tech

Управление **TLS**-сертификатами в инфраструктуре

Пару слов обо мне

Дмитрий Рыбалка

Старший инженер ИТ-инфраструктуры

Содержание

1. Узнаем что за сертификаты и протоколы их передачи
2. Не Let’s Encrypt едины
3. Раскроем вопрос безопасности и раскрытия информации
4. Управление сертификатами в среде Kubernetes
    1. Cert manager
    2. kubernetes-replicator
    3. vault-secrets-webhook
    4. External secrets
5. Наши опыт и текущая точка на пути

Kubernetes
FIRST

Kubernetes

2

Дата-центра

6

Зон доступности

10+

Кластеров

tech

Kubernetes

10K+
Pod

5K+
Сертификатов

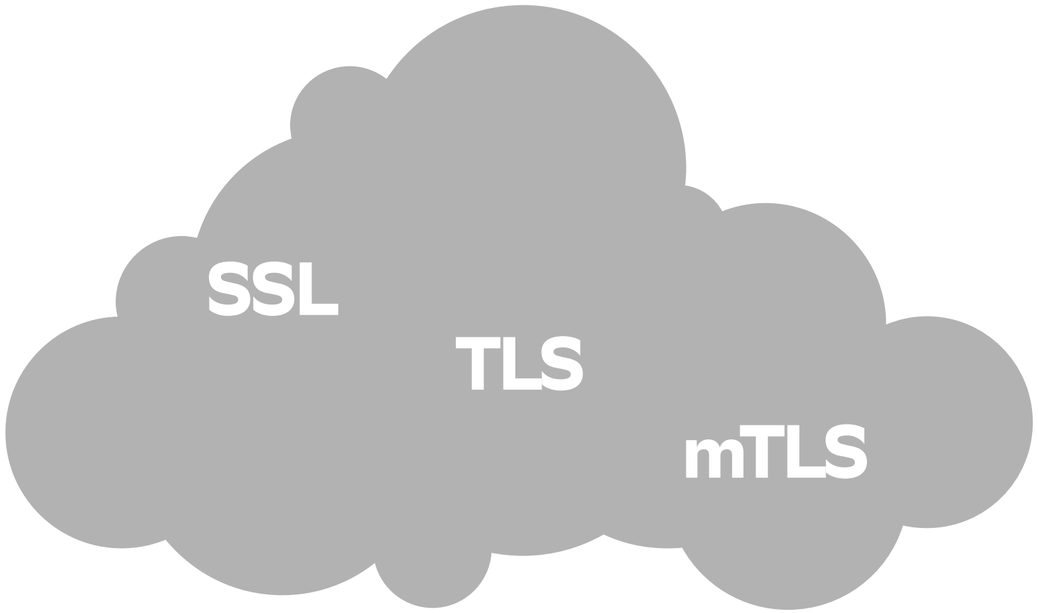
200+
Node

Протоколы

Secure Sockets Layer (SSL)

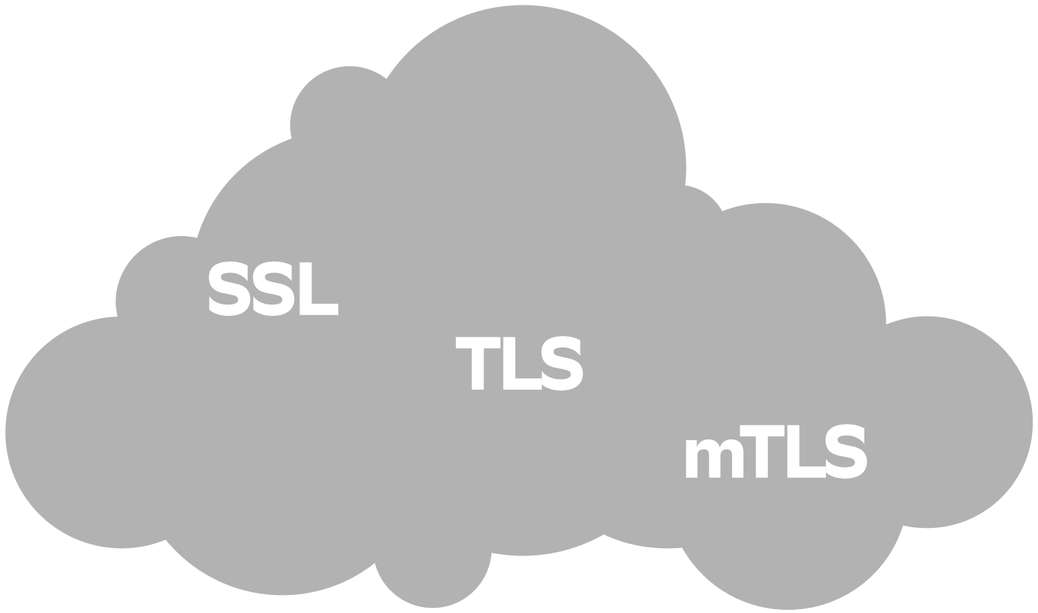
Transport Layer Security (TLS)

Two Way TLS или mutual TLS (mTLS)



Сертификаты

Сертификаты SSL/TLS позволяют браузерам проверять подлинность веб-сайтов и устанавливать с ними зашифрованные сетевые соединения с использованием протокола SSL/TLS.



Amazon (c)

Протоколы

Transport Layer Security (TLS)


```
kind: Secret

type: kubernetes.io/tls

data:
  tls.crt: (цепочка сертификатов)
  tls.key: (приватный ключ)
```

Протоколы

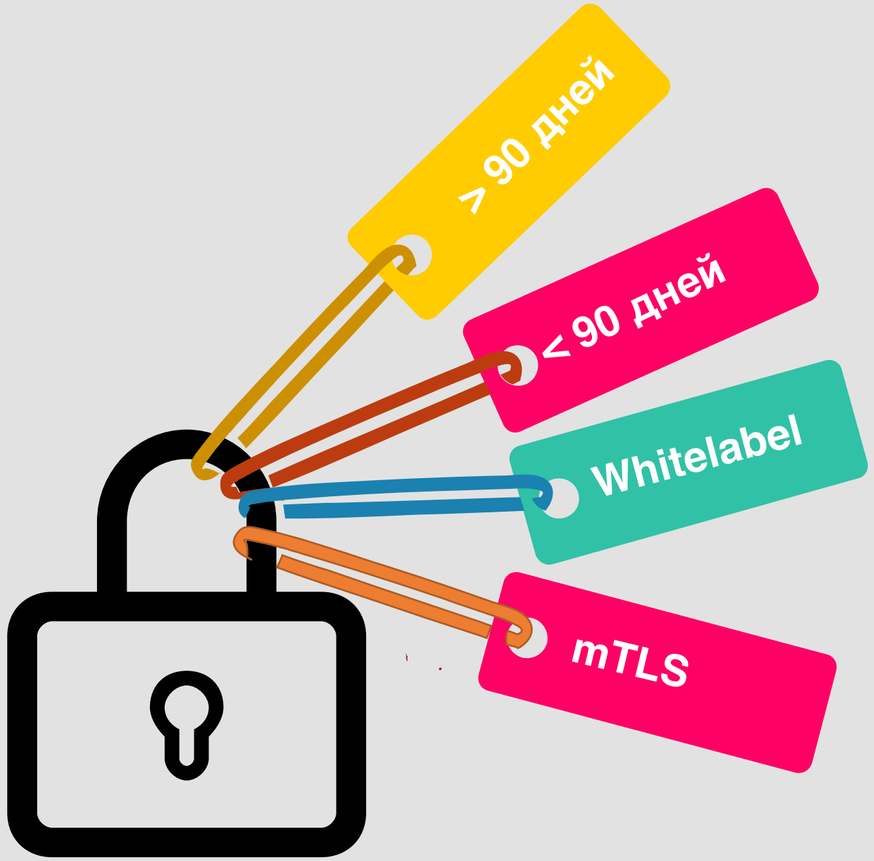
Two Way TLS или mutual TLS (mTLS)

kind: Secret

type: Opaque

data:
  tls.crt: (цепочка сертификатов)
  tls.key: (приватный ключ)
  ca.crt: (1 или набор ca сертификатов удаленной системы)

