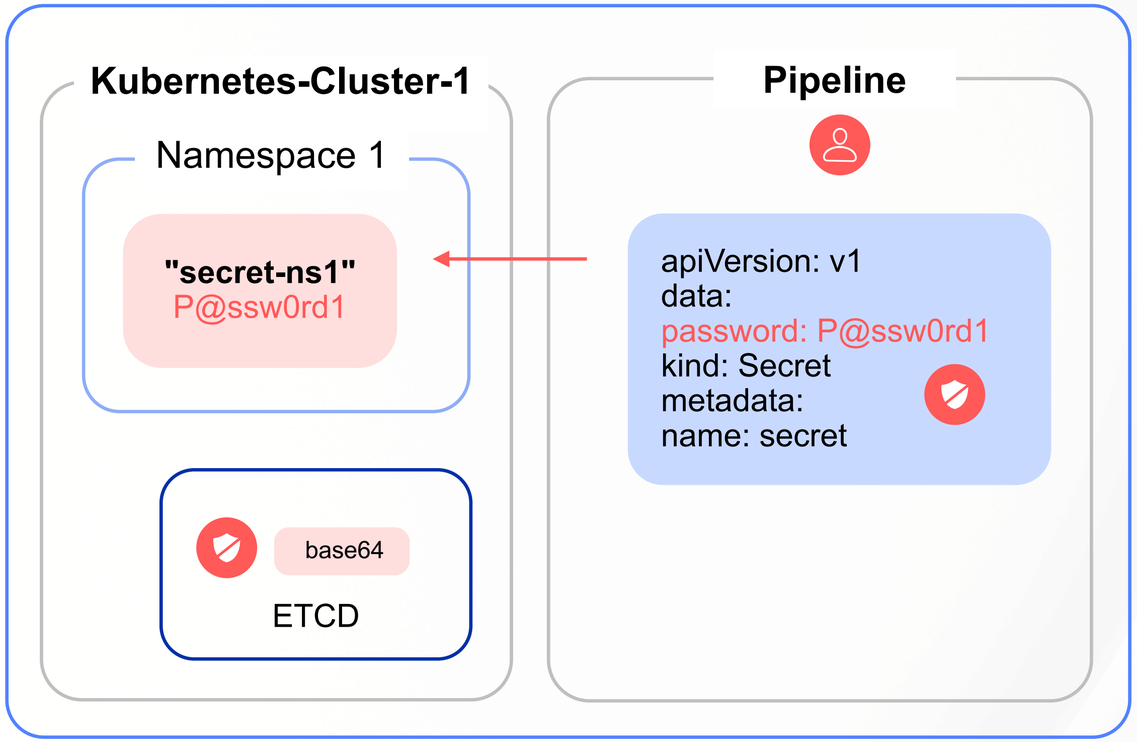
Application Pipeline



Secrets и их проблемы

Основные Проблемы

- Отображение в base64 внутри yaml манифеста (небезопасная доставка)
- Доступ на управление секретами в k8s = полный доступ ко всем секретам ns + ручные операции
- Тяжело следить за событиями (стандартные аудит логи k8s = боль)



Secret Manager

Решения:

- **Безопасная доставка секретов без yaml** (шифрование канала, аутентификация, авторизация)
- **Гранулярные доступы и группировка**
- **Единое хранилище секретов** (можно добавлять одни секреты из разных ns/clusters)
- **Версионирование**
- **Централизованный аудит** (позволяет легко получать читаемые события аудита)
- **Защита от удаления**

Известные Secrets Managers

Встроенные в облако

AWS Secrets Manager

GCP Secret Manager

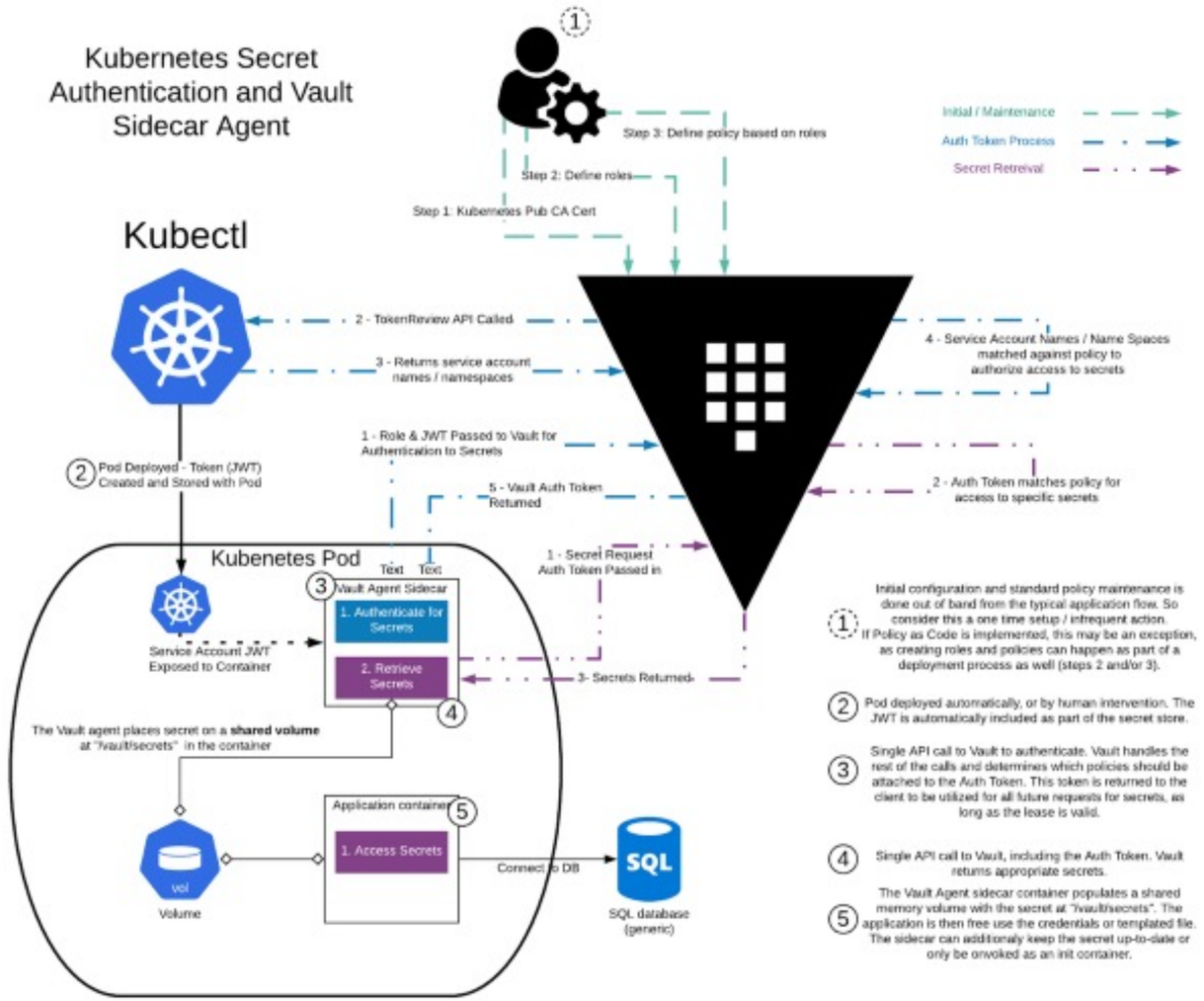
Yandex. Cloud Lockbox

Отдельные

HashiCorp Vault

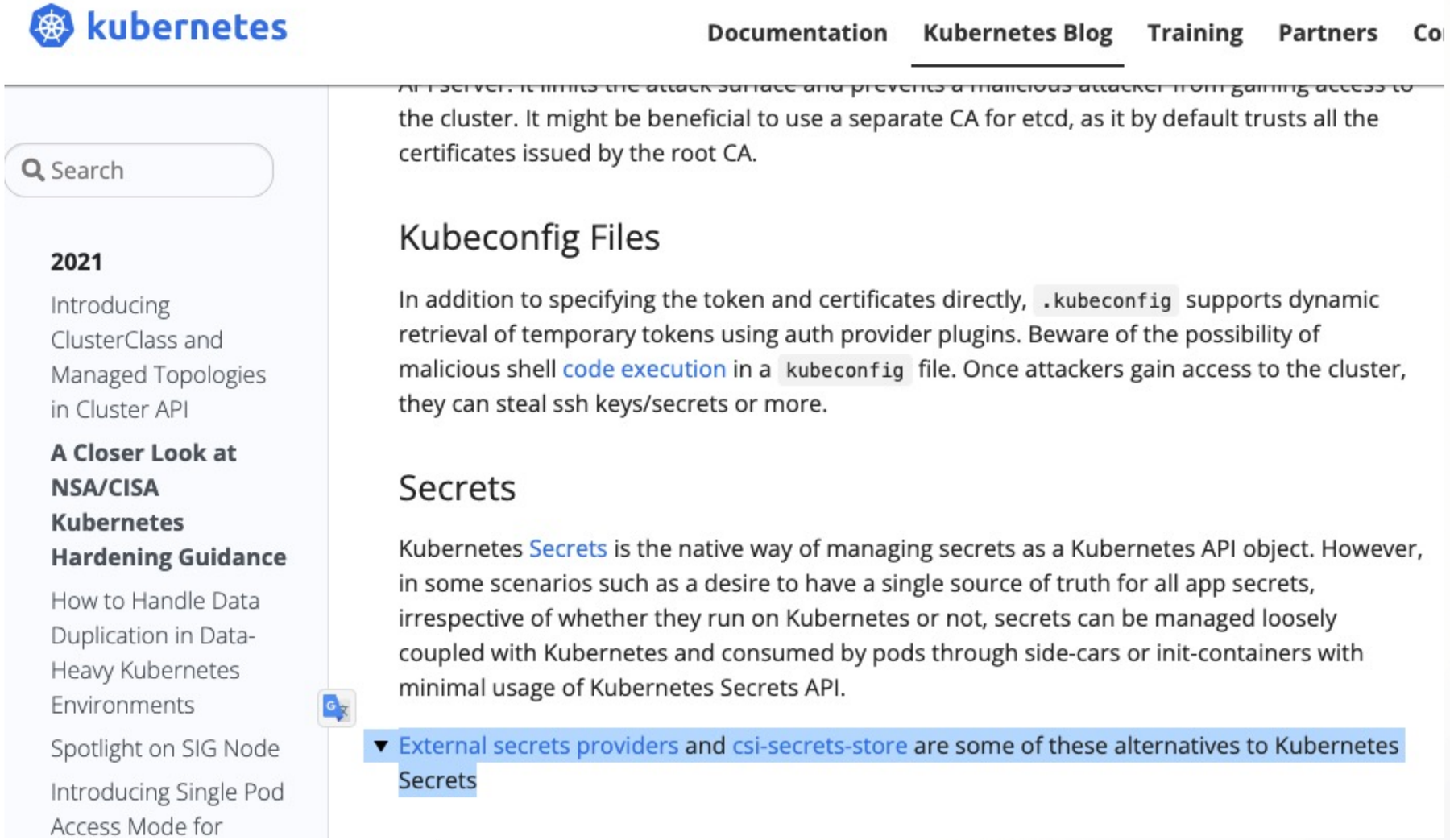
CyberArck Conjur

Интеграция с k8s: прошлое



https://medium.com/hashicorp-engineering/hashicorp-vault-delivering-secrets-with-kubernetes-1b358c03b2a3

