3 июня 2025 Москва, LOFT HALL#2

БЕКОН '25

Конференция по БЕзопасности
КОНтейнеров и контейнерных сред

Kyverno: Рецепты правильного приготовления

Евгений Берендяев

Kubernetes-инженер, Авито

whoami

БЕКОН

- Инженер эксплуатации Kubernetes в avito.tech
- У нас большой контакт с безопасниками
- **60** кластеров в эксплуатации
- Прод кластера – от **100** до **500** нод,
  до **25000** подов
- **Bare metal**, облака, виртуальные машины

В докладе

БЕКОН

- Зачем вам Policy Engine? А почему Kyverno?
- Как деплоить и обновлять Kyverno?
- Как защититься от отказа Kyverno? Как не навредить Kubernetes’у?
- Как обеспечить observability?
- Как дёшево сделать нагрузочный тест?
- Как гибко деплоить политики?
- Как сделать CI для политик?
- Как дела с нативными Kubernetes Policy? Стоит ли внедрять?

Зачем вам Policy Engine?

Зачем Policy Engine?

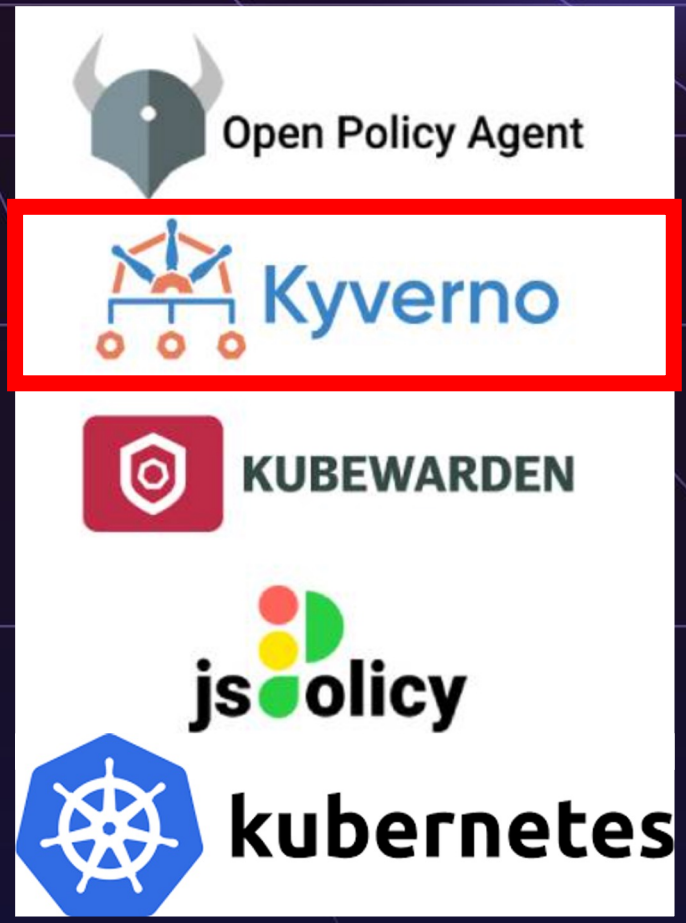
БЕКОН

- Превентивный харденинг
- Митигация уязвимостей
  - CVE-2024-7646 (NGINX controller)
  - CVE-2025-1767 (gitRepo volumes)
  - CVE-2025-32445 (Argo events)
- Заковыристые правила
- Стандартизация
- Мутация, генерация, очистка ресурсов

Почему Kyverno?

БЕКОН

- Простой DSL
- Устроил и нас, и безопасников
- Пользуемся 1.12.5. Самая свежая – 1.14.1.



Все Policy Engine…

БЕКОН

- Имеют кучу CR
- Забивают etcd
- Нагружают kube-apiserver
- Нужны тесты политик
- Нужна гибкость политик
- Нужна защита от отказа PE
- Если вы пишете свой PE – вам всё это **тоже придётся предусмотреть**

Вам придётся

БЕКОН

- Настроить мониторинг и алертинг PE
- Проверить и допилить мониторинг и алертинг Kubernetes Control Plane
- Донастроить kube-apiserver и etcd
- Настроить тесты и деплой
- **Особенно** если кластеров много
- **Особенно** если они большие
- **Всё это касается любого Policy Engine**

БЕКОН

Как деплоить и обновлять Kyverno?

Матрица совместимости. Официальная. Суровая.

БЕКОН

Версия Kyverno	Kubernetes, минимальная	Kubernetes, максимальная
1.6.x	1.16	1.23
1.7.x	1.21	1.23
1.8.x	1.23	1.25
1.9.x	1.24	1.26
1.10.x	1.24	1.26
1.11.x	1.25	1.28
1.12.x	1.26	1.29
1.13.x	1.28	1.31
1.14.x	1.29	1.32

Взято отсюда: раз, два

Подход 1. Строгое соответствие матрице

БЕКОН

Плюсы

- Уверенность, что всё будет работать «как надо»

Минусы

- Разные метрики
- Разные спеки политик
- Разные values в helm
- Разная реализация внутренних механизмов
- Это **постоянно** меняется

Подход 2. Одна версия на все кластера

БЕКОН

Плюсы

- Отсутствует оверхед

Минусы

- **Необходимость тщательной выверки политик**
- Поддержка кастомного чарта

Итог

- Подход работает. Но с ограничениями

Как модифицировать чарт?

БЕКОН

- Убрать хардкод версии k8s из Chart.yaml
- If/else для Job’ов

```
# kubeVersion: '≥1.25.0-0'
```

```
{{- if (semverCompare "<1.21-0" .Capabilities.KubeVersion.GitVersion) }}
apiVersion: batch/v1beta1
{{- else }}
apiVersion: batch/v1
{{- end }}
```

Немного об ArgoCD

БЕКОН

- AppSets – способ раскатки на много кластеров
- Это наш типовой аппсет

```yaml
---

apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: coredns
  namespace: argocd
spec:
  generators:
    - merge:
        mergeKeys:
          - server
        generators:
          - clusters:
              selector:
                matchLabels:
                  argocd.argoproj.io/secret-type: cluster
                matchExpressions:
                  - key: k8sversion
                    operator: NotIn
                    values:
                      - [redacted]
              values:
                limits-memory: '2Gi'
                requests-cpu: '2'
                requests-memory: '2Gi'
                version: '[redacted]'
```

Сделайте рубильник, отключающий kyverno

БЕКОН

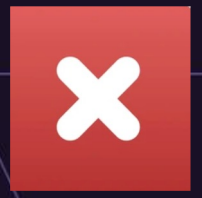
- ArgoCD label selectors

```
generators:
  - clusters:
      selector:      Kirill Kovalev, 23 months ago
        matchLabels:
          argocd.argoproj.io/secret-type: cluster
        matchExpressions:
          - key: kyverno-disabled
            operator: NotIn
            values:
              - "true"
```

Не работайте с лейблами через argocd-cli!