Разделение сертификатов



Сертификаты

< 90 дней

Используются для
среды разработки

Сертификаты

< 90 дней

Используются для
среды разработки

Issuer Let’s Encrypt

Сертификаты

< 90 дней

Используются для
среды разработки

Issuer Let’s Encrypt

Only Wildcard

Сертификаты

> 90 дней

Whitelabel

Используются для
среды разработки и
продакшн среды

Сертификаты

> 90 дней

Whitelabel

Используются для
среды разработки и
продакшн среды

Issuer any

Сертификаты

> 90 дней

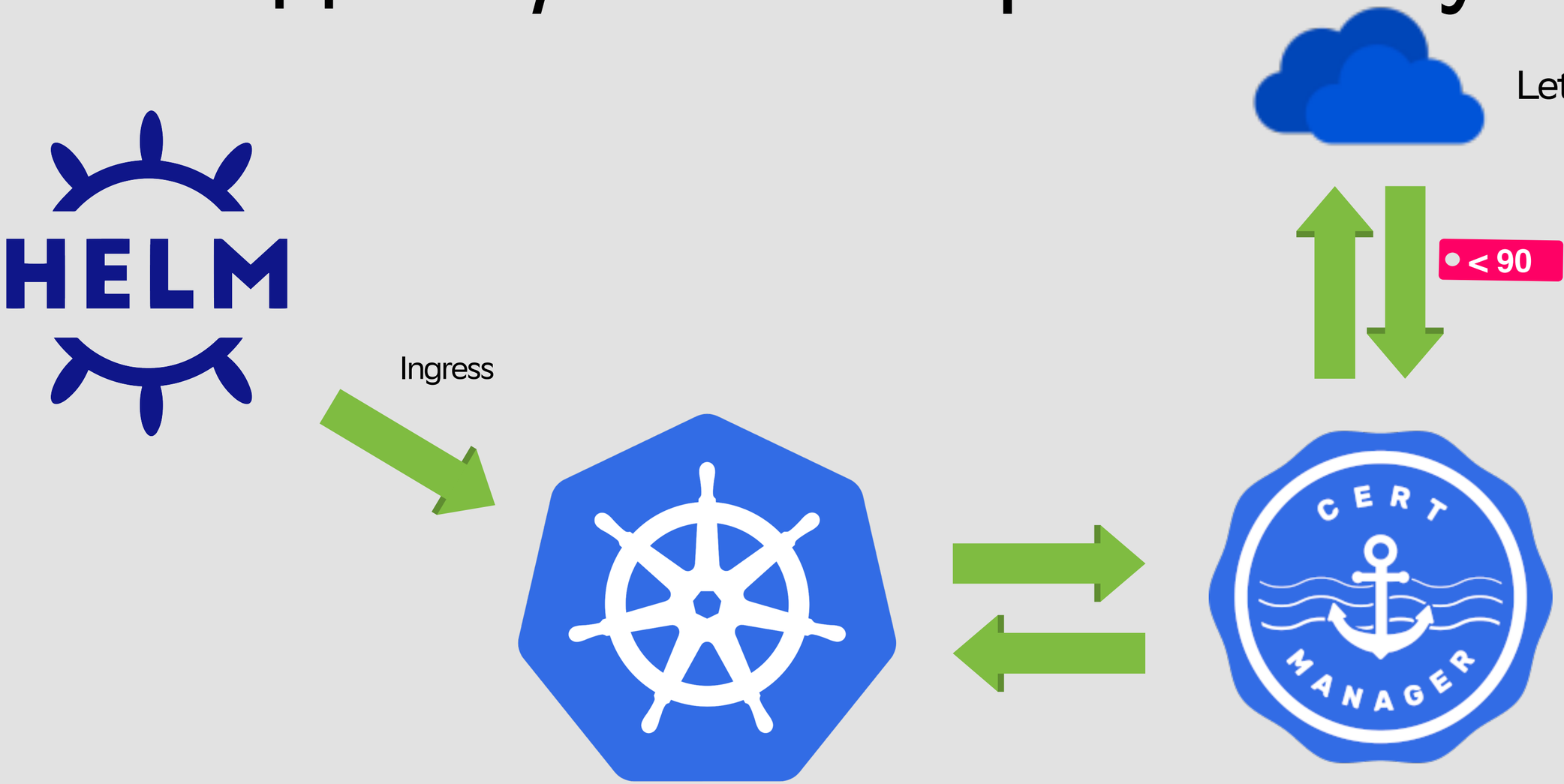
Whitelabel

Используются для среды разработки и продакшн среды

Issuer any

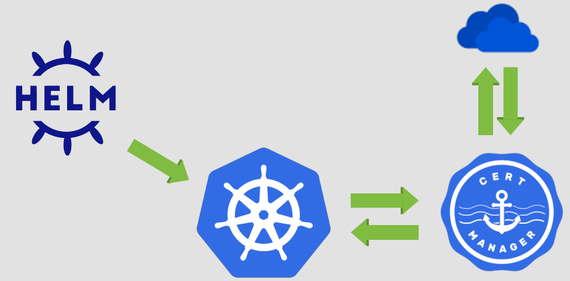
Wildcard / Per host

Очевидный/Самый простой путь



Плюсы подхода

+ Автоматизация
+ Простой мониторинг

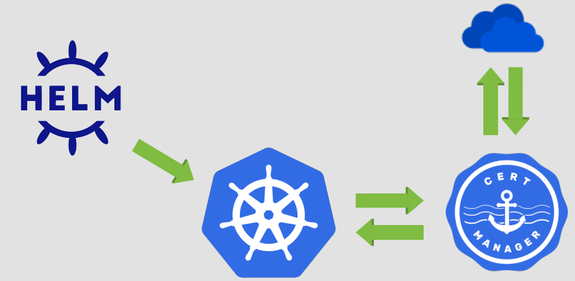


Плюсы подхода

+ Автоматизация
+ Простой мониторинг

Минусы подхода

- Отсутствует управление
- Дубли сертификатов
- Только <90 дней
- Проблемы с безопасностью
- Работа в рамках 1 кластера