Интеграция с k8s: настоящее



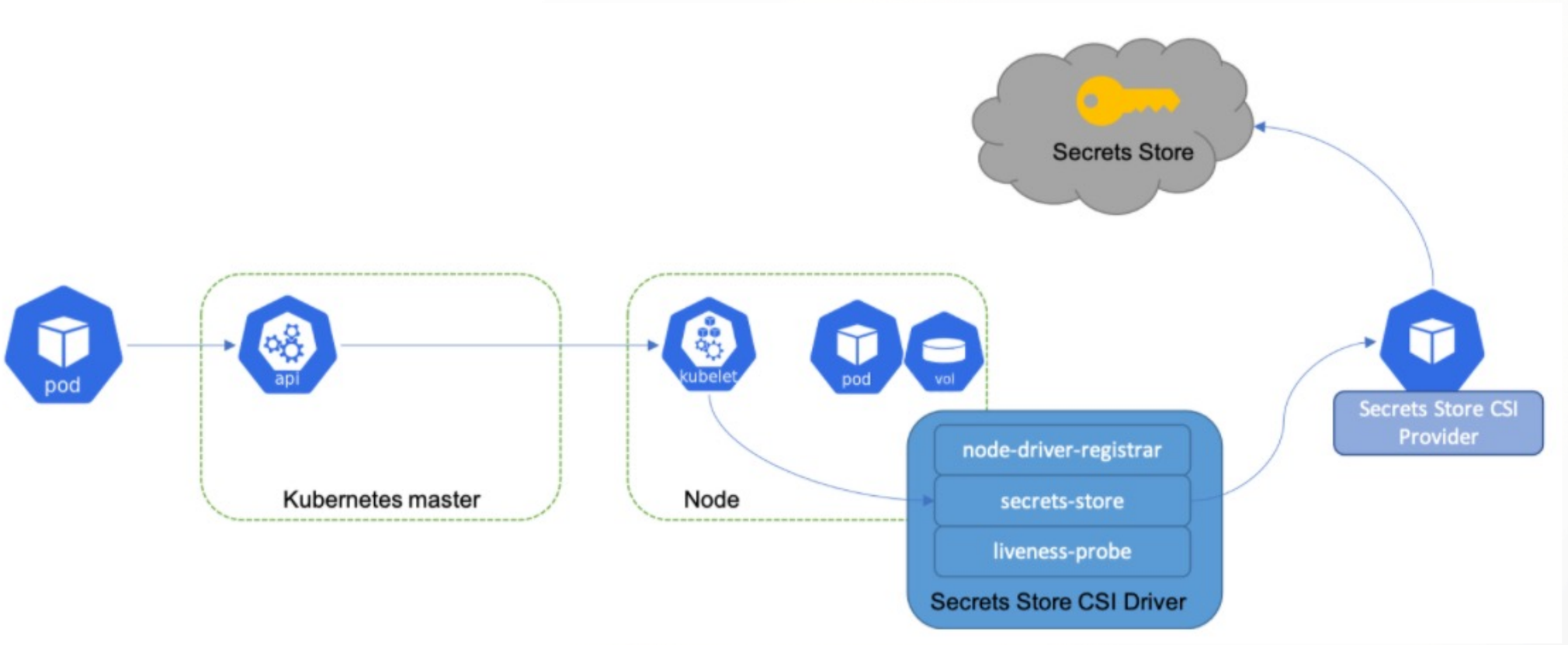
https://kubernetes.io/blog/2021/10/05/nsa-cisa-kubernetes-hardening-guidance/#secrets

Secrets Store CSI Driver

Secrets Store CSI Driver:

- Монтирует секреты в поды (как volume) с помощью Container Storage Interface (CSI) volume.
- Придумана командой “Kubernetes SIGs”
- Поддерживаются SecretManagers: Google, HashiCorp Vault, AWS, Azure
- Умеет монтировать несколько секретов одновременно
- Из минусов: автоматическое обновление секретов в alpha, синхронизация с k8s secrets в alpha

Secrets Store CSI Driver



https://secrets-store-csi-driver.sigs.k8s.io/concepts.html

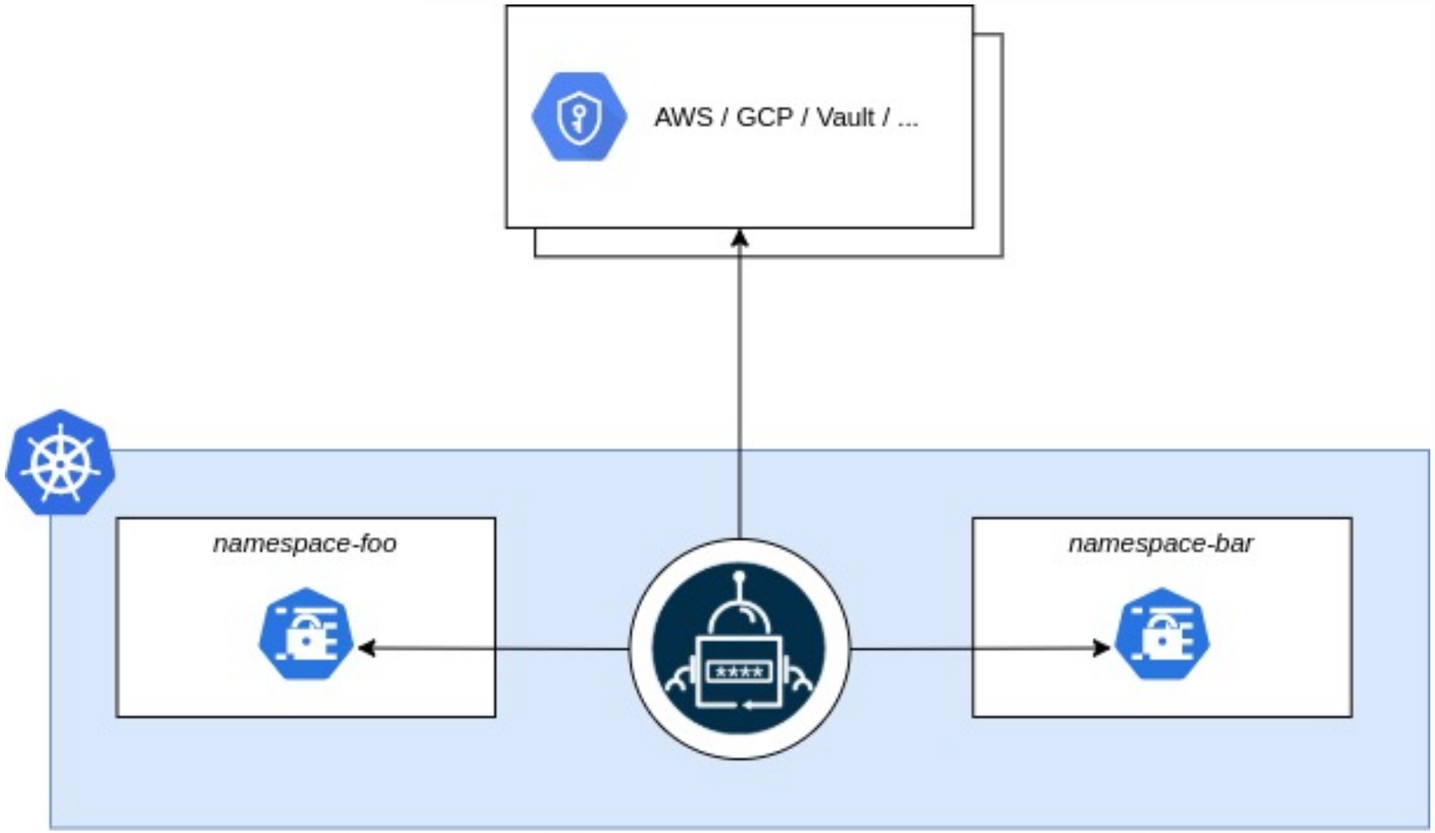
External Secrets

External Secrets

External Secrets:

- K8s operator – монтирует секреты в нативные объекты secrets
- Придумана командой “GoDaddy и Container Solutions”
- Поддерживаются SecretManagers: AWS Secrets Manager, HashiCorp Vault, Google Secrets Manager, Azure Key Vault, Yandex Cloud Lockbox

External Secrets



https://external-secrets.io/

lockbox-tf — mirtov8@mirtov8-osx — ..ay/lockbox-tf — -zsh — 107×26
♥ 22% вс 17 окт - 17:35 ~/Documents/terraform-play/lockbox-tf
@mirtov8

ETCD в незашифрованном виде

- Злоумышленник попал на master host
- Незашифрованный бэкап ETCD
- Диск с файлами прочитан или украден

```
[root@cka-master:/etc/kubernetes/manifests# ETCDCTL_API=3 etcdctl --cert /etc/kubernetes/pki/apiserver-etcd-c
lient.crt --key /etc/kubernetes/pki/apiserver-etcd-client.key --cacert /etc/kubernetes/pki/etcd/ca.crt get /
registry/secrets/default/default-token-vhb4v
/registry/secrets/default/default-token-vhb4v
k8s


v1Secret?
?
default-token-vhb4vdefault"*$d04e1ee1-5738-4a2f-adf7-7698f1fac9452· ??b-
"kubernetes.io/service-account.namedefaultbI
!kubernetes.io/service-account.uid$798ffd8d-564a-4cbd-b746-0f1a750757b9z??
kube-controller-managerUpdatev· ??FieldsV1:?
?{"f:data":{".":{},"f:ca.crt":{},"f:namespace":{},"f:token":{}},"f:metadata":{"f:annotations":{".":{},"f:kul
ernetes.io/service-account.name":{},"f:kubernetes.io/service-account.uid":{}}},"f:type":{}}?
ca.crt-----BEGIN CERTIFICATE-----
MIIC5zCCAc+gAwIBAgIBADANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDEwprdWJl
cm5ldGVzMB4XDTIxMDIxMDA2NDQxN1oXDTMxMDIwODA2NDQxN1owFTETMBEGA1UE
AxMKa3ViZXJuZXRlczCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANNq
KgRC3R6Gaw/m93WeqOMo8lSz5VBKjXOUgvdBtfmZZo+Mt6hGPDjhNqs3UPo5YqkX
K68UXVlHsNH4dBg4TSpZgb9WF2dYeonUvSpS2oFg/CwXPjJ058zWj64mvxQ18T/7
N71eAvIiWD1oJ9mSEkwqbVVTVv3IzKZqqplcOeHMpGbJjpw5uAGUzhTGbvFuPBE7
IfrVN2oigdisKEBRqfW5Ccd3OvUineB+lBu0ubPbObIHj2bir83CfxatFYGYStH6
HKKVEtt/Q44zPAoAfNw2UUnkxHQ7wKCMUa4OOjCNPbmvdOu0CsYDvHVXsKzPgcE0
BaHT9dK3czuS+1GFeaUCAwEAAaNCMEAwDgYDVR0PAQH/BAQDAgKkMA8GA1UdEwEB
/wQFMAMBAf8wHQYDVR0OBBYEFGGzTowaWSqlBVUwiAlGddzq1tuPMA0GCSqGSIb3
DQEBCwUAA4IBAQA3NPGa61ZRQGWS4Q6I/c2kuyct4WJv8l3VkSymXZboWD+8zF0J
bfg5Be6vpqr28vzlOAjQheMJir9Kh1Zqd26Omz9JYGzrTWhJKTCmRk3oAnrbU4Fm
Q/LCNcO0wcIhX7xIKI9y0Ek+8U2DjO/UrwFS44XZUIm70/BilHybn+TaCowNvW5+
mYVS48ALPHFyhPmVs9WVRx7m/nrt1WItSF90CaZj+I1C8BeAE8uBgt9z+yWNegwR
e8yQXFRtv7eID9Kn5ZtY7f/5luzPtwz5kLnNsNJ8zss6qgEMXan0IrqFbkHvvYHj
JPr2Hhap7rfScKC1M9jN0yFCSejmnIWokxIS
```