БЕКОН

```
→  ~ kubectl -n argocd label secrets \
> ${cluster-secret} kyverno-disabled=true
```



```
→  ~ argocd cluster set ${cluster} \
> --label kyverno-disabled=true
```

Важно: защитите ArgoCD!!!

БЕКОН

- Есть критическая уязвимость CVE-2024-31989
- Пароль на redis
- Запрет на уровне NetworkPolicy
- Идеально – унести в отдельный кластер
- Подробно здесь: 33 минута

Сделайте регламент и чеклист апгрейда

БЕКОН

Проверка фичей:
- Новые функции
- Изменённые функции
- Фикс старых проблем
- Deprecations политик

Проверка багов:
- Баги в отдаче метрик
- **Баги в удалении репортов**
- **Баги с OOM и крашами контейнеров**

Сетап в тест

Cooldown период (проверка работы политик)

Сетап в 1 прод

Сетап всюду

Summary #1

БЕКОН

- Много версий – много печали
- Попробуйте одну версию для всего
- Сделайте рубильник отключения Kyverno
- Формализуйте процесс апгрейда версии

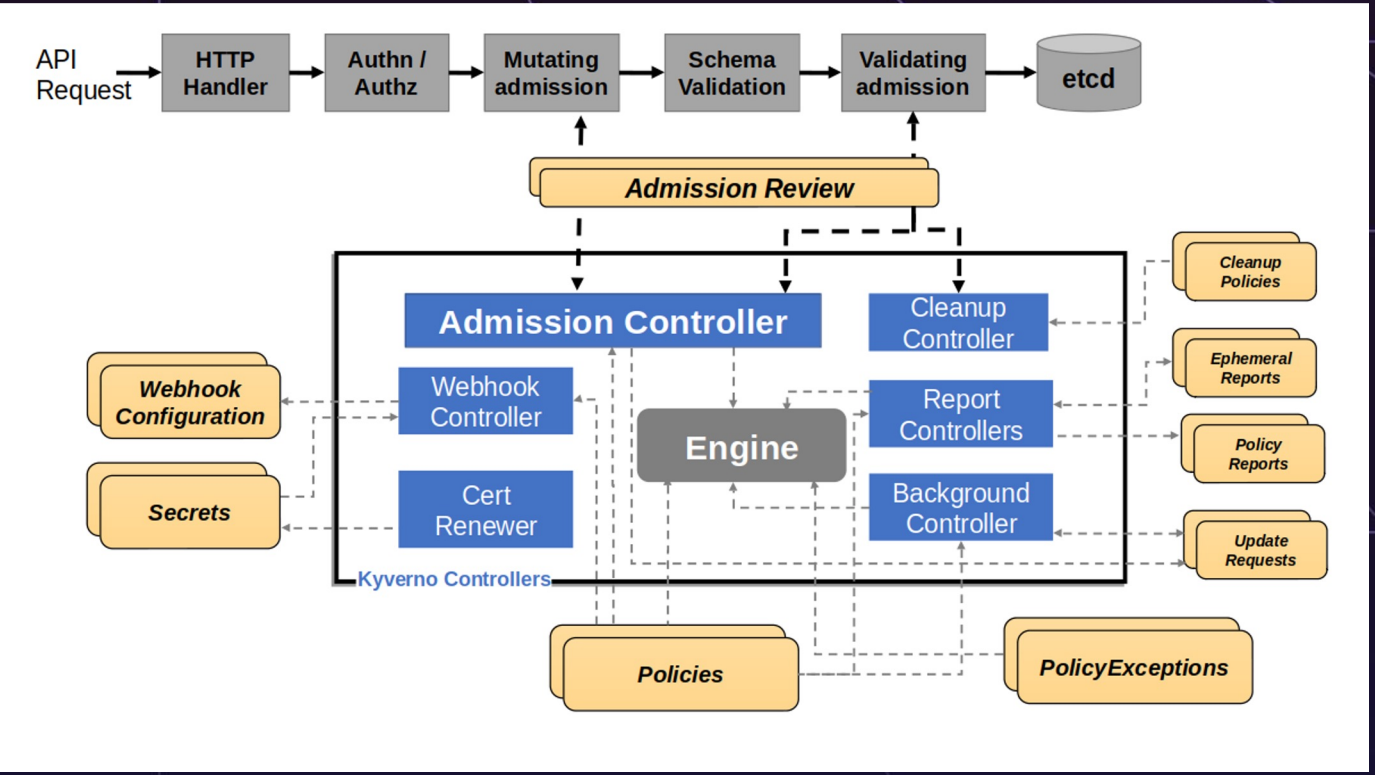
БЕКОН

Как защититься от отказа Kyverno и k8s Control Plane?

Отказоустойчивость сетапа

БЕКОН

- Admission Controller 3 реплики
- Background Controller - 2,
  Report Controller - 2,
  Cleanup Controller - 2
- **Сделайте алерт на недоступность Kyverno**
- forceFailurePolicyIgnore – не на проде!