Wildcard vs Per Host

Wildcard vs Per host

Кол-во сертификатов

Wildcard

*.example.com

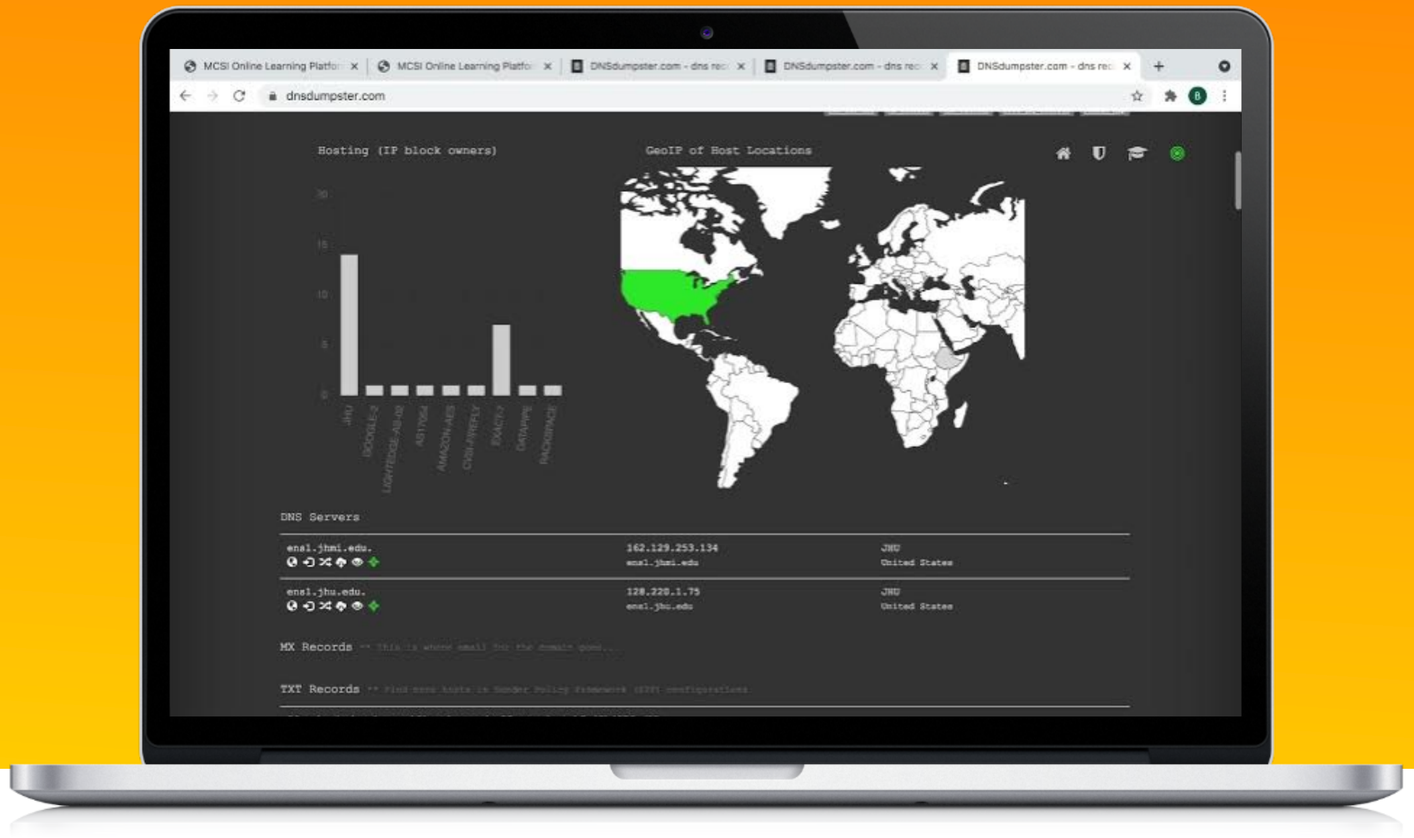
VS

Per host

host1.example.com
host2.example.com
….
host100.example.com
…
hostN.example.com

Wildcard vs Per host

Раскрытия информации



dnsdumpster

Дамп DNS зоны

Проверка sharing ip

Рисует схемы и …

dnsdumpster

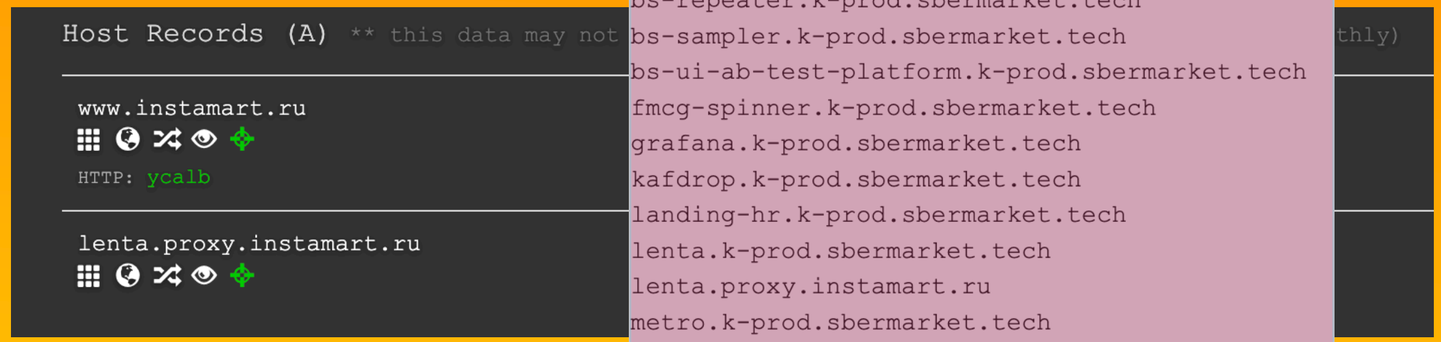
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

www.instamart.ru HTTP: ycalb	178.154.243.118
lenta.proxy.instamart.ru	130.193.56.45

Дамп DNS зоны

Проверка sharing ip

Рисует схемы и …




```
alertmanager.k-prod.sbermarket.tech
auth.k-prod.sbermarket.tech
bs-ab-admin.k-prod.sbermarket.tech
bs-admin-panel.k-prod.sbermarket.tech
bs-catalog.k-prod.sbermarket.tech
bs-mr-assigner-go.k-prod.sbermarket.tech
bs-rekki.k-prod.sbermarket.tech
bs-repeater.k-prod.sbermarket.tech
bs-sampler.k-prod.sbermarket.tech
bs-ui-ab-test-platform.k-prod.sbermarket.tech
fmcg-spinner.k-prod.sbermarket.tech
grafana.k-prod.sbermarket.tech
kafdrop.k-prod.sbermarket.tech
landing-hr.k-prod.sbermarket.tech
lenta.k-prod.sbermarket.tech
lenta.proxy.instamart.ru
metro.k-prod.sbermarket.tech
netbox.k-prod.sbermarket.tech
pochtovic.k-prod.sbermarket.tech
prometheus.k-prod.sbermarket.tech
replacoon.k-prod.sbermarket.tech
sbermarket.k-prod.sbermarket.tech
shopper.k-prod.sbermarket.tech
```

Дамп DNS зоны

Проверка sharing ip

Рисует схемы и …

Crt .sh

Полная и подробная история

Наличие расширенного поиска

Не прощает ошибок

Crt .sh

2021-02-15	2021-02-15	2021-05-16	vault-vpn.k-sec.sbermarket.tech	vault-vpn.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-15	2021-02-15	2021-05-16	vault-1-vpn.k-sec.sbermarket.tech	vault-1-vpn.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-15	2021-02-15	2021-05-16	vault-2-vpn.k-sec.sbermarket.tech	vault-2-vpn.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-15	2021-02-15	2021-05-16	vault-1-vpn.k-sec.sbermarket.tech	vault-1-vpn.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-15	2021-02-15	2021-05-16	vault-0-vpn.k-sec.sbermarket.tech	vault-0-vpn.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-15	2021-02-15	2021-05-16	vault-vpn.k-sec.sbermarket.tech	vault-vpn.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-15	2021-02-15	2021-05-16	vault-0-vpn.k-sec.sbermarket.tech	vault-0-vpn.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-13	2021-02-13	2021-05-14	sonar.k-sec.sbermarket.tech	sonar.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-13	2021-02-13	2021-05-14	sonar.k-sec.sbermarket.tech	sonar.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-10	2021-02-10	2021-05-11	airflow.k-content.sbermarket.tech	airflow.k-content.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-10	2021-02-10	2021-05-11	airflow.k-content.sbermarket.tech	airflow.k-content.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-09	2021-02-09	2021-05-10	bs-mr-assigner-go.k-prod.sbermarket.tech	bs-mr-assigner-go.k-prod.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-09	2021-02-09	2021-05-10	bs-mr-assigner-go.k-prod.sbermarket.tech	bs-mr-assigner-go.k-prod.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-09	2021-02-09	2021-05-10	defectdojo.k-sec.sbermarket.tech	defectdojo.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-09	2021-02-09	2021-05-10	defectdojo.k-sec.sbermarket.tech	defectdojo.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-09	2021-02-09	2021-05-10	defectdojo.k-sec.sbermarket.tech	defectdojo.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-09	2021-02-09	2021-05-10	defectdojo.k-sec.sbermarket.tech	defectdojo.k-sec.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-09	2021-02-09	2021-05-10	webhook.k-infra.sbermarket.tech	webhook.k-infra.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-09	2021-02-09	2021-05-10	webhook.k-infra.sbermarket.tech	webhook.k-infra.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-08	2021-02-08	2021-05-09	pims-api.sbermarket.tech	pims-api.sbermarket.tech pims.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3
2021-02-08	2021-02-08	2021-05-09	pims-api.sbermarket.tech	pims-api.sbermarket.tech pims.sbermarket.tech	C=US, O=Let's Encrypt, CN=R3

Полная и подробная история

Наличие расширенного поиска

Не прощает ошибок

Wildcard vs Per host

Масштаб при компрометации

Wildcard

*.example.com

VS

Per host

host1.example.com
host2.example.com
....
host100.example.com
...
hostN.example.com