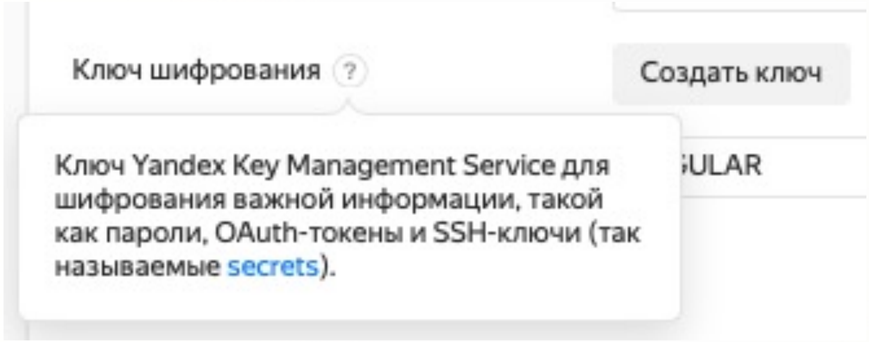
В ETCD в зашифрованном виде

```
root@cka-master:~# ETCDCTL_API=3 etcdctl --cert /etc/kubernetes/pki/apiserver-etcd-client.crt --key /etc/kub
ernetes/pki/apiserver-etcd-client.key --cacert /etc/kubernetes/pki/etcd/ca.crt get /registry/secrets/default
/very-secure
/registry/secrets/default/very-secure
k8s:enc:aescbc:v1:key1:
                       ??$E??w\V??d?    )?X?h????8gM{???H?i>UJ?wIFV?????)??1?{
                                                                               f?d?uw?8??[?-$(}?2цN??u???|?;?
?Yiq_t8???f♦C??(??"??
                     ?
w?o??
     ?=B?;?yVz?.,?+??ä?,h%??B???ә??'??-(?
                                         c?W6?A?'??4Й??L?)2????A7L??%<??m?h?6?sq?Π??K???M"??yG??
```

Шифрование ETCD в облаках «из коробки»