Почему может рухнуть etcd

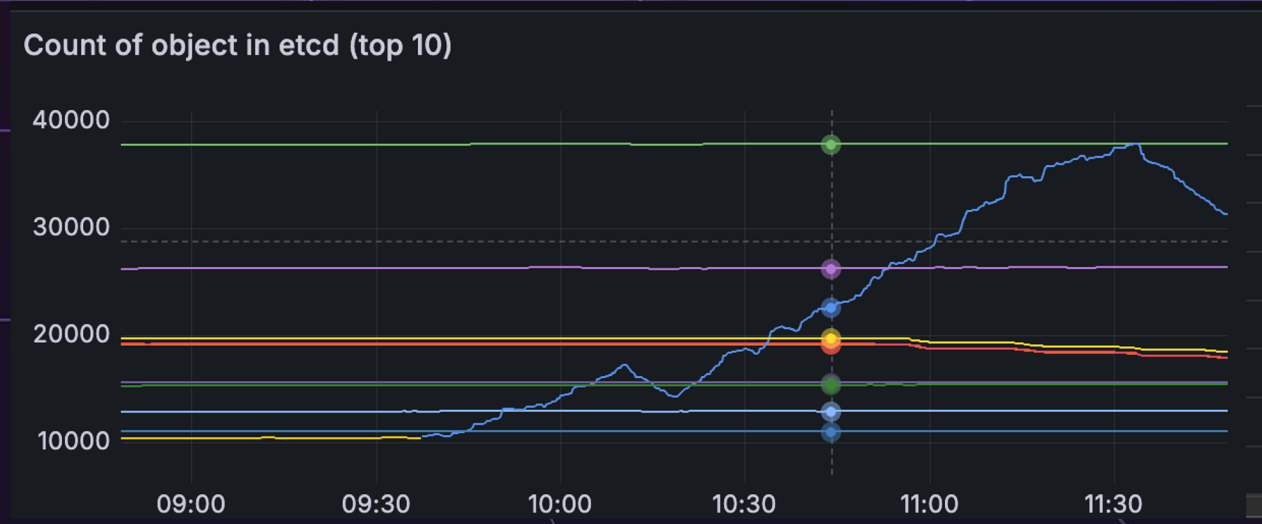
БЕКОН

- Тысячи CR Reports
- etcd закрывается на запись, если распух
- Некоторые версии Kyverno багуют в части удаления репортов (1.12.2)
- 3 раза прилёг прод

Как обезопасить etcd

БЕКОН

- quota-backend-bytes: 8 GB
- etcd_mvcc_db_total_size_in_bytes / etcd_server_quota_backend_bytes
- Гайд, как делать etcd дефрагментацию
- apiserver_storage_objects{resource=~".*kyverno.*"}
- workqueue_depth{job="kube-controller-manager", name="garbage_collector_attempt_to_delete"}



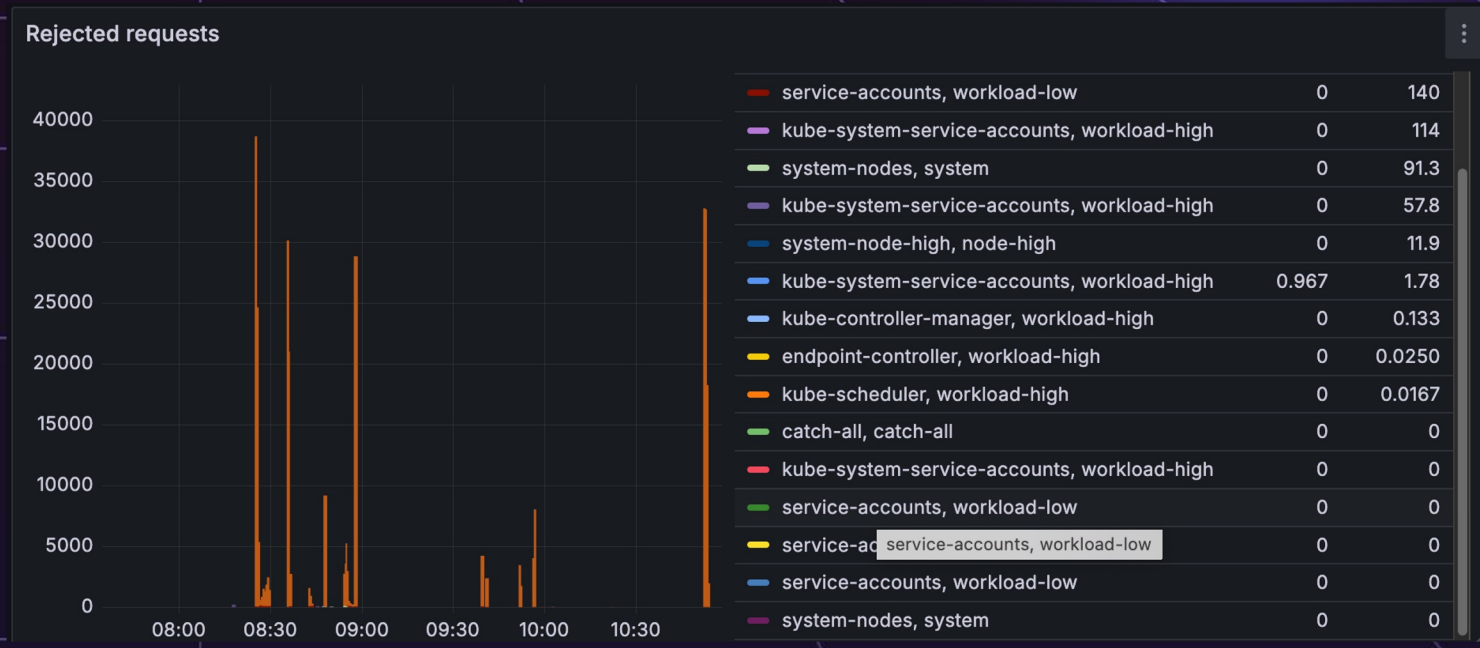
Как обезопасить kube-apiserver

БЕКОН

- API Priority and Fairness (K8s 1.18+)
- В чарте есть готовые настройки
- Готовый APF дашборд
- Рассчитайте свои (пример)

У нас:

- Хотим обрабатывать 300 rps от kyverno
- nominalConcurrencyShares = 30
- queues=16
- queuesLengthLimit=75
- handSize=4



Summary #2

БЕКОН

- High availability контроллеров
- Настройте метрики/алерты/дашборды etcd
- Настройте метрики/алерты/дашборды kube-apiserver
- Начните пользоваться APF

БЕКОН

Как обеспечить observability?