Наш выбор

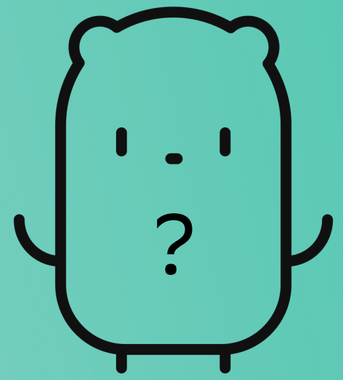
Wildcard

?Где найти идеального издателя

Free wildcard ACME DNS01

More More cert 14/30/90 day

Delegated Domains for DNS01



Let’s Encrypt

ZeroSSL

CloudFlare

Sectigo

DigiSert

Google Trust Services

Let’s Encrypt vs ZeroSSL

Let’s Encrypt vs ZeroSSL

Плюсы Let’s Encrypt

+ Бесплатность для wildcard
+ Поддержка SAN & wildcard
+ Поддержка RSA/ECDSA сертификатов
+ Возможность увеличить raite limits
+ Delegated Domains for DNS01

Плюсы Let’s Encrypt

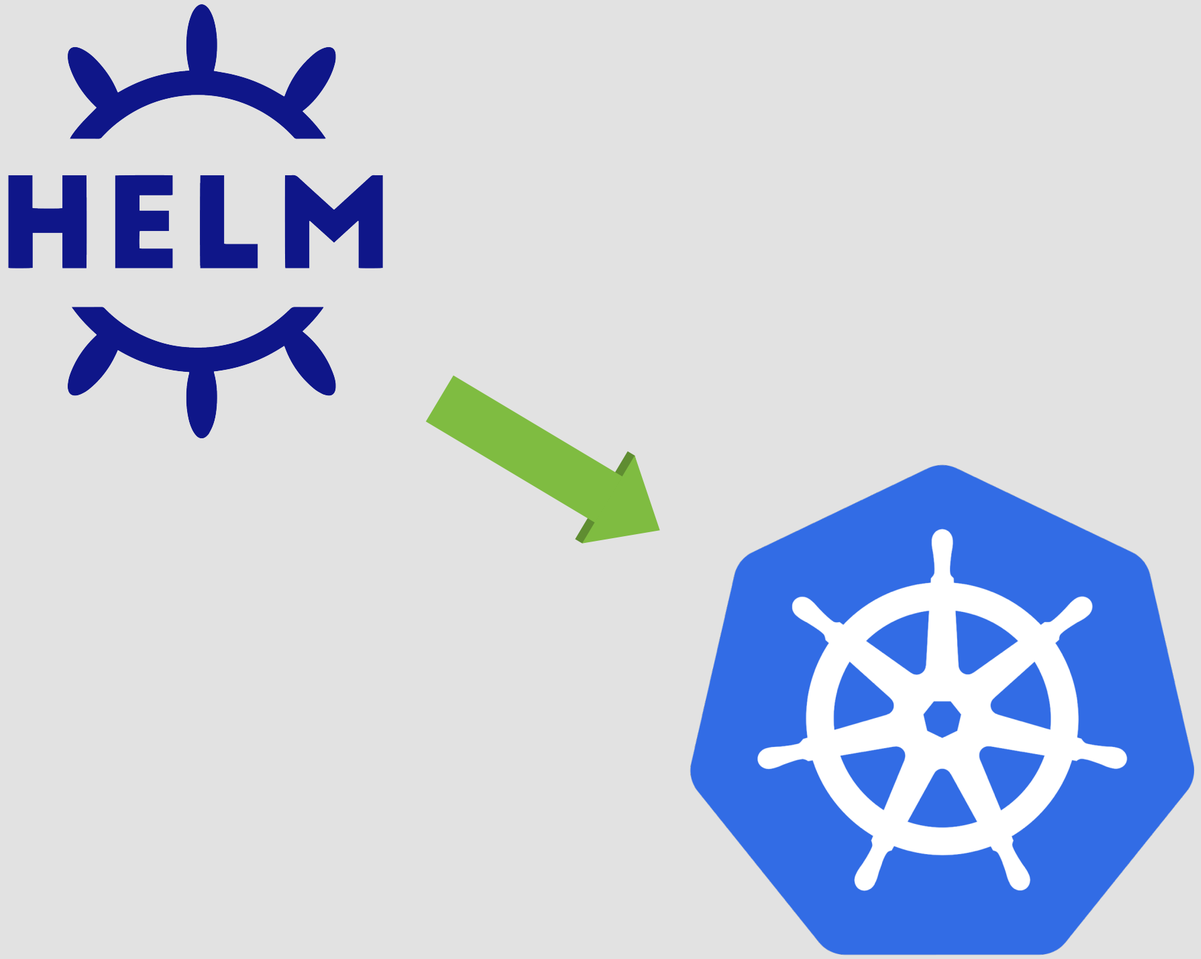
+ Бесплатность для wildcard
+ Поддержка SAN & wildcard
+ Поддержка RSA/ECDSA сертификатов
+ Возможность увеличить raite limits
+ Delegated Domains for DNS01

Минусы Let’s Encrypt

- Raite Limits API
- Возможные санкции

Kubernetes

Начало (выпуск сертификата)



внутри

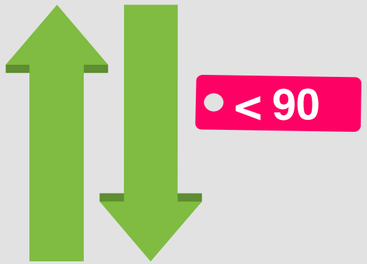
```yaml
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: secret-name-wild-le
  namespace: release-namespace
  annotations:
    meta.helm.sh/release-name: release-name
    meta.helm.sh/release-namespace: release-namespace
  labels:
    app.kubernetes.io/managed-by: Helm
spec:
  dnsNames:
    - '*.examle.com'
  issuerRef:
    kind: ClusterIssuer
    name: issuer-name-dns
  secretName: secret-name-wild-le
  secretTemplate:
    annotations:
      replicator.v1.mittwald.de/replication-allowed: 'true'
      replicator.v1.mittwald.de/replication-allowed-namespaces: .*

```

Запрос выпуска сертификата через let’s Encrypt

Начало (выпуск сертификата)

Let’s Encrypt



Начало (выпуск сертификата)

XXX +

Доменов

~~http~~

~~access~~

tech

Let’s Encrypt

DNS01 Challenge

Delegated Domains for DNS01

внутри

Delegated Domains for DNS01

https://cert-manager.io/docs/configuration/acme/dns01/#configuring-dns01-challenge-provider

```
_acme-challenge.example.com    IN  CNAME   _acme-challenge.less-privileged.example.org.
```