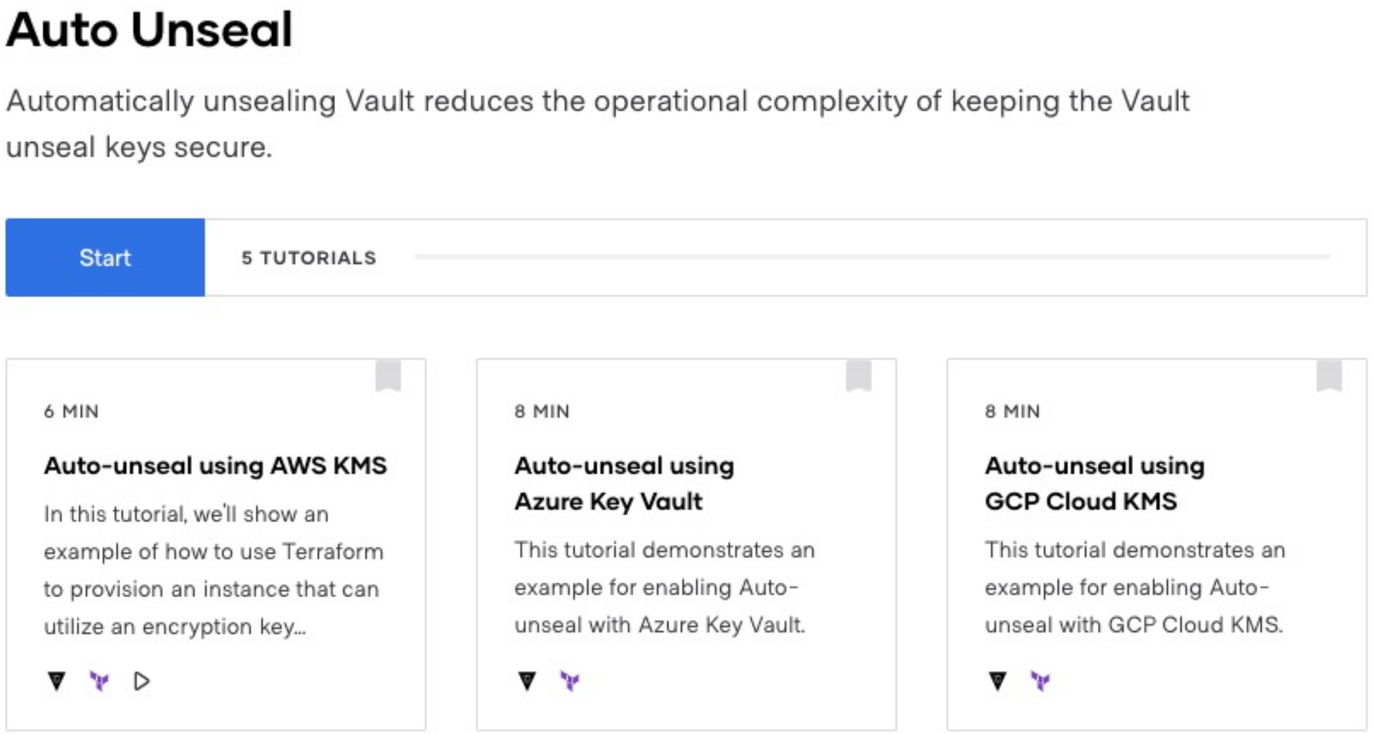
aws

Yandex Cloud



Hashicorp Vault в облаках

- Unseal: процесс подготовки Vault к работе (получение мастер-ключа)*

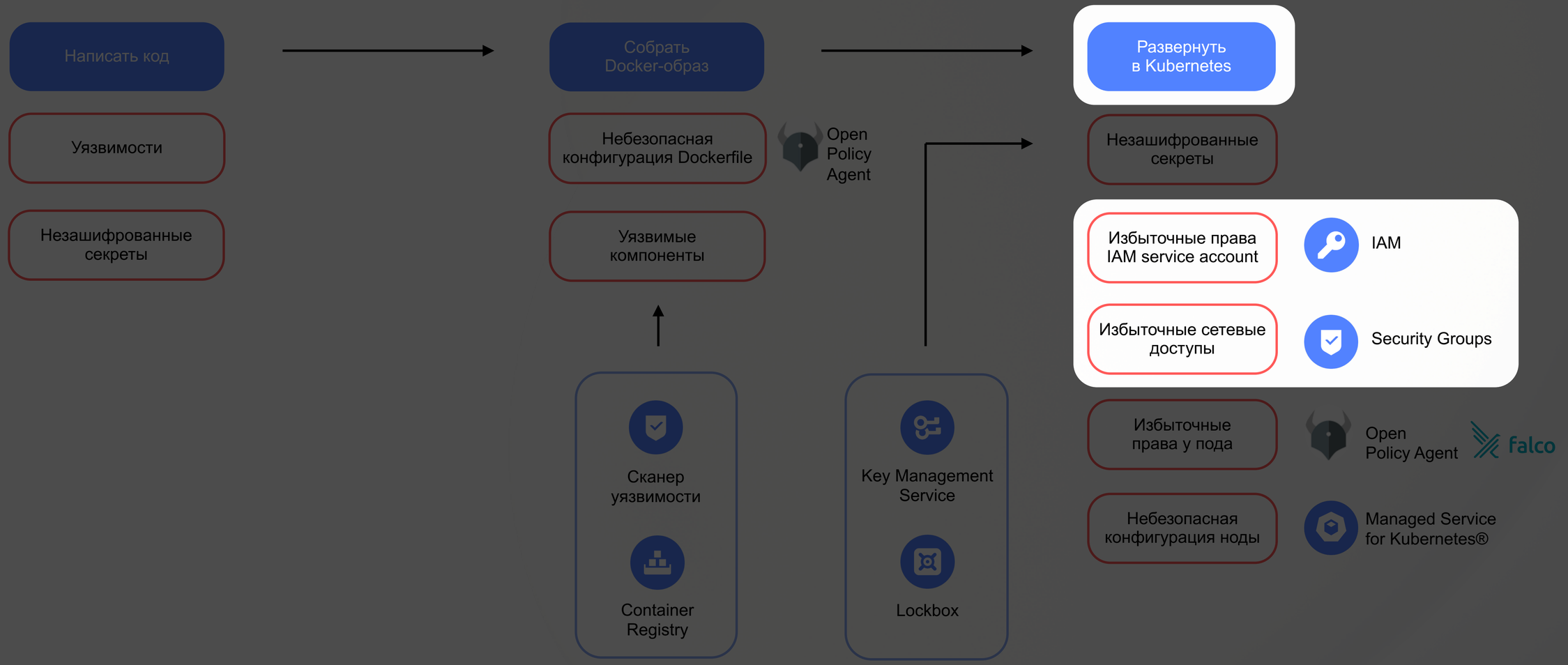


* Данную проблему решает Auto-unseal интеграция с Yandex.Cloud KMS

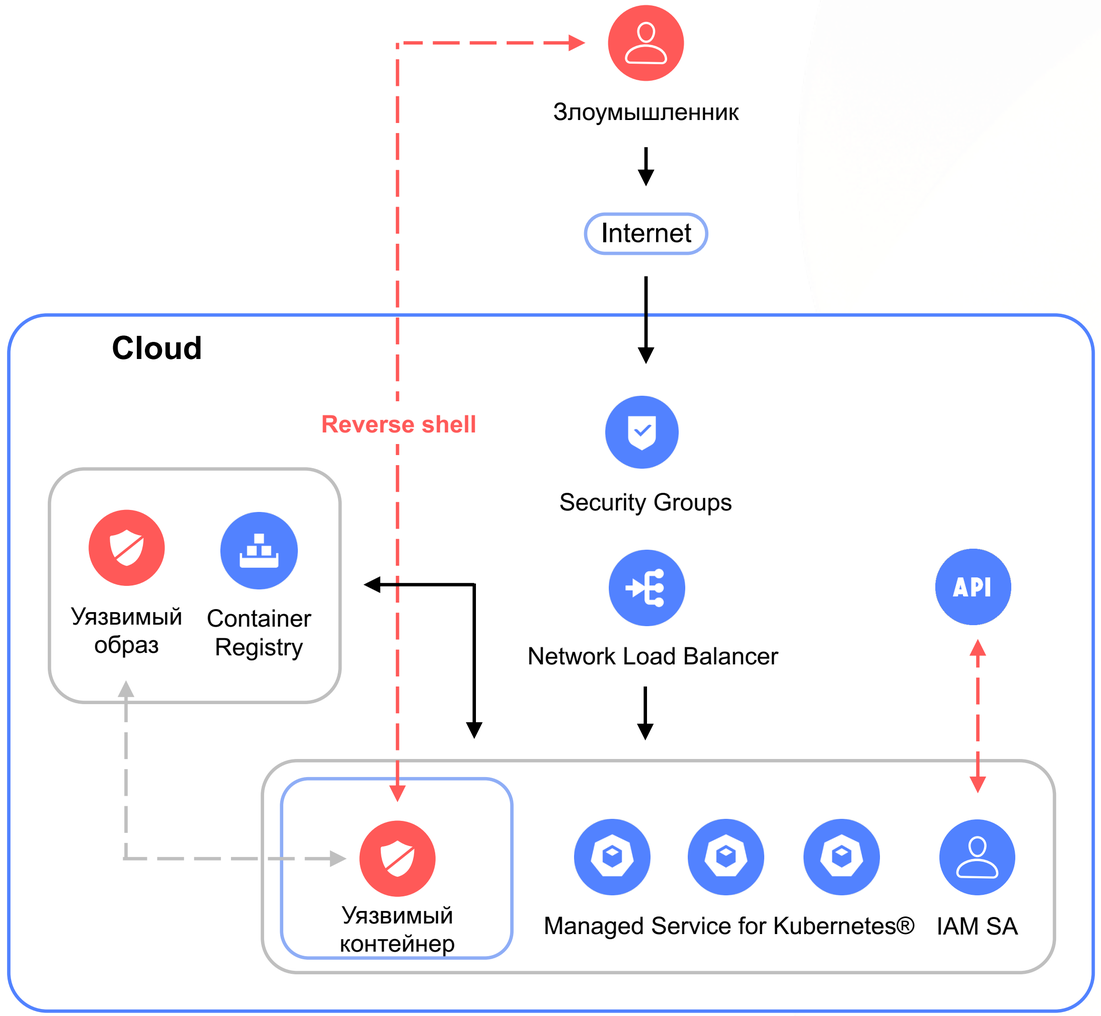
Избыточные права или сетевые доступы

Схема контейнерной разработки

Application Pipeline



Избыточные права или сетевые доступы



- Избыточные права IAM service account
  k8s service account
- Избыточные сетевые доступы
  - сетевой доступ
    к сервису метаданных:

    http://169.254.169.254/latest/meta-data/<элемент>
  - сетевой доступ в другие pods,
    namespaces, в интернет и т. д.

Cloud

mirtov-scale-folder
Folder

Folder dashboard
Service accounts
Federations
Incident notifications
Operations

Folder dashboard

Create resource

Compute Cloud

2 VM
2 Disks

Virtual Private Cloud

1 Network
5 Subnets
2 Addresses

Managed Service for Kubernetes

1 Cluster

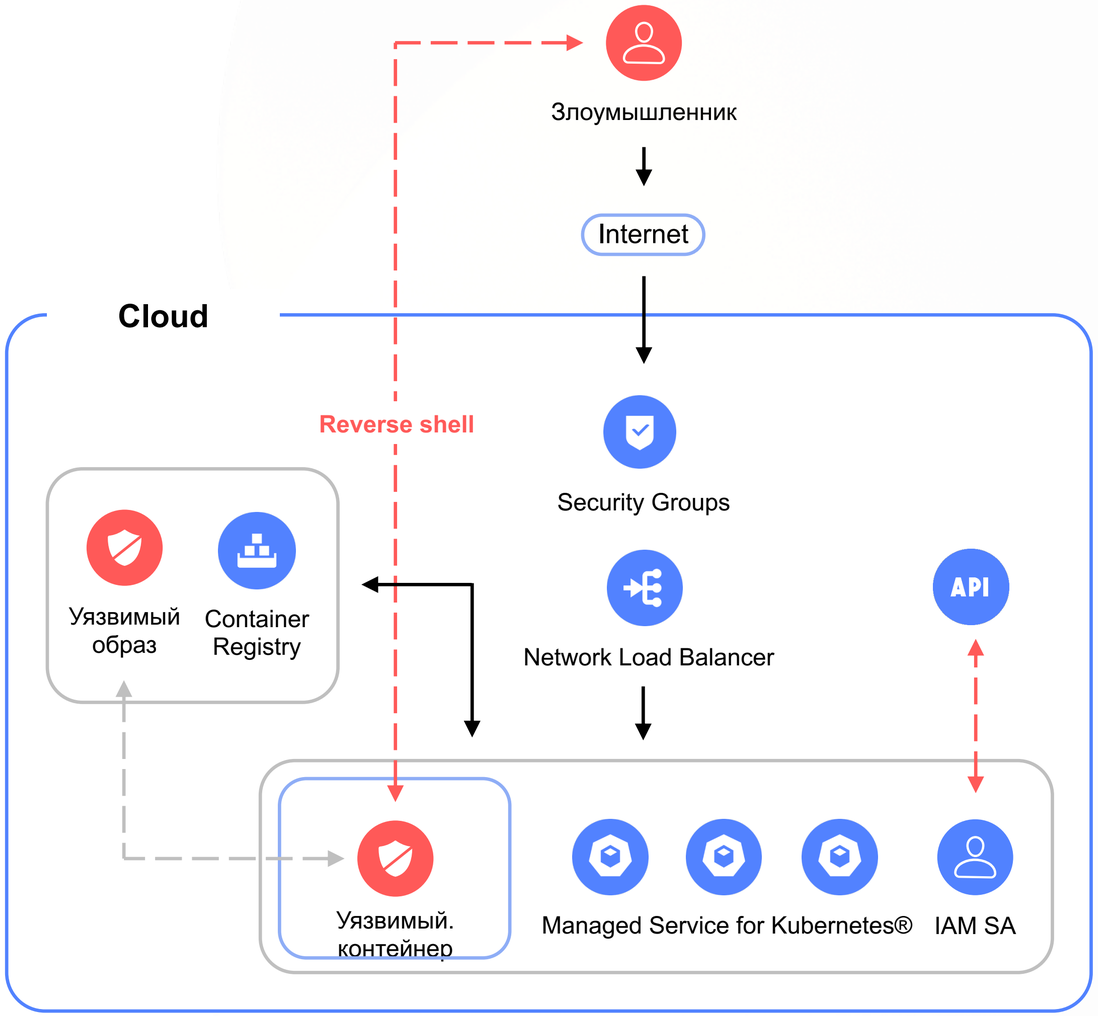
Cloud DNS PREVIEW

2 Zones
11 Records

Services

- Compute Cloud
- Managed Service for PostgreSQL
- Managed Service for MongoDB
- Managed Service for ClickHouse
- Managed Service for Redis
- Managed Service for MySQL
- Managed Service for Kafka
- Managed Service for Elasticsearch NEW
- Managed Service for SQL Server NEW
- Managed Service for Greenplum PREVIEW
- Object Storage
- Virtual Private Cloud
- Network Load Balancer
- Application Load Balancer PREVIEW
- Container Registry
- Data Proc
- Managed Service for Kubernetes
- Yandex Database
- Message Queue
- Cloud Functions
- Serverless Containers PREVIEW
- Key Management Service
- DataSphere
- IoT Core

Избыточные права или сетевые доступы



mirtov8@mirtov8-osx:~

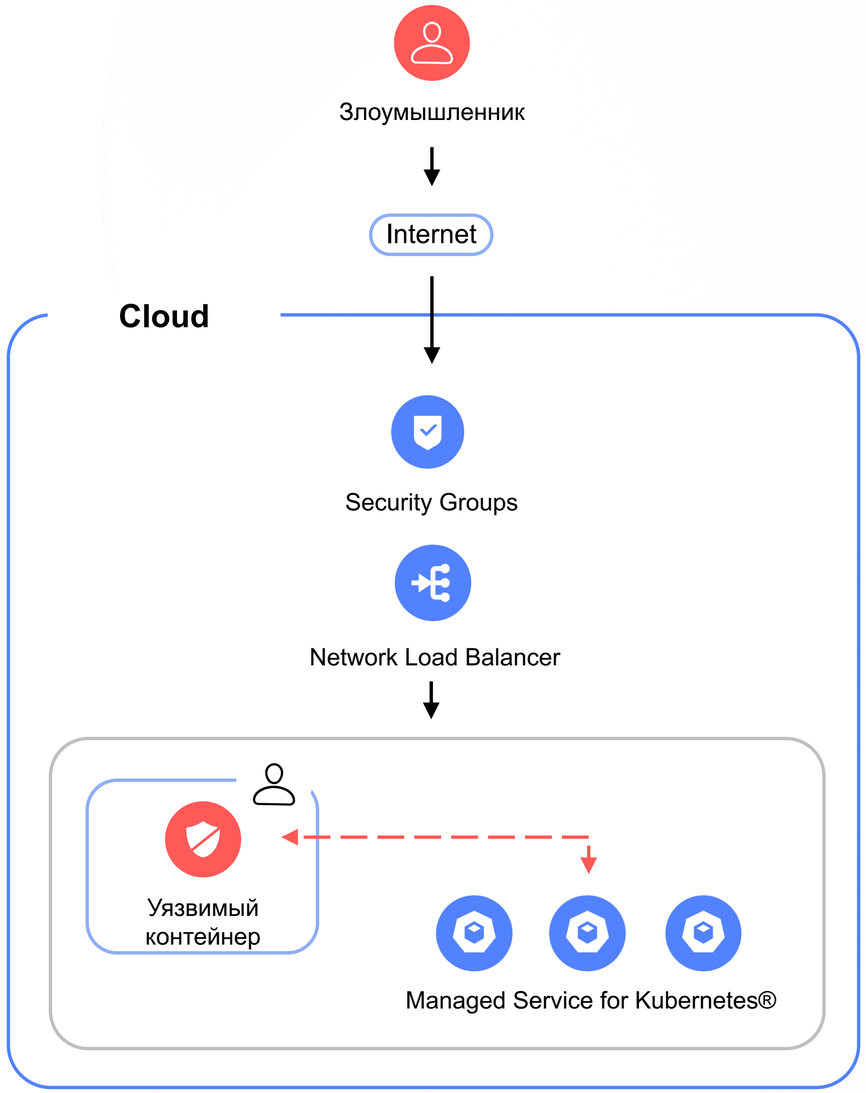
root@k8s-hack: /home/alex (ssh)