Что делать с метриками

БЕКОН

- Выберите критичные метрики
- Режьте ненужные
  в scrape_config vmagent
- Дропайте ненужные лейблы
  (bucket boundaries)

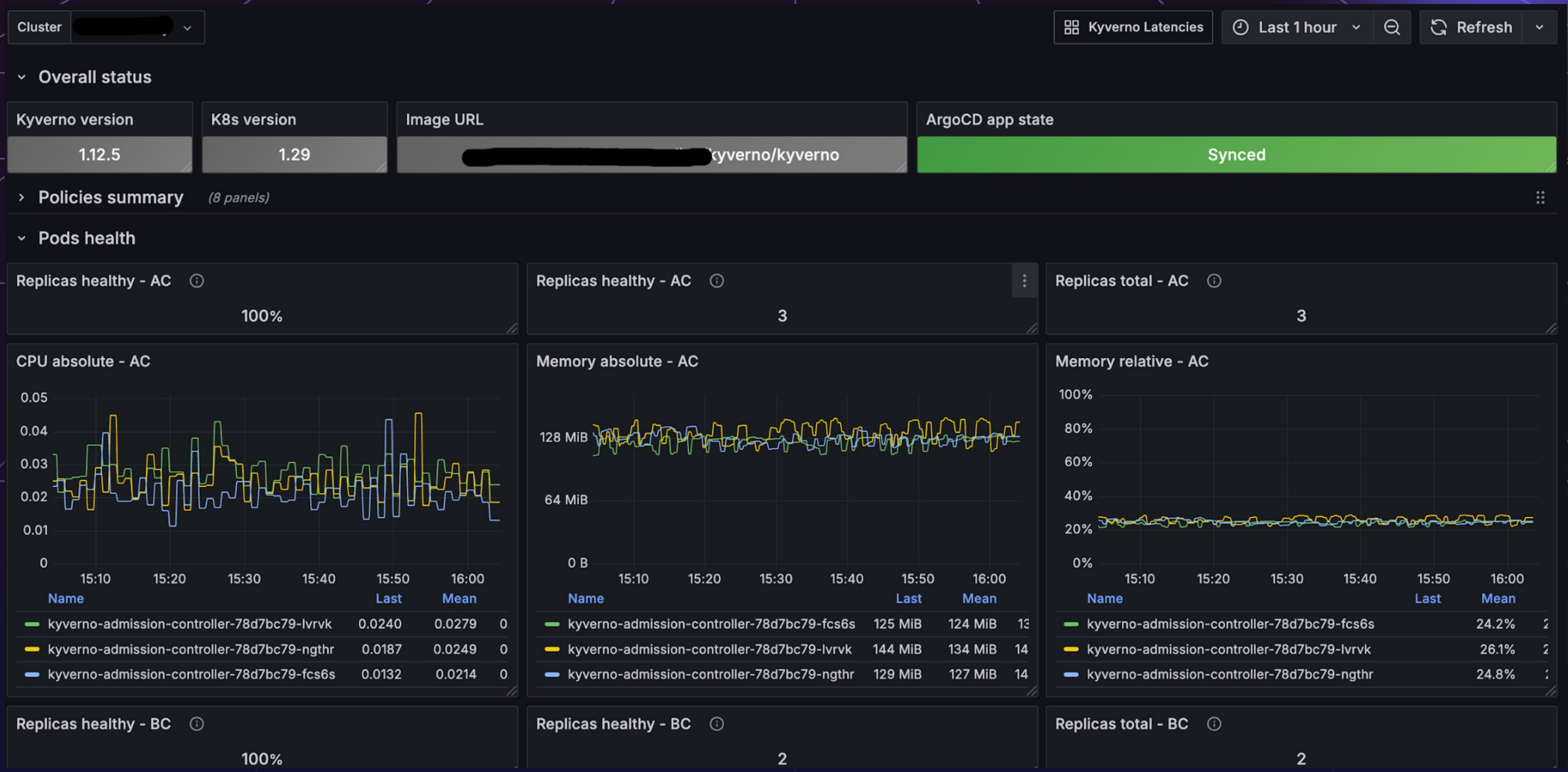
Содержание раздела

Критичные метрики

- kyverno_policy_rule_info_total
- kyverno_policy_results_total
- kyverno_http_requests_total
- kyverno_http_requests_duratior
- kyverno_policy_execution_durat
- kyverno_admission_review_dur
- kyverno_admission_requests_t
- kyverno_controller_drop_total
- kyverno_policy_changes_total
- kyverno_client_queries_total

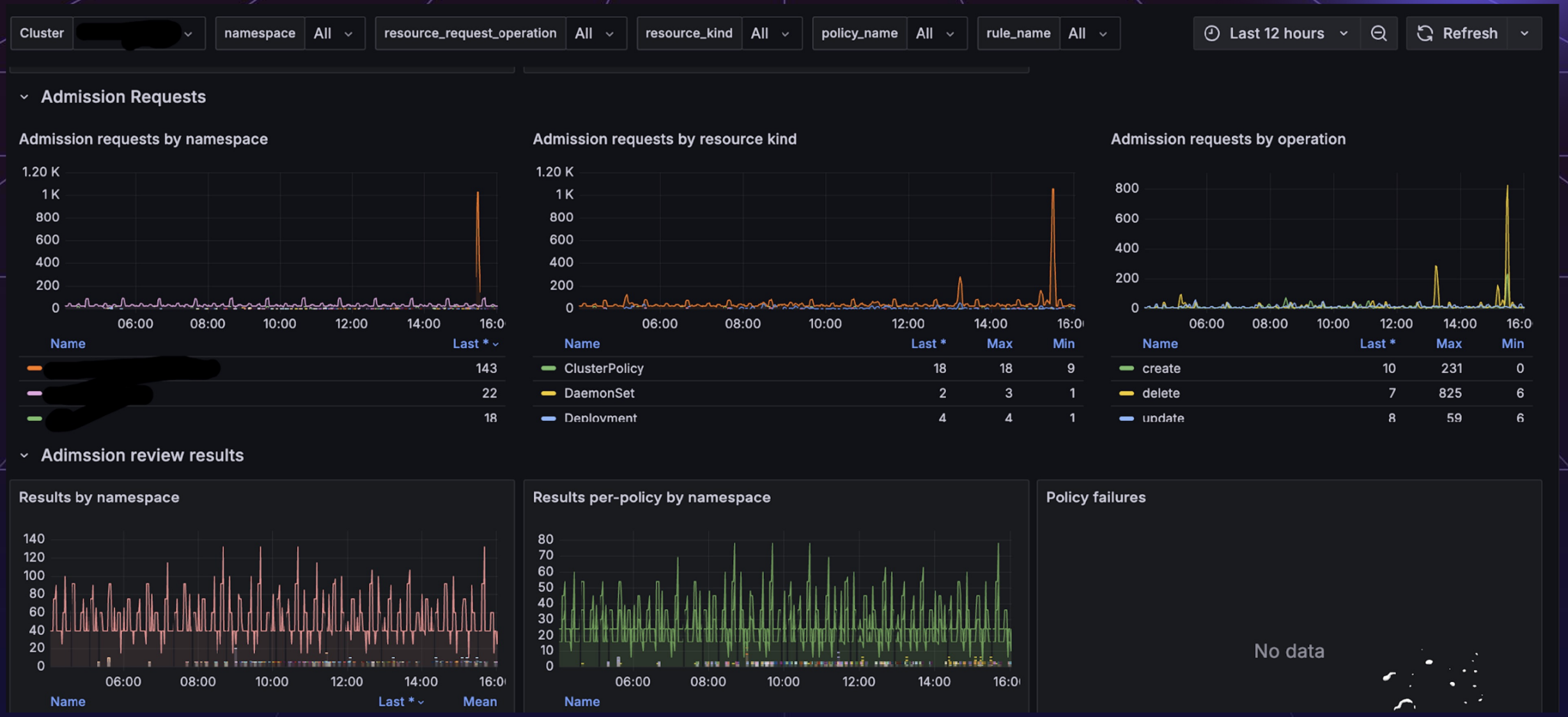
Kyverno Status (линк)