Исходный домен

Домен делегации

внутри

Delegated Domains for DNS01

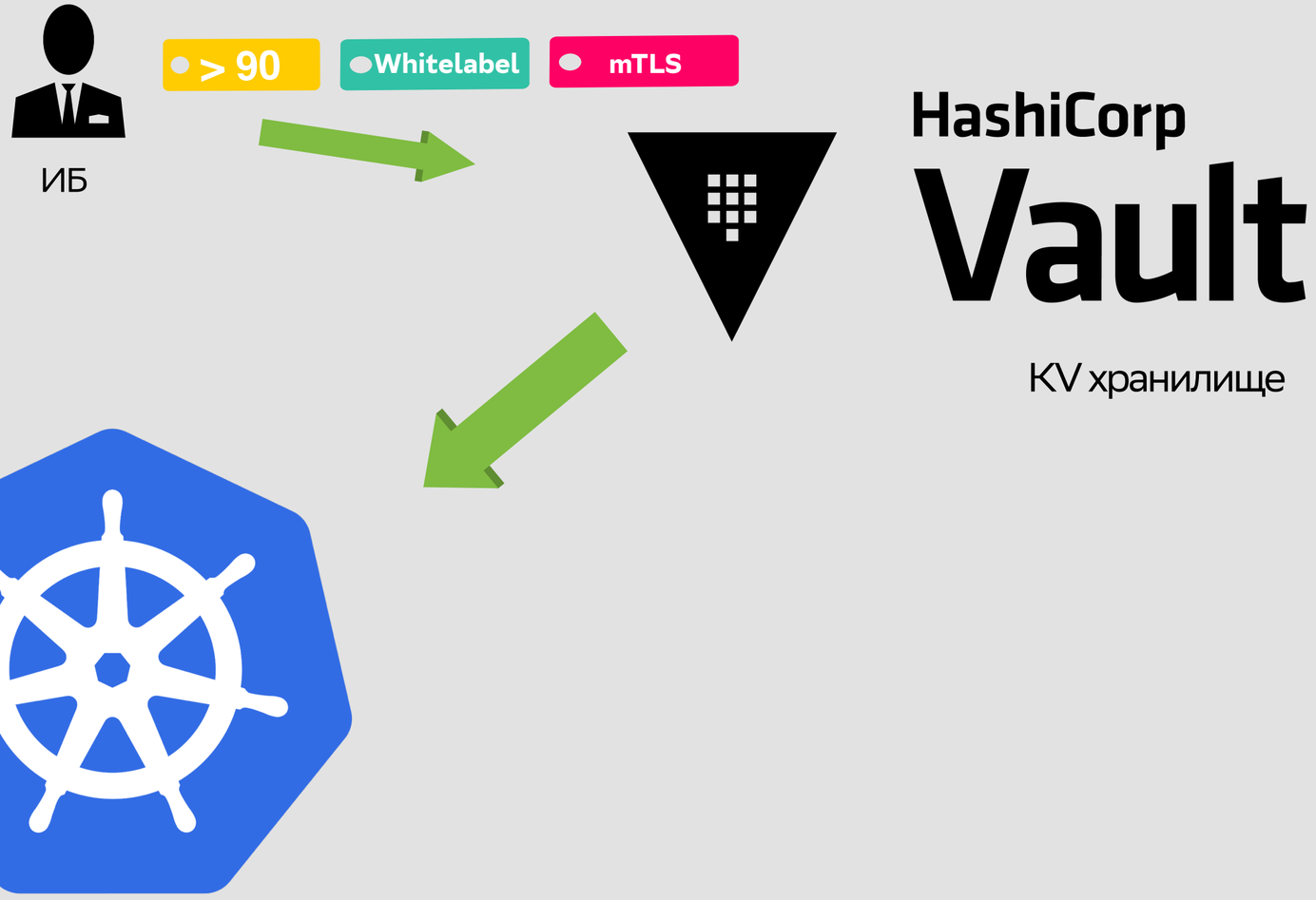
https://cert-manager.io/docs/configuration/acme/dns01/#configuring-dns01-challenge-provider

```
_acme-challenge.example.com      IN  CNAME   _acme-challenge.less-privileged.example.org.
_acme-challenge.www.example.com  IN  CNAME   _acme-challenge.less-privileged.example.org.
_acme-challenge.foo.example.com  IN  CNAME   _acme-challenge.less-privileged.example.org.
_acme-challenge.bar.example.com  IN  CNAME   _acme-challenge.less-privileged.example.org.
```

Исходный домен

Домен делегации

Начало (создание сертификата)

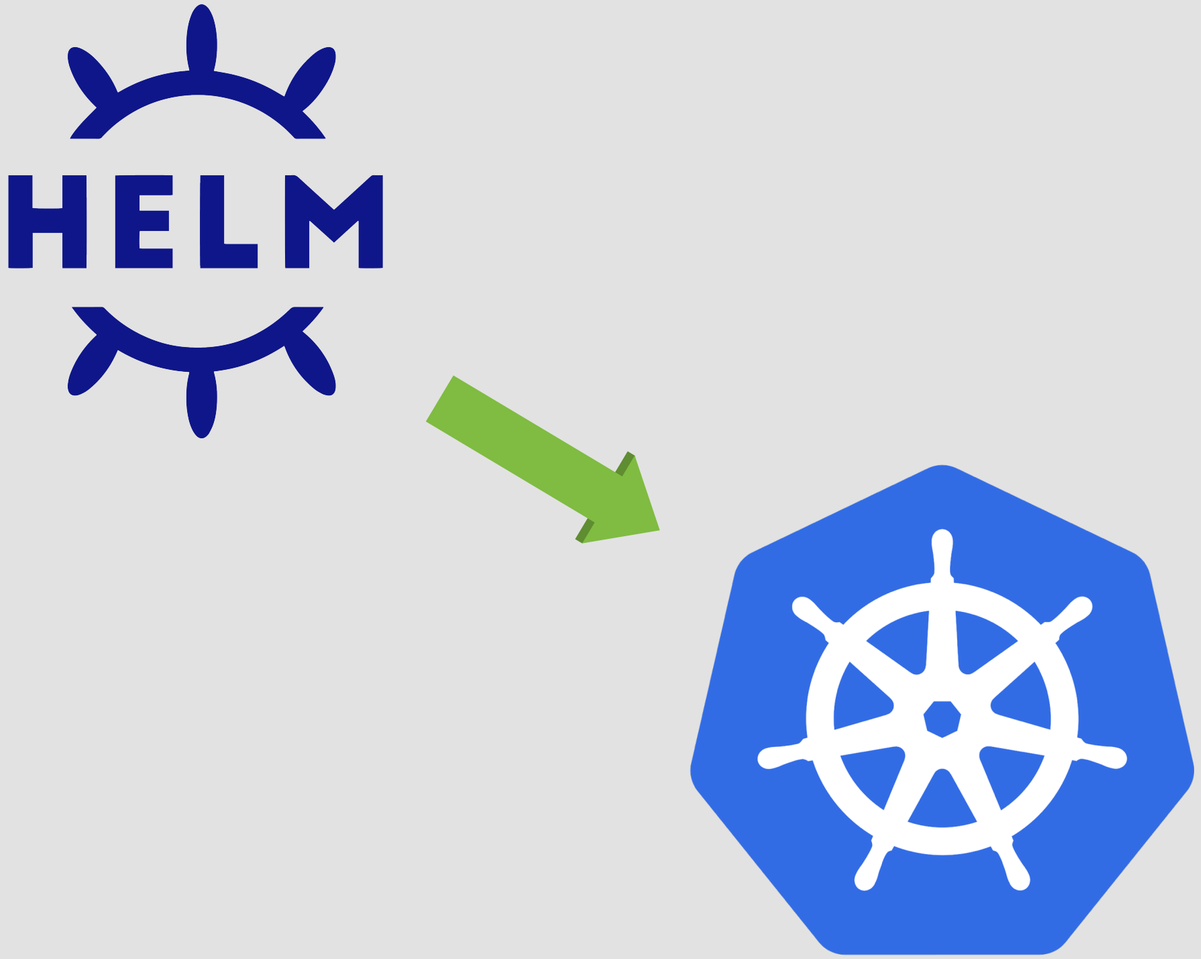


внутри

banzaicloud/vault-secrets-webhook

https://bank-vaults.dev/docs/mutating-webhook

Начало (выпуск сертификата)



внутри

banzaicloud/vault-secrets-webhook

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: secret-name-wild-vault
  namespace: release-namespace
  annotations:
    vault.security.banzaicloud.io/vault-addr: https://vault.local
    vault.security.banzaicloud.io/vault-path: vault-patch
    vault.security.banzaicloud.io/vault-role: vault-role
    vault.security.banzaicloud.io/vault-serviceaccount: vault-sa
type: kubernetes.io/tls
data:
  tls.crt: "dmF1bHQ6azhzL2RhdGEvcGF0Y2gvdG8vY2VydGlmaWNhdGUjdGxzLmNydAo="
  tls.key: "dmF1bHQ6azhzL2RhdGEvcGF0Y2gvdG8vY2VydGlmaWNhdGUjdGxzLmtleQo="
```

Запрос сертификата из vault

внутри

banzaicloud/vault-secrets-webhook

```
  annotations:
    vault.security.banzaicloud.io/vault-addr: https://vault.local
    vault.security.banzaicloud.io/vault-path: vault-patch
    vault.security.banzaicloud.io/vault-role: vault-role
    vault.security.banzaicloud.io/vault-serviceaccount: vault-sa
type: kubernetes.io/tls
data:
  tls.crt: "dmF1bHQ6azhzL2RhdGEvcGF0Y2gvdG8vY2VydGlmaWNhdGUjdGxzLmNydAo="
  tls.key: "dmF1bHQ6azhzL2RhdGEvcGF0Y2gvdG8vY2VydGlmaWNhdGUjdGxzLmtleQo="