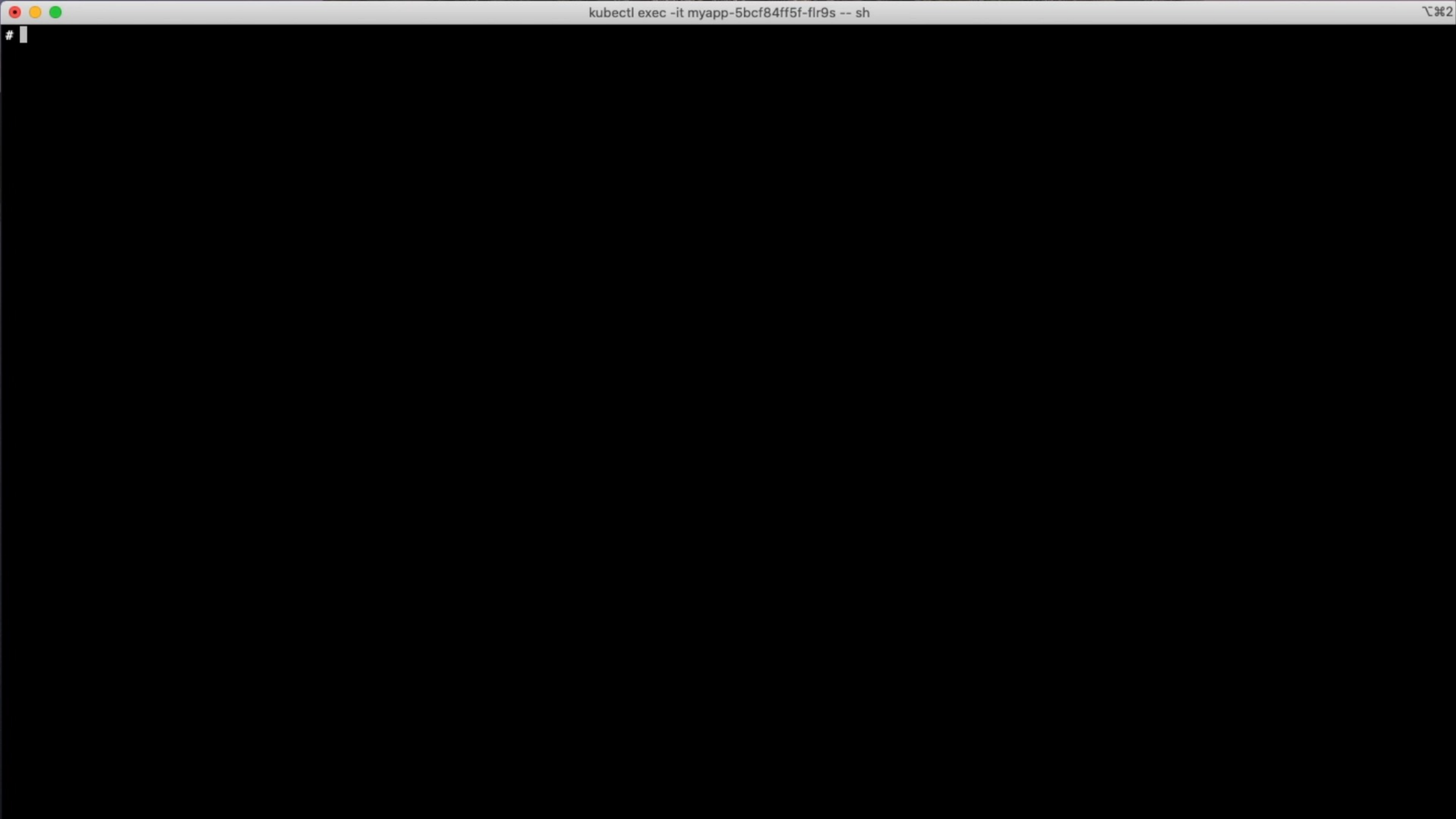
```
root@myapp-5bcf84ff5f-flr9s:/tmp#
```

~ (-zsh)

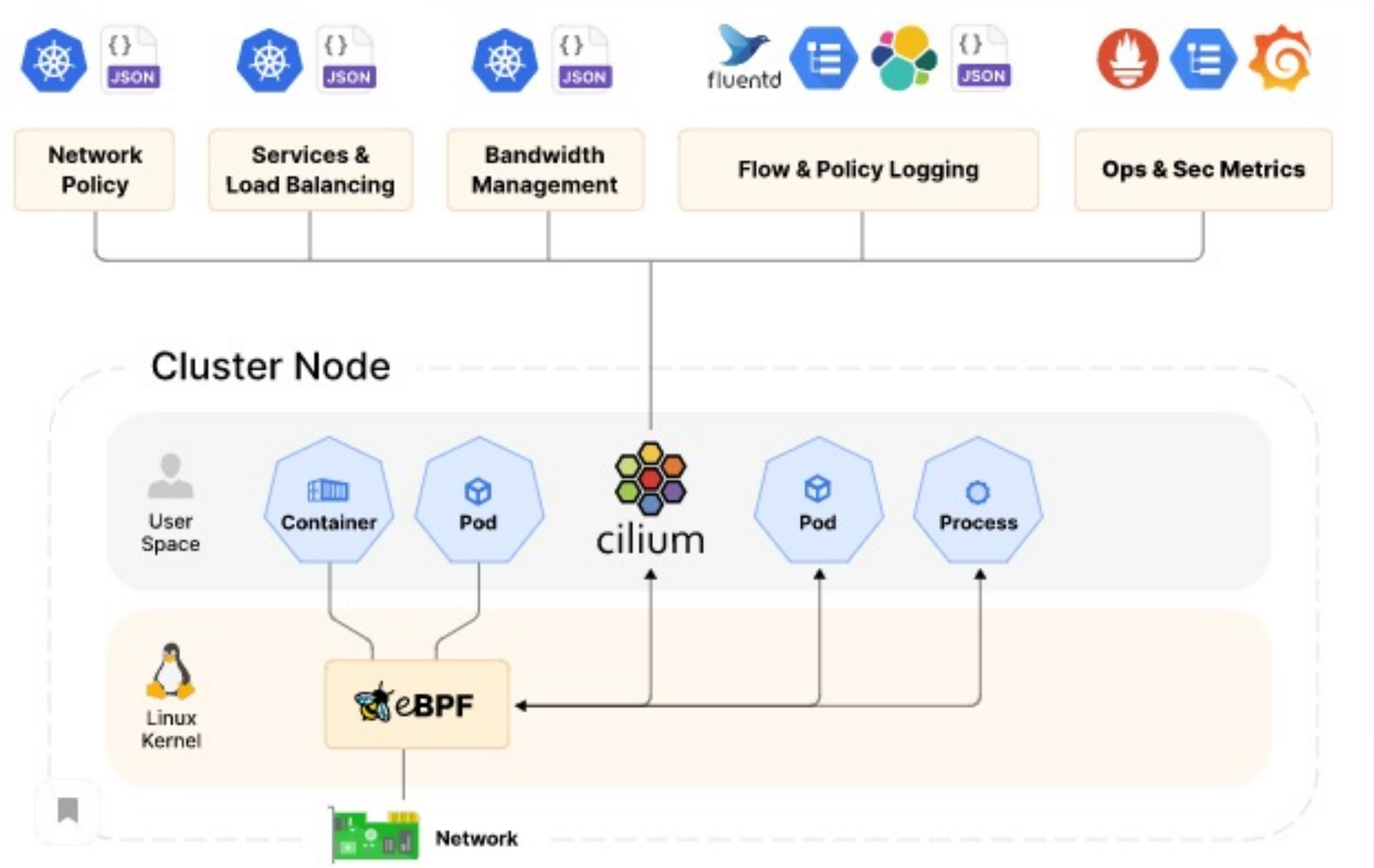
пт 27 авг - 19:41 ~
@mirtov8

Избыточные права или сетевые доступы

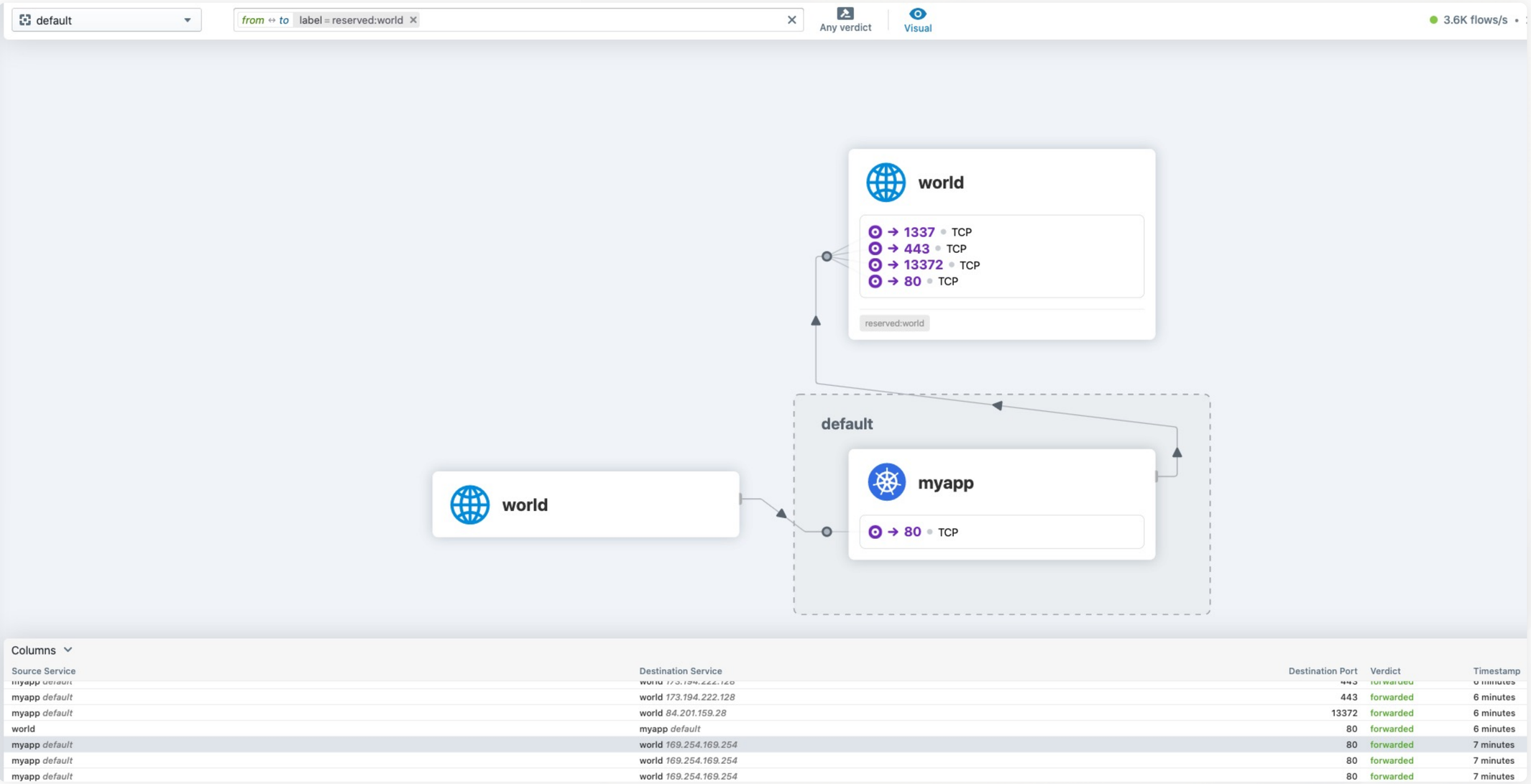



kubectl exec -it myapp-5bcf84ff5f-flr9s -- sh
⌥⌘2
#

Cilium


JSON
JSON
JSON
fluentd
JSON
Network Policy
Services & Load Balancing
Bandwidth Management
Flow & Policy Logging
Ops & Sec Metrics
Cluster Node
User Space
Container
Pod
cilium
Pod
Process
Linux Kernel
eBPF
Network