БЕКОН



Kyverno Latencies (линк)

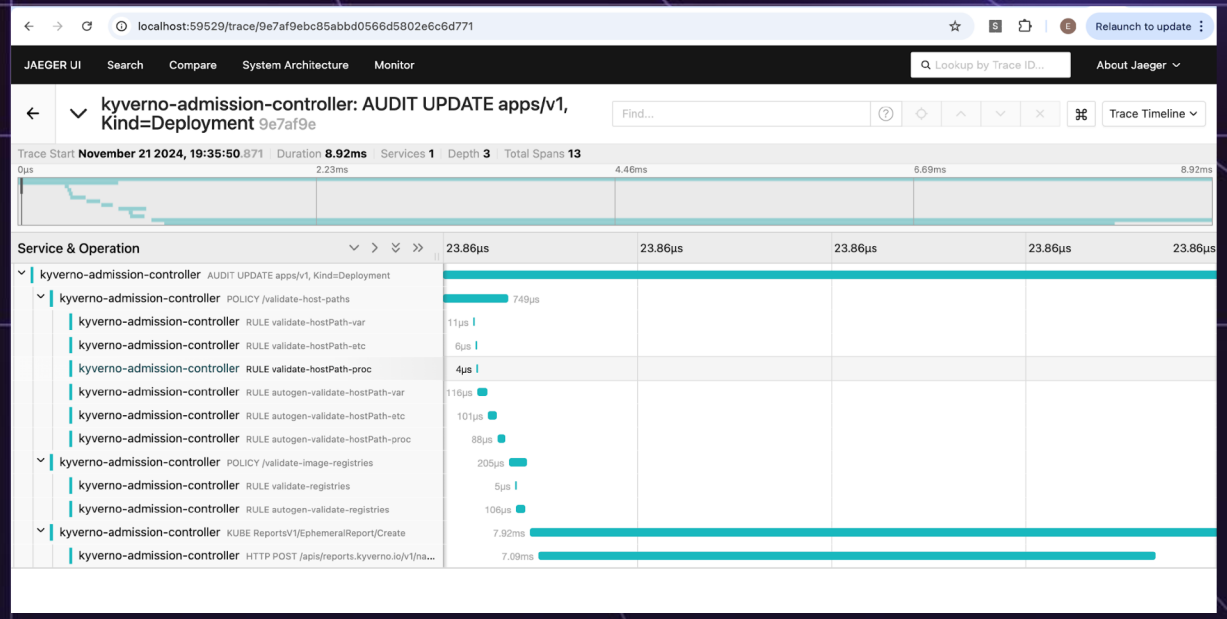
БЕКОН



Как сделать дешёвый трейсинг

БЕКОН

- Jaeger – для анализа трейсов
- Kyverno умеет слать трейсы в Jaeger
- Включается/выключается по лейблу в ArgoCD
- Активно пользуемся при тестах



Summary #3

БЕКОН

- Собирайте только нужные метрики, дропайте ненужные
- Формализуйте траблшутинг. Дашборды в этом помогут.
- Собирайте трейсы Kyverno, когда вам это нужно

БЕКОН

Как дёшево сделать нагрузочный тест?

Сайзинг kyverno

БЕКОН

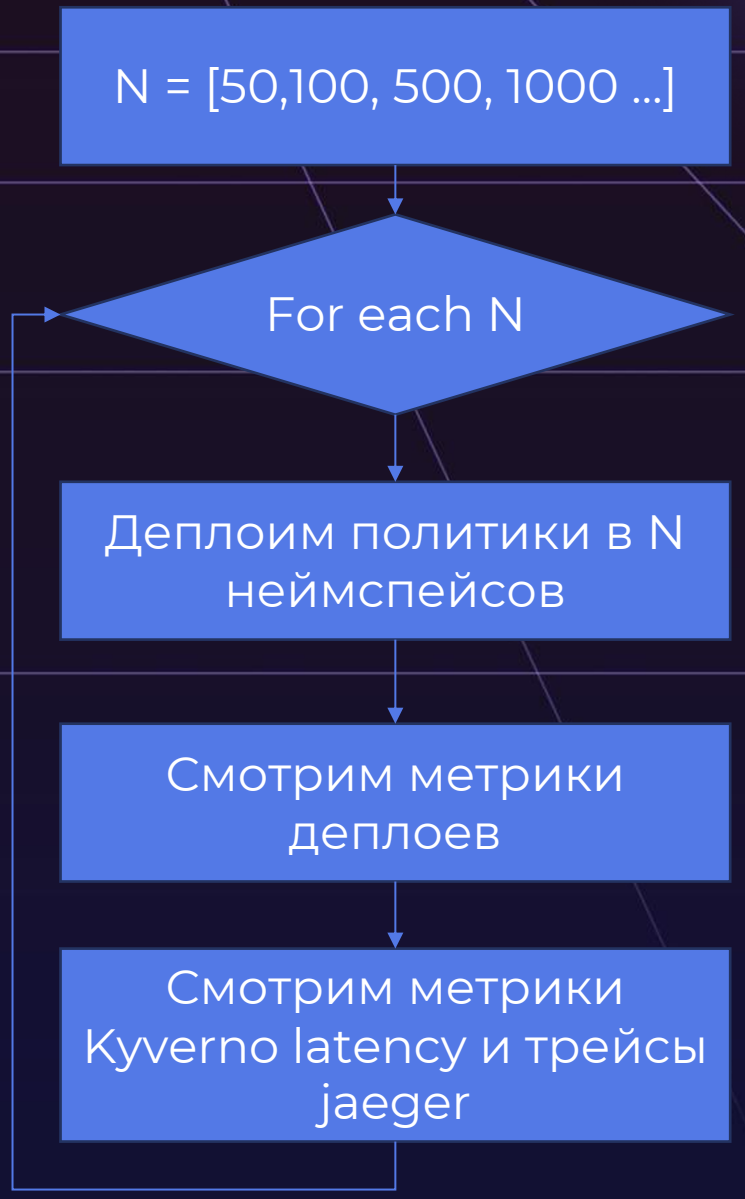
replicas	# policies	Rule Type	Mode	Subject	Virtual Users/Iterations	Latency (avg/max)	Memory (max)	CPU (max)	Memory Limit
1	17	Validate	Enforce	Pods	100/1,000	42.67ms / 141.24ms	114Mi	148m	default (384Mi)
1	17	Validate	Enforce	Pods	200/5,000	80.74ms / 409.35ms	215Mi	3237m	default (384Mi)
1	17	Validate	Enforce	Pods	500/10,000	203.86ms / 1.5s	471Mi	4851m	512Mi
3	17	Validate	Enforce	Pods	100/1,000	35.61ms / 92.61ms	104Mi	289m	default (384Mi)
3	17	Validate	Enforce	Pods	200/5,000	67.37ms / 327.12ms	122Mi	1336m	default (384Mi)
3	17	Validate	Enforce	Pods	500/10,000	163.08ms / 3.02s	239Mi	2769m	512Mi