#где
  tls:crt: "vault:k8s/data/patch/to/certificate#tls.crt"
  tls.key: "vault:k8s/data/patch/to/certificate#tls.key"
```

Запрос сертификата из vault

tech

внутри

banzaicloud/vault-secrets-webhook

```
  annotations:
    vault.security.banzaicloud.io/vault-addr: https://vault.local
    vault.security.banzaicloud.io/vault-path: vault-patch
    vault.security.banzaicloud.io/vault-role: vault-role
    vault.security.banzaicloud.io/vault-serviceaccount: vault-sa
type: kubernetes.io/tls
data:
  tls.crt: "dmF1bHQ6azhzL2RhdGEvcGF0Y2gvdG8vY2VydGlmaWNhdGUjdGxzLmNydAo="
  tls.key: "dmF1bHQ6azhzL2RhdGEvcGF0Y2gvdG8vY2VydGlmaWNhdGUjdGxzLmtleQo="

#где
  tls:crt: "vault:k8s/data/patch/to/certificate#tls.crt"
  tls.key: "vault:k8s/data/patch/to/certificate#tls.key"
```

Запрос сертификата из vault

внутри

kubernetes-replicator

https://github.com/mittwald/kubernetes-replicator

Функционал:

- Синхронизация Secret между NameSpace

внутри

kubernetes-replicator

https://github.com/mittwald/kubernetes-replicator

```
replicator.v1.mittwald.de/replication-allowed: 'true'
replicator.v1.mittwald.de/replication-allowed-namespaces: .*
```

Секрет **Источник**

внутри

kubernetes-replicator

https://github.com/mittwald/kubernetes-replicator

```
replicator.v1.mittwald.de/replication-allowed: 'true'
replicator.v1.mittwald.de/replication-allowed-namespaces: .*
```

Секрет **Источник**

внутри

kubernetes-replicator

https://github.com/mittwald/kubernetes-replicator

Секрет **Приемник**

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: secret-name-vault
  annotations:
    replicator.v1.mittwald.de/replicate-from: ns/secret-name-vault
    replicator.v1.mittwald.de/replicated-from-version: ''
type: kubernetes.io/tls
data:
  tls.key: ""
  tls.crt: ""
```

внутри

kubernetes-replicator

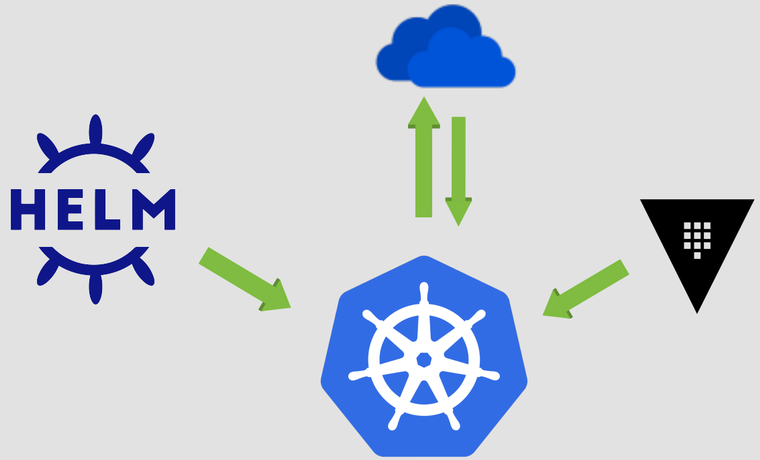
https://github.com/mittwald/kubernetes-replicator