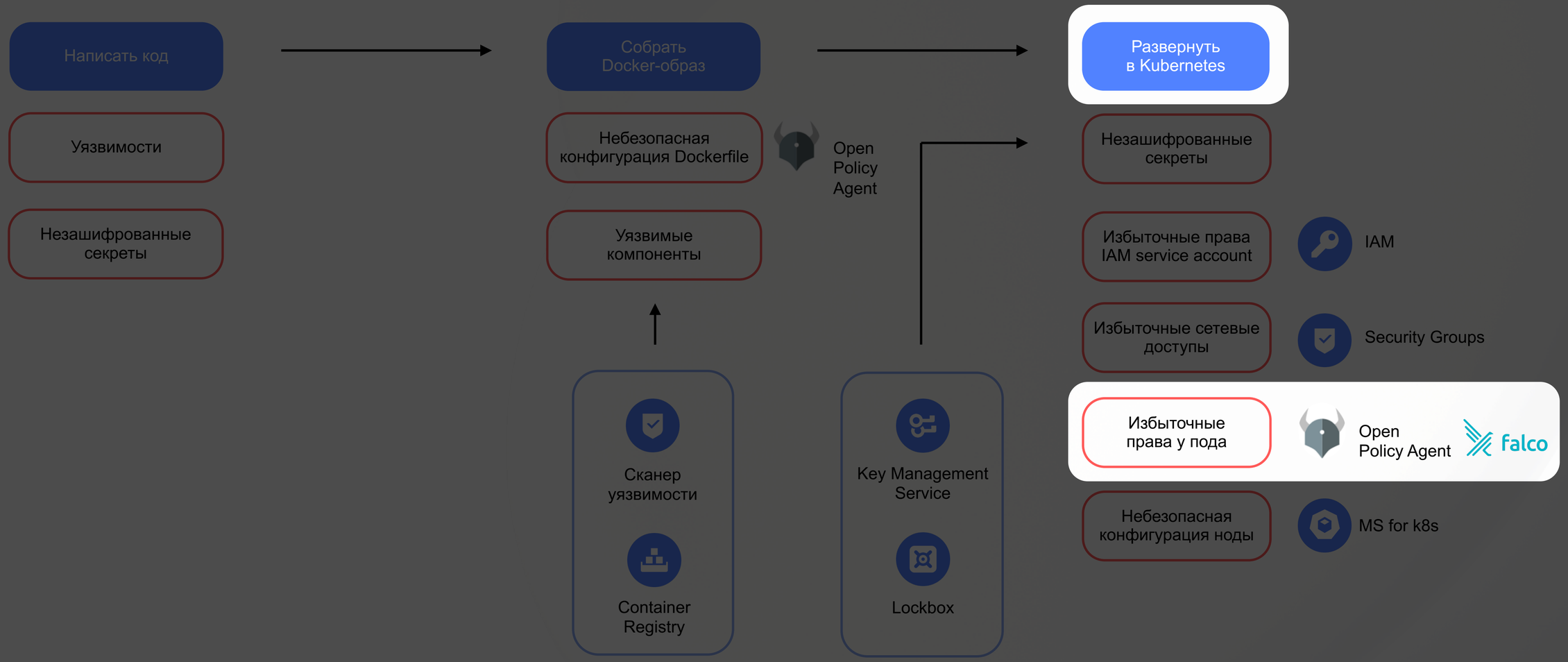
Сетевые политики. Cilium



Аномальное поведение или отсутствие контроля

Схема контейнерной разработки

Application Pipeline



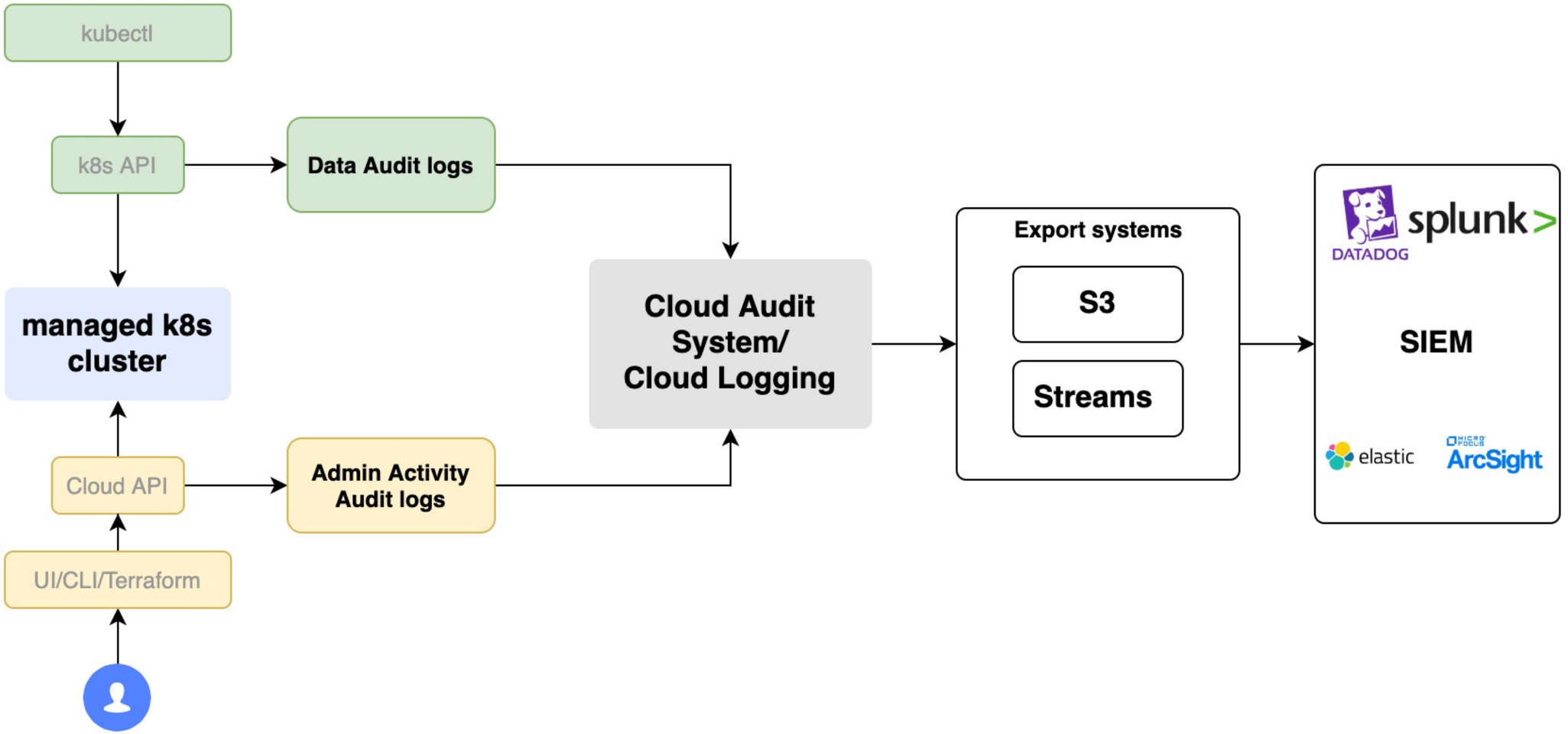
K8s cloud audit logs

Аудит логи k8s в облаке

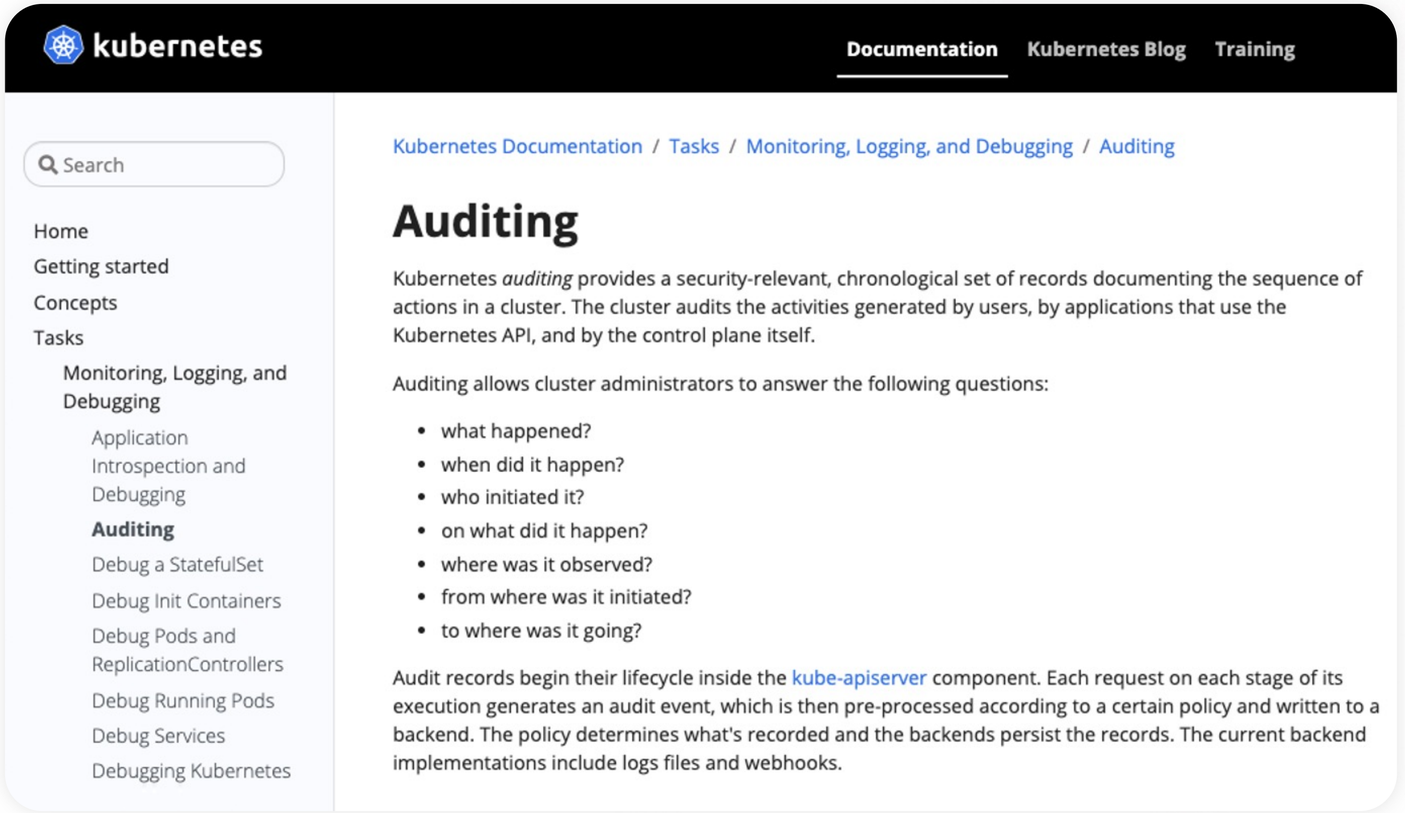
- Admin Activity audit logs - логи работы с API облака через UI/CLI/Terraform (пример: создан кластер, изменен кластер, действия с nodes и др.)
- Data audit logs – логи встроенные в k8s (k8 native audit logs) (пример: создан pod, назначены права внутри k8s и др.)