Есть дока…

Нагрузочное тестирование

БЕКОН

- 30 политик / 1-3 правила в политике
- Политики в режиме аудита
- 10 минут между итерациями
- Подопытный кластер – стейджинг с сотнями деплоев в день
- Максимально дёшево (без доп инфры и инструментов)



Нагрузочное тестирование

БЕКОН

Кол-во неймспейсов	Avg rule execution	Avg policy execution	Max policy execution
100	1 ms	361 ms	10 s
600	6 ms	352 ms	10 s
1100	12 ms	325 ms	10 s
1600	25 ms	364 ms	10 s
2100	40 ms	371 ms	10 s
2600	55 ms	401 ms	9 s
3600	93 ms	423 ms	8 s
4200	119 ms	434 ms	7 s

WTF

Нагрузочное тестирование

БЕКОН

- Рулы с validate спеки работают быстро
- Рулы с походом во внешку - медленно
- Выявили самую долгую политику (**проверка подписи образов в Harbor**)
- Jaeger сильно помог

Summary #4

БЕКОН

- Начните с дешёвого load testing
- Напишите load testing guide
- Обращайте внимание на политики с походом во внешку

БЕКОН

Как гибко деплоить политики?

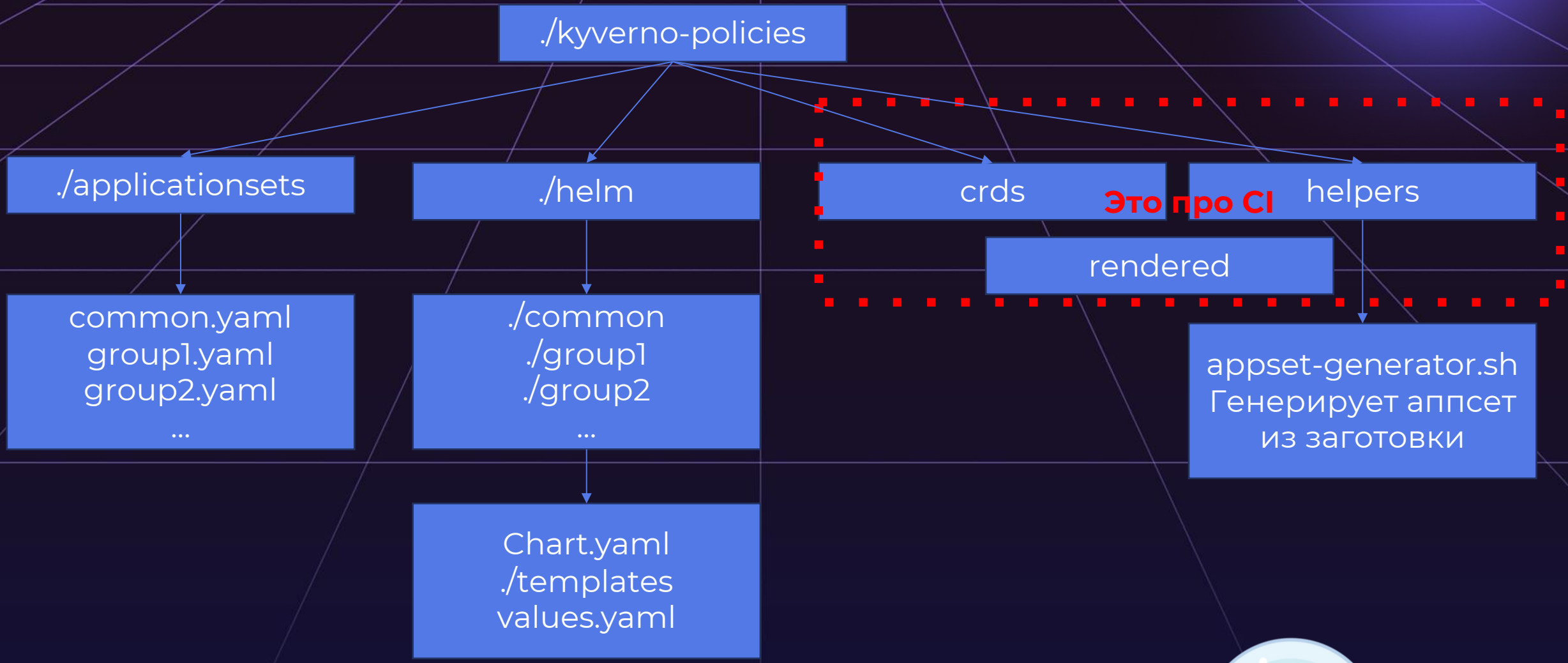
Что такое «гибко»?

БЕКОН

- Варьировать параметры политик
- Варьировать набор политик
- Не делать копипасты
- Не строгать кучу деплоев

Как выглядит репо с политиками?