Секрет **Приемник**

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: secret-name-vault
  annotations:
    replicator.v1.mittwald.de/replicate-from: ns/secret-name-vault
    replicator.v1.mittwald.de/replicated-from-version: ''
type: kubernetes.io/tls
data:
  tls.key: ""
  tls.crt: ""
```

Плюсы подхода

+ Декларативный подход
+ Мониторинг состояния

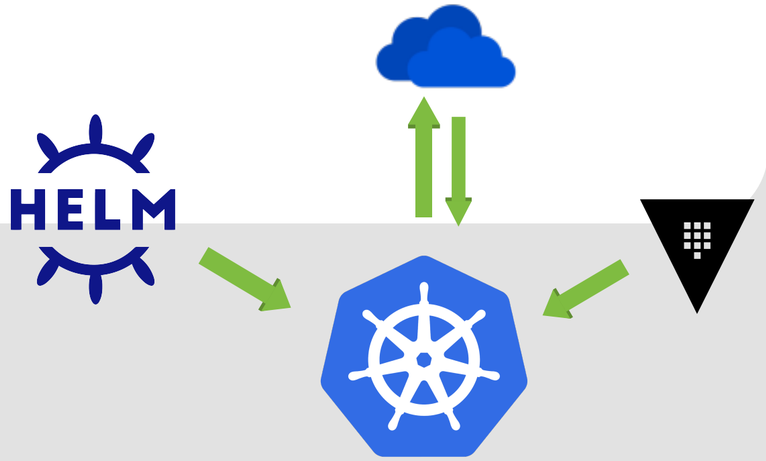


Плюсы подхода

+ Декларативный подход
+ Мониторинг состояния

Минусы подхода

- Сложность обновления (helm upgrade —force)
- Наличие копии сертификата в каждом NameSpace

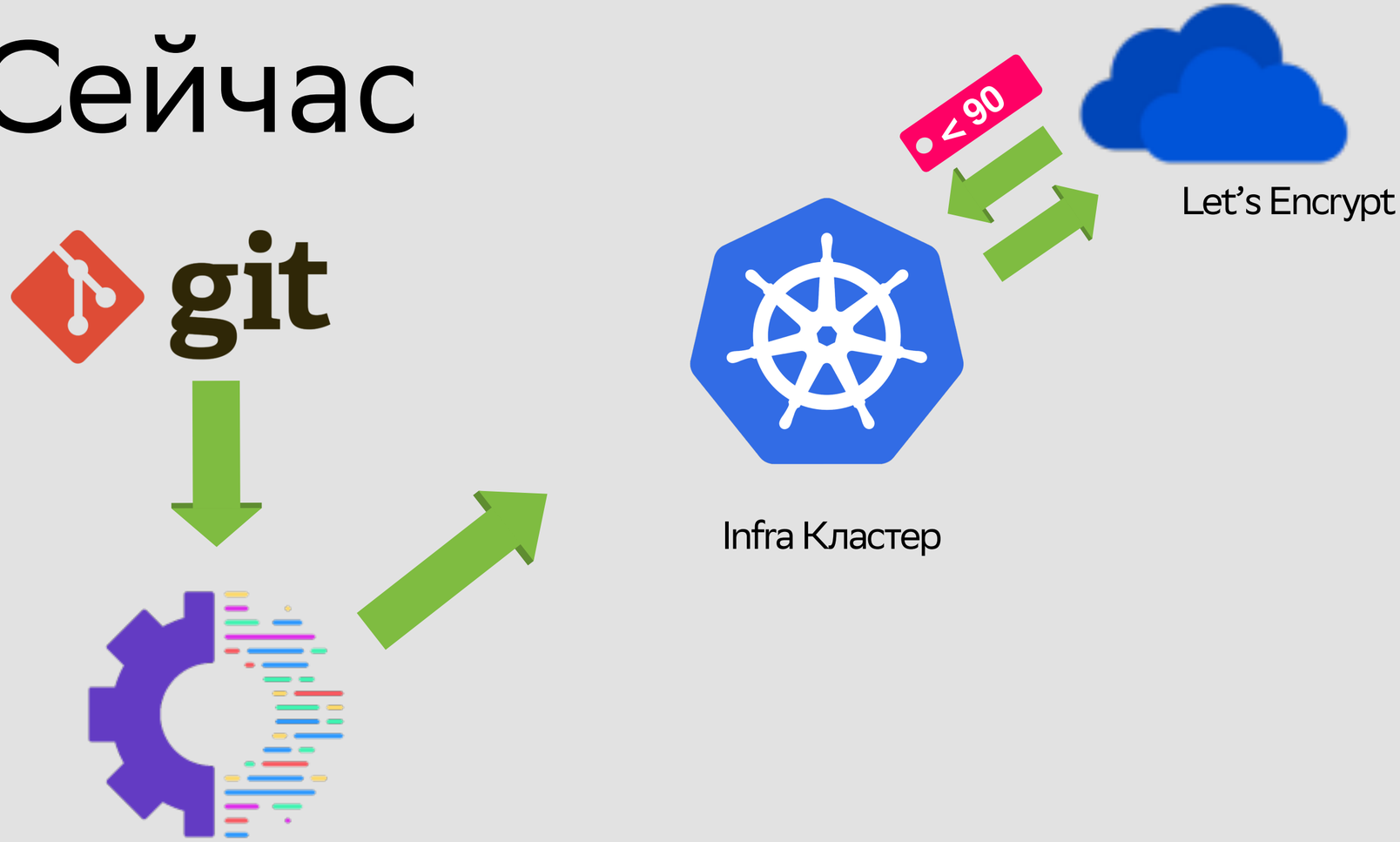


Сейчас

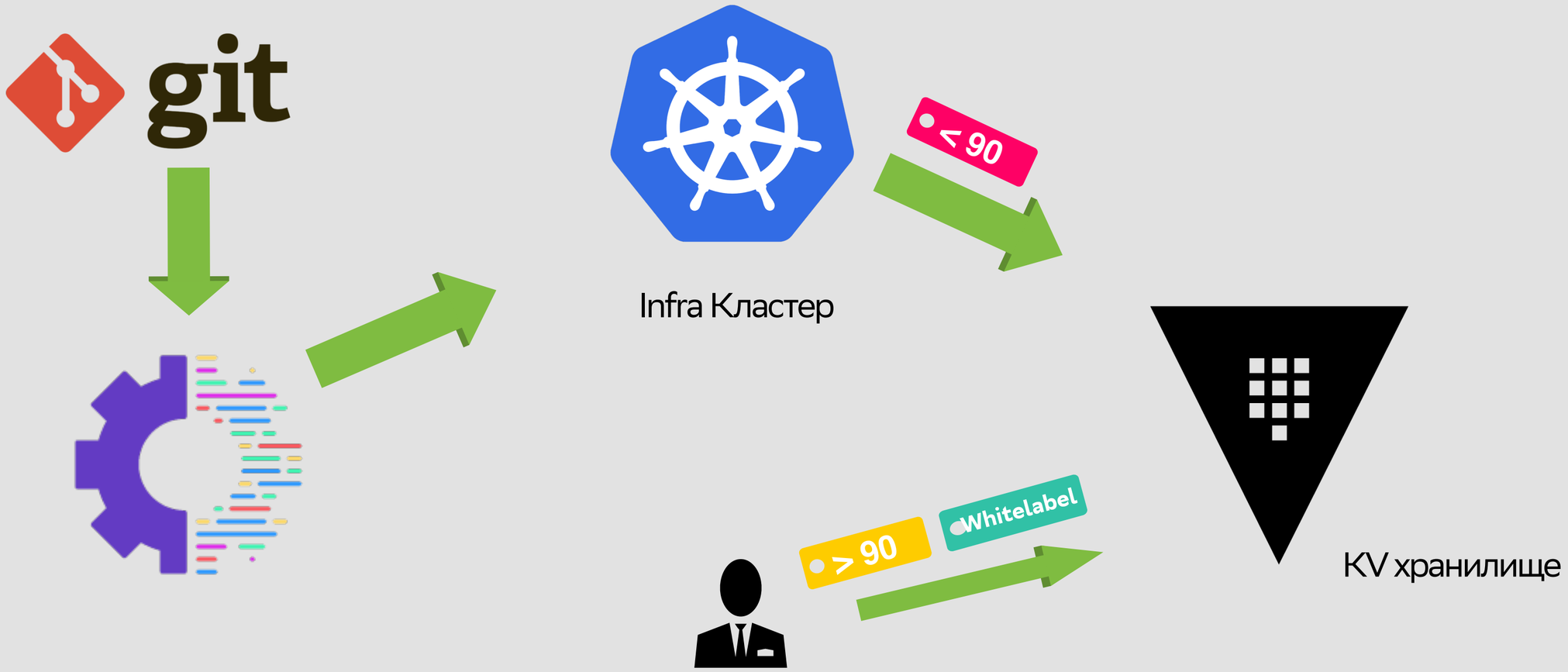
Все запросы
- Создание
- Отзыв

Фиксируются в Git

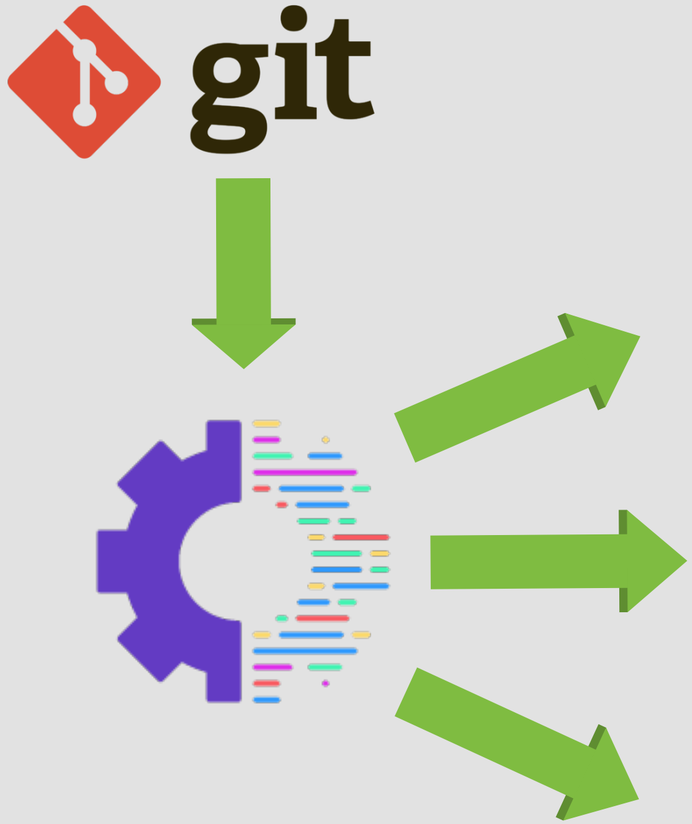
Сейчас

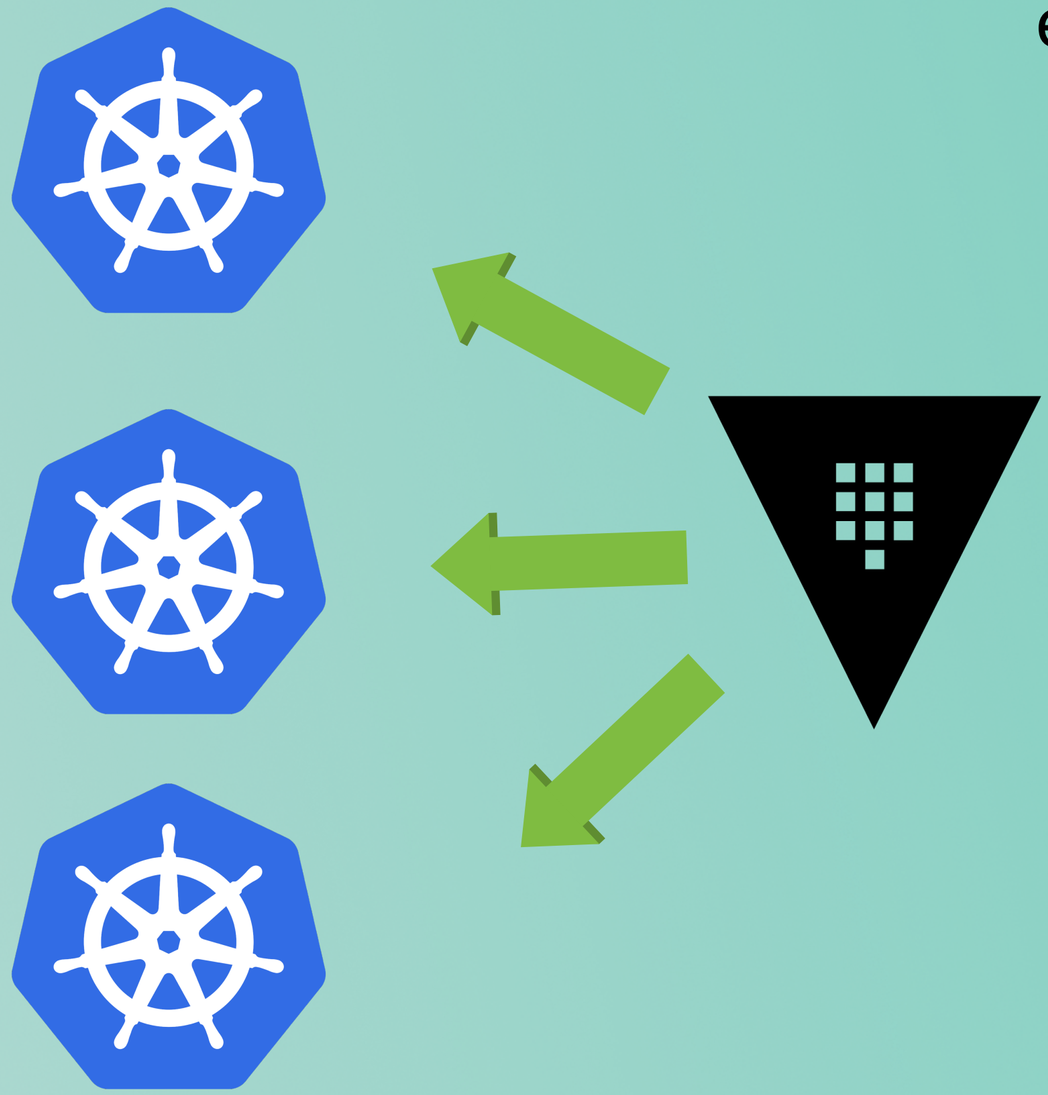


Сейчас



Сейчас





external-secrets

внутри

external-secrets

https://external-secrets.io/

внутри

external-secrets

https://external-secrets.io/

Функционал:

- Синхронизация с Vault (и многими другими)
- Мониторинг
- Выборочное копирование Secret in NameSpace

Плюсы подхода

+ Мониторинг каждого шага
+ Контроль целостности
+ Постоянная / периодическая синхронизация с vault
+ Версионность
+ Единое место хранения
+ Быстрая и массовая замена сертификата (~ 10минут)

Плюсы подхода

+ 2 оператора (Cert manager + External-secrets)
+ Мониторинг каждого шага
+ Постоянная / периодическая синхронизация с vault
+ Версионность
+ Единое место хранения
+ Быстрая и массовая замена сертификата (~ 5минут)

Минусы подхода

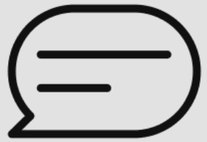