aws Google Cloud Yandex Cloud

Облако

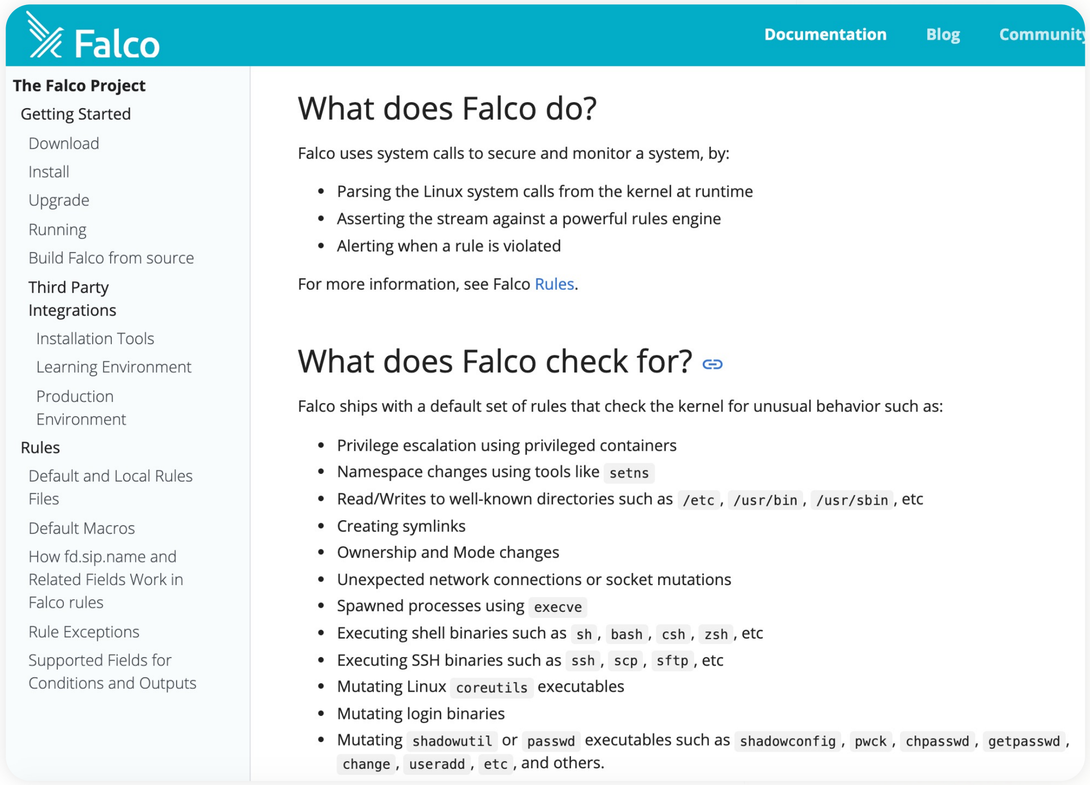


Yandex Managed Service for Kubernetes®



```
{
  "kind" : "Event",
  "apiVersion" : "audit.k8s.io/v1",
  "level" : "RequestResponse",
  "auditID" : "c8ffdc9f-7231-4919-9d5b-32fb95458f84",
  "stage" : "RequestReceived",
  "requestURI" : "/apis/constraints.gatekeeper.sh/v1beta1/k8spspallow
  rivilegeescalationcontainer/psp-allow-privilege-escalation-containe
  r",
  "verb" : "delete",
  "user" : {
    "username" : "kubernetes-admin",
    "groups" : [
      "system:masters",
      "system:authenticated"
    ]
  },
  "sourceIPs" : [
    "10.129.0.19"
  ],
```

Анализ аномального поведения, runtime security



Falco

Многие знают, устанавливали, тестировали, но не многие выгружают, анализируют, работают с его алертами (это непросто)

Анализ аномального поведения (runtime security)

README.md

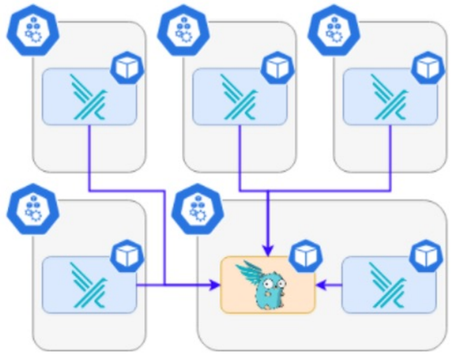
Falcosidekick

release v2.24.0 | last commit 15 days ago | license MIT | docker pulls 1.04M | circleci passing

Description

A simple daemon for connecting `Falco` to your ecossytem. It takes a `Falco` 's events and forward them to different outputs in a fan-out way.

It works as a single endpoint for as many as you want `Falco` instances :



Outputs

Alerting

- AlertManager
- Opsgenie
- PagerDuty

Logs

- Elasticsearch
- Loki
- AWS CloudWatchLogs
- Grafana (annotations)

Object Storage

- AWS S3
- GCP Storage
- Yandex S3 Storage

Policy Engine

Встроенные

PodSecurity Policies (Kubernetes v1.22 [deprecated])

- ✗ Проблемы с авторизацией
- ✗ Нет dry-run mode (audit mode)
- ✗ Неудобство использовании
- ✗ Др.

PodSecurity admission controller (Kubernetes v1.22 [alpha])

- ✓ Dry-run mode (audit mode)
- ✓ Нативный механизм k8s
- ✓ Удобен в использовании (ns labels)
- ✗ Сырой и необкатан
- ✗ Отсутствие гранулярности и гибкости

Внешние

OPA Gatekeeper

- ✗ Использует rego как язык политик (не удобен)
- ✓ Поддержка community (Google, Microsoft)
- ✗ Использует 2 ресурса политик (сложно для управления)
- ✓ Возможность использования за пределами k8s

Kyverno

- ✓ Простой k8s-like язык политик
- ✓ Частые updates и поддержка контента
- ✓ Расширенные возможности алерта в режиме аудит
- ✗ Молодой продукт

Kyverno

Policy Reporter

CI passing | go report A+ | coverage 93%

Motivation

Kyverno ships with two types of validation. You can either enforce a rule or audit it. If you don't want to block developers or if you want to try out a new rule, you can use the audit functionality. The audit configuration creates PolicyReports which you can access with `kubectl`. Because I can't find a simple solution to get a general overview of this PolicyReports and PolicyReportResults, I created this tool to send information about PolicyReports to different targets like Grafana Loki, Elasticsearch or Slack.

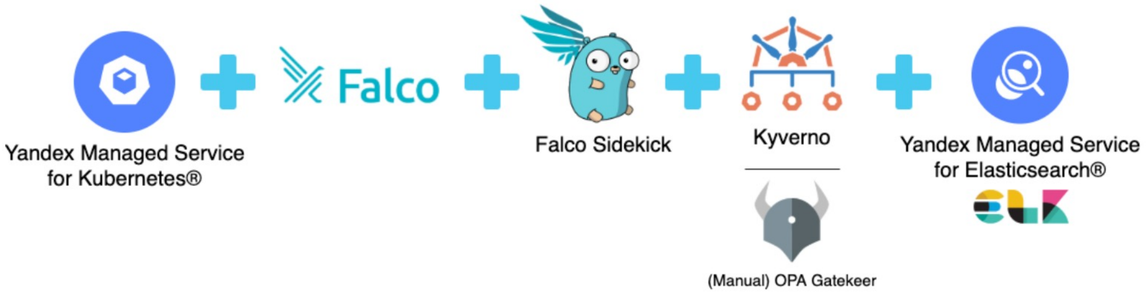
Targets

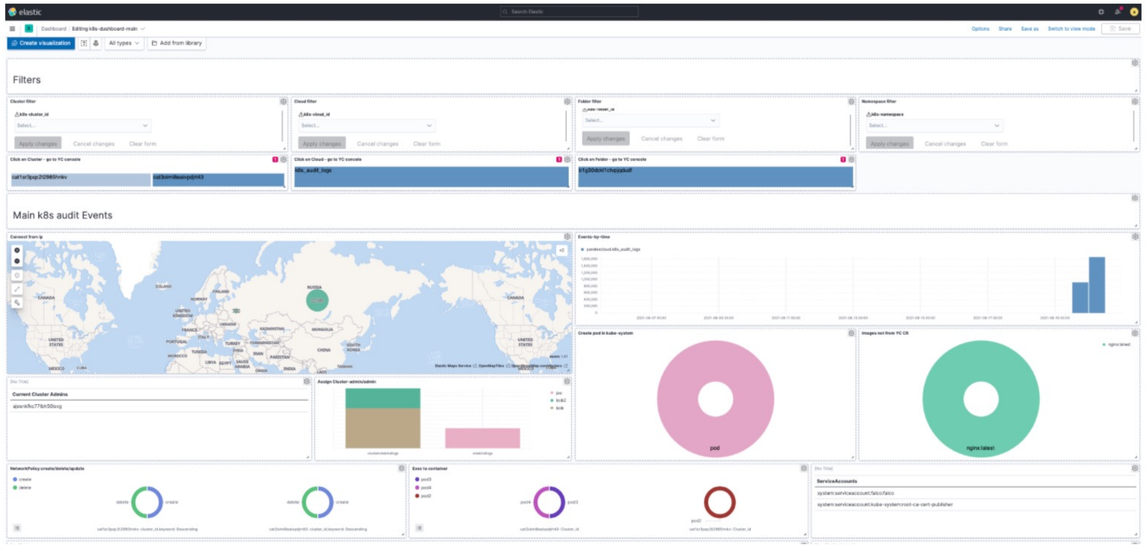
Policy Reporter supports the following Targets to send new (Cluster)PolicyReport Results too:

- Grafana Loki
- Elasticsearch
- Slack
- Discord
- MS Teams
- Policy Reporter UI

Решение по анализу логов ИБ Kubernetes

Yandex Cloud: Анализ логов безопасности k8s в ELK: аудит-логи, policy engine, falco