БЕКОН



Нюансы

БЕКОН

- Проверяйте, что аппсет катится туда, куда вам надо
  - argocd appset generate (2.13+)
- Экранируйте {{}} в шаблонах
- Используйте PR description и делайте ревью политик

```
deny:
  conditions:
    any:
      - key: {{`"{{request.operation || 'BACKGROUND'}}"`}}
```

Summary #5

БЕКОН

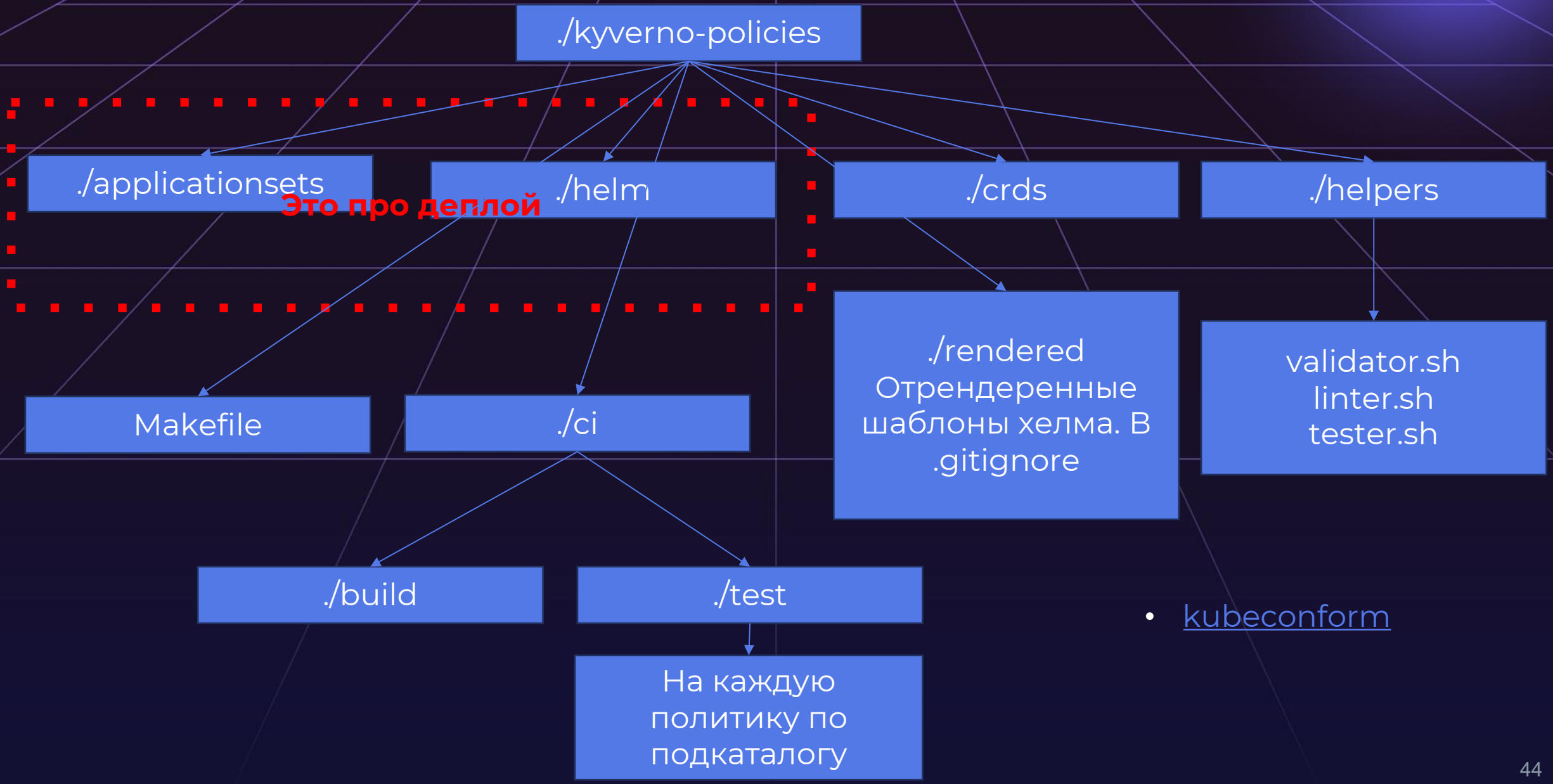
- Используйте мощь GitOps
- Если у вас нет GitOps – время внедрить
- Используйте наш шаблон репозитория!

БЕКОН

Как сделать CI политик?

Как выглядит репо с политиками?