- Доступы к сертификатам на уровне NameSpace
- Все еще сложный процесс

Мониторинг

X.509 Certificate Exporter

https://github.com/enix/x509-certificate-exporter

Мониторинг



X.509 Certificate Exporter

Функционал:

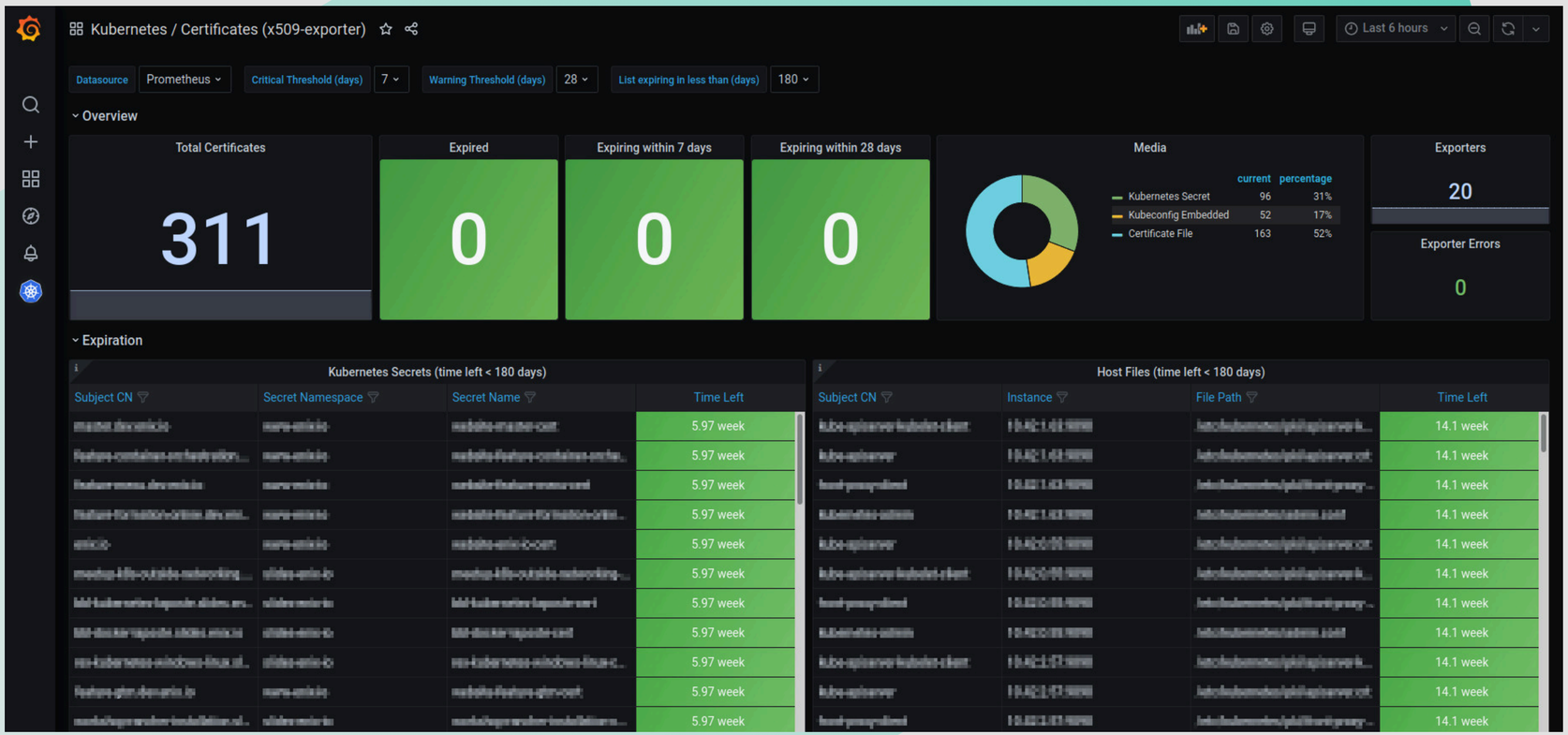
- Мониторинг kubernetes.io/tls & opaque
- Проверка Валидности
- Простой и понятный Grafana Dashboard

Мониторинг

X.509 Certificate Exporter

Функционал:

- Мониторинг kubernetes.io/tls & opaque
- Проверка Валидности
- Проверка отзыва
- Простой и понятный Grafana Dashboard



Источник: https://github.com/enix/x509-certificate-exporter/blob/main/docs/grafana-dashboard.jpg

Мониторинг

ssl_exporter

https://github.com/ribbybibby/ssl_exporter

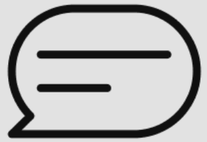
Мониторинг

ssl_exporter

Функционал:

- Проверка отзыва по OCSP (из коробки)
- Проверка отзыва по CRL (патч)

Мониторинг



vault_ssl_exporter

Своя разработка (ведем работы для публичной публикации)

Чистота и Забота

Авто очистка Secrets

Args:
-enable-certificate-owner-ref=true

Helm:

path: /global/enableCertificateOwnerRef
value: true

Чистота и Забота

Авто очистка Secrets

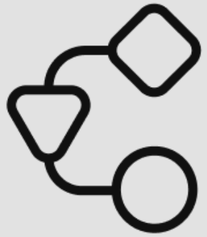
Args:
-enable-certificate-owner-ref=true

Helm:

path: /global/enableCertificateOwnerRef
value: true

ExternalSecret:
path: /spec/target/deletionPolicy
value: Delete

Подводя итоги



Декларативный контроль шагов

Помнить о безопасности

Мониторинг на всех этапах

Подводя итоги

Декларативный контроль шагов

Помнить о безопасности

Мониторинг на всех этапах

Управлять TLS-сертификатами легко

спасибо за внимание

tech