GitHub

Kubernetes: описание решения

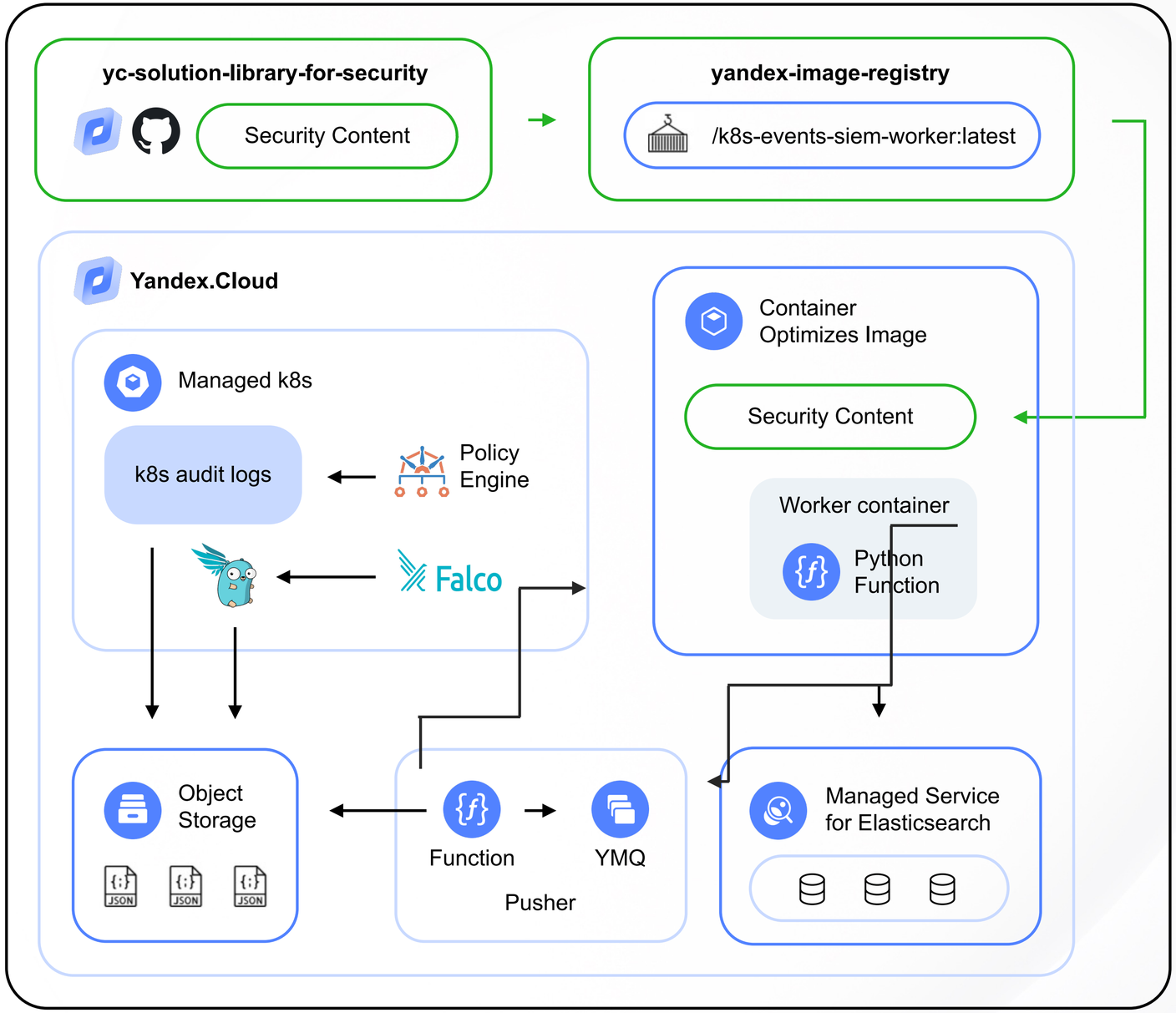
Managed Service for Kubernetes®

Falco

Falco Sidekick

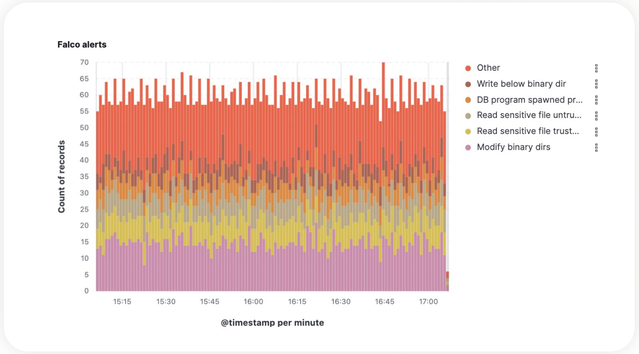
Kyverno

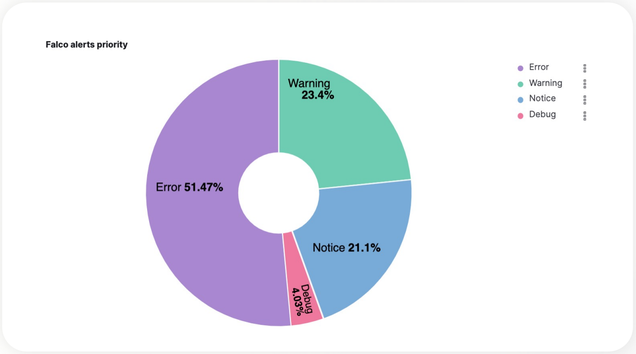
Managed Service for Elasticsearch



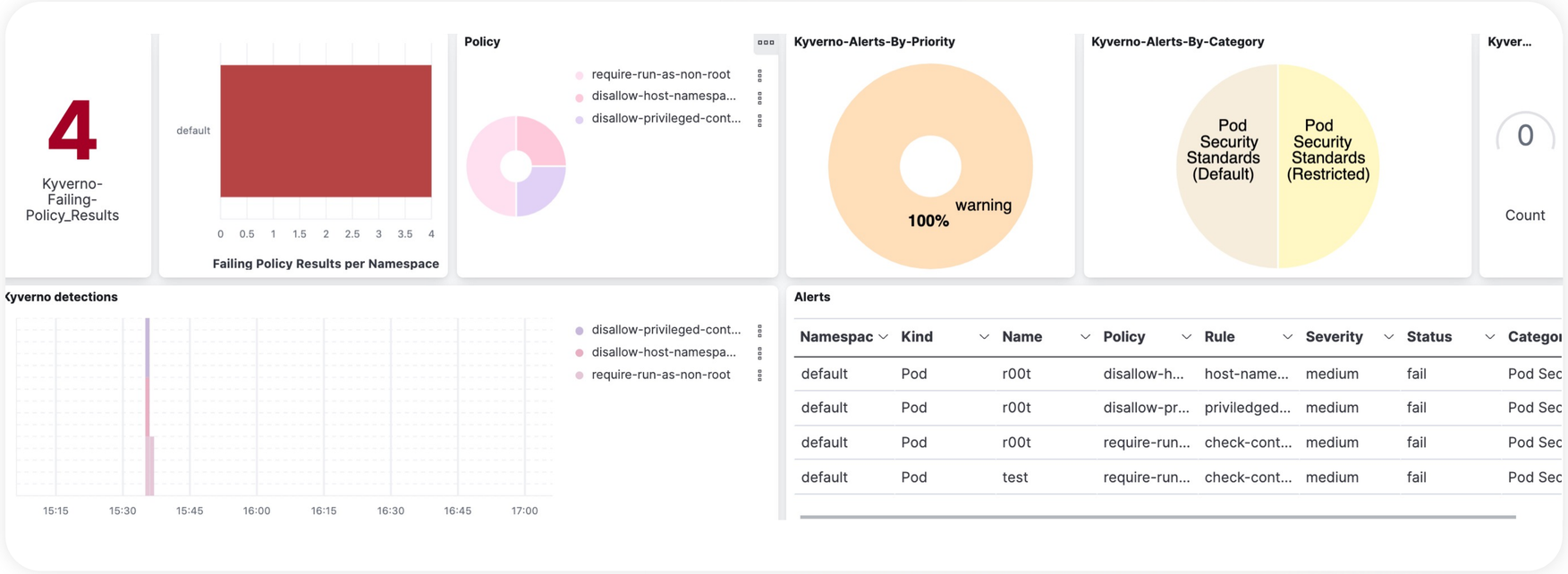
Улов Falco по результатам атаки

- Обнаружил запуск reverse shell в поде (так мы попали внутрь контейнера через уязвимость shellshock)
- Обнаружил запуск пакетного менеджера apt-get install из пода
- Обнаружил запуск kubectl из пода (также отслеживает запуск Docker)
- Обнаружил запуск привилегированного контейнера “securityContext”:{“privileged”:true}





Улов Policy Engine по результатам атаки



- Detect/Prevent: запуск привилегированного контейнера "securityContext":{"privileged":true}
- Detect/Prevent: запуск контейнера с shared host namespace "securityContext":{"hostPID":true}

elastic

Search Elastic

D | Discover | Search:Yandexcloud:k8s:kyverno:Interesting fields | Options | New | Save | Ope

verb : create

verb : create

k8s-audit*

Search field names

Filter by type 0

Selected fields 5

- t cloud_id
- t cluster_id
- t folder_id
- t objectRef.namespace
- t cluster_url

Available fields 100

Popular

- t objectRef.name
- t _id
- t _index
- # _score
- t _type
- @timestamp
- t annotations.authentication.k8s.io/legacy-token

3 hits | Reset search | Sep 18, 2021 @ 14:55:47.887 - Sep 18, 2021 @ 15:55:47.887 | Auto

Time	cloud_id	cluster_id	folder_id	objectRef.namespace	cluster_url
Sep 18, 2021 @ 15:36:17.634	b1gq9j4sbpge1hdasvtp	cath4iqmpib957g7o7ko	b1gh4nansv4ebqqmeu7b	default	https://console.cloud.yandex.ru/folders/b1gh4naed-kubernetes/cluster/cath4iqmpib957g7o7ko
Sep 18, 2021 @ 15:35:32.741	b1gq9j4sbpge1hdasvtp	cath4iqmpib957g7o7ko	b1gh4nansv4ebqqmeu7b	default	https://console.cloud.yandex.ru/folders/b1gh4naed-kubernetes/cluster/cath4iqmpib957g7o7ko
Sep 18, 2021 @ 15:35:27.364	b1gq9j4sbpge1hdasvtp	cath4iqmpib957g7o7ko	b1gh4nansv4ebqqmeu7b	default	https://console.cloud.yandex.ru/folders/b1gh4naed-kubernetes/cluster/cath4iqmpib957g7o7ko

Expanded document | View surrounding documents | View s

Table | JSON

t _id 4wDn-HsBRvsvEEjFr5L-

Обновления Kubernetes-нод

Обновление k8s в облаках

- Обновление нужно как для nodes, так и для master
- Провайдер предоставляет инструменты обновления, но не может заставить ими пользоваться
- Можно сканировать виртуальные машины

Выводы

„Тестирование программы может весьма эффективно продемонстрировать наличие ошибок, но безнадежно неадекватно для демонстрации их отсутствия.“

Эдсгер Вибе Дейкстра

Выводы

- Постройте диалог с безопасником, узнайте модель угроз
- Встройте статические проверки в CI
- Добавьте алерты на странные действия в вашем кластере
- Посмотрите, какие встроенные средства есть у вашего провайдера (и какие рекомендации он дает)

Спасибо!
Вопросы?

Спикеры:
Алексей Миртов, Yandex.Cloud
Любовь Гринкевич, Yandex.Cloud