БЕКОН



- kubeconform

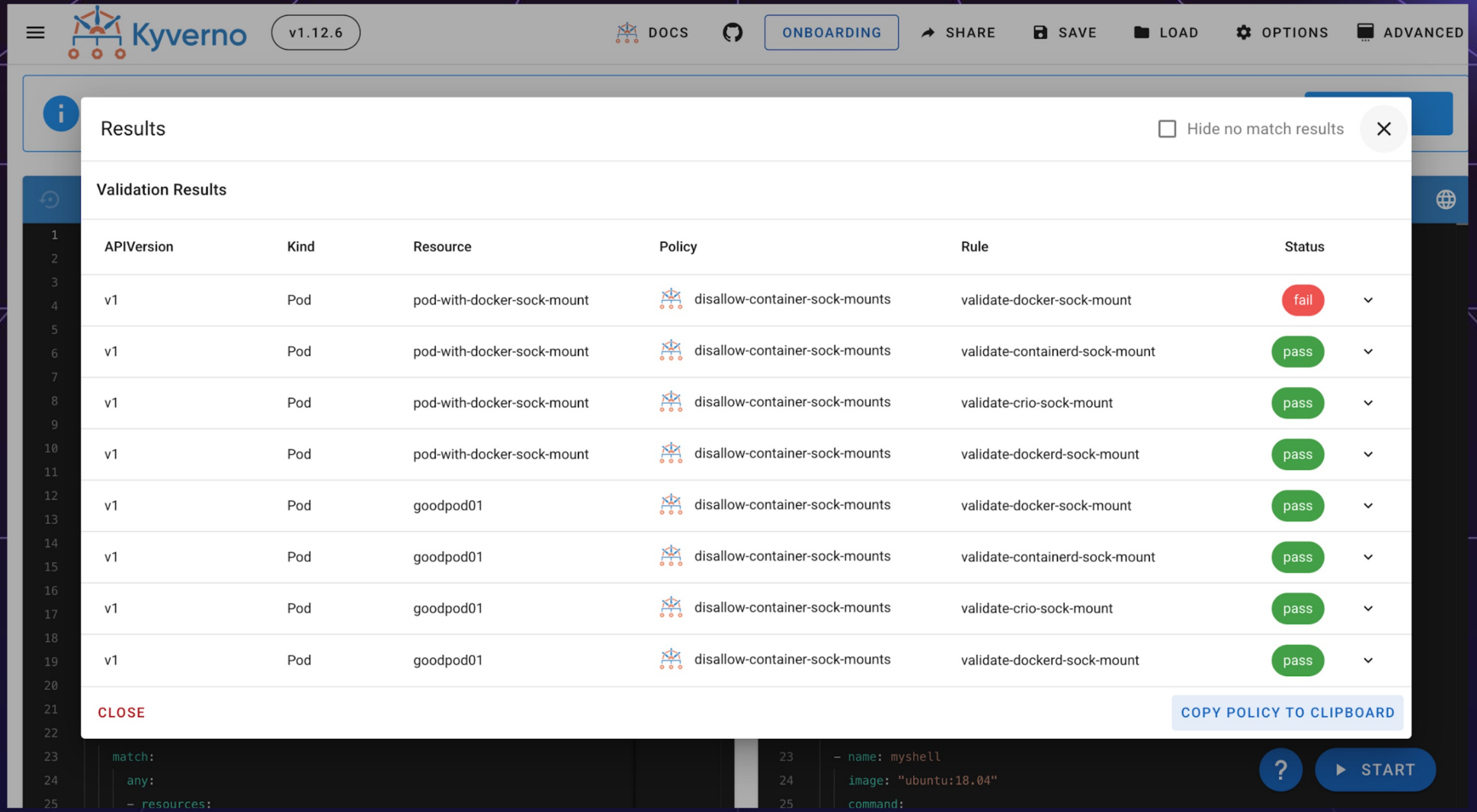
Как писать тесты?

БЕКОН

А также – Kyverno Playground! (чарт)

Kyverno Playground

БЕКОН

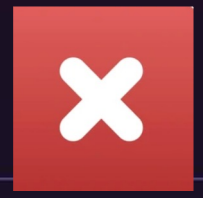


Ставьте из чарта

Нужен ли kyverno apply в CI политик?

БЕКОН

- Если кластеров мало
- Если кластера небольшие



- Если кластеров много
- Если кластера большие

- Можно встроить в CI приложений

Summary #6

БЕКОН

- Сделайте CI с валидацией, линтовкой и тестами
- Если маленькая инфра – то и с kyverno apply

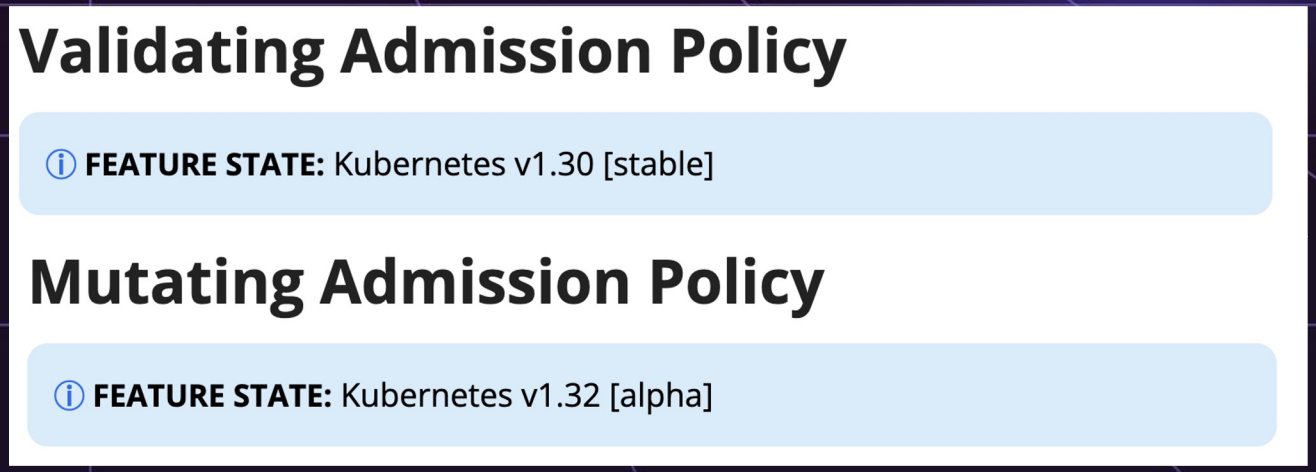
БЕКОН

Что с k8s-native политиками?

Что умеет Kubernetes нативно?

БЕКОН

- Валидировать ресурсы
- Мутировать ресурсы
- … И всё
- MAP/VAP работают внутри kube-apiserver



Kyverno 1.14

БЕКОН

- Хотят единый API для политик – extended CEL
- Хотят опереться на VAP/MAP

Feature	K8s ValidatingAdmissionPolicy	Kyverno ValidatingPolicy
Enforcement	Admission	Admission, Background, Pipelines, ...
Payloads	Kubernetes	Kubernetes, Any JSON or YAML
Distribution	Kubernetes API server	Helm, CLI, Web Service, API, SDK
CEL Library	Basic	Extended
Bindings	Manual	Automatic
Auto-generation	⛔	Pod Controllers, ValidatingAdmissionPolicy
External Data	⛔	Kubernetes resources or API calls
Caching	⛔	Global Context, image verification results
Background scans	⛔	Periodic, On policy creation or updates
Exceptions	⛔	Fine-grained exclusions
Reporting	⛔	Policy WG Reports, Policy Reporter, etcd offload
Testing	⛔	Kyverno CLI (unit), Chainsaw (e2e)

Summary #7

БЕКОН

- Интеграция с нативными возможностями – хорошо, но рано
- Мы пока не тестировали
- Это тема для будущих докладов

Другие материалы

БЕКОН

- QR на наши дашборды и репозиторий ->
- ~~Нестандартное применение Kyverno (SafeCode 2024)~~
- Как правильно готовить Kyverno и работать с его алертами (БеКон 2023)
- Kyverno: старт без грабель (DevOpsConf 2024)

Дашборды

Репо с политиками

berendiaev
eaberendyaev@avito.ru