Безопасность Kubernetes

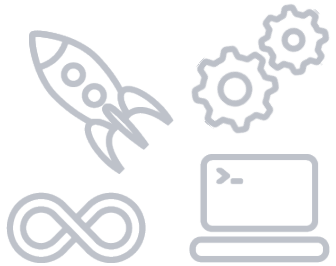
Beeline™

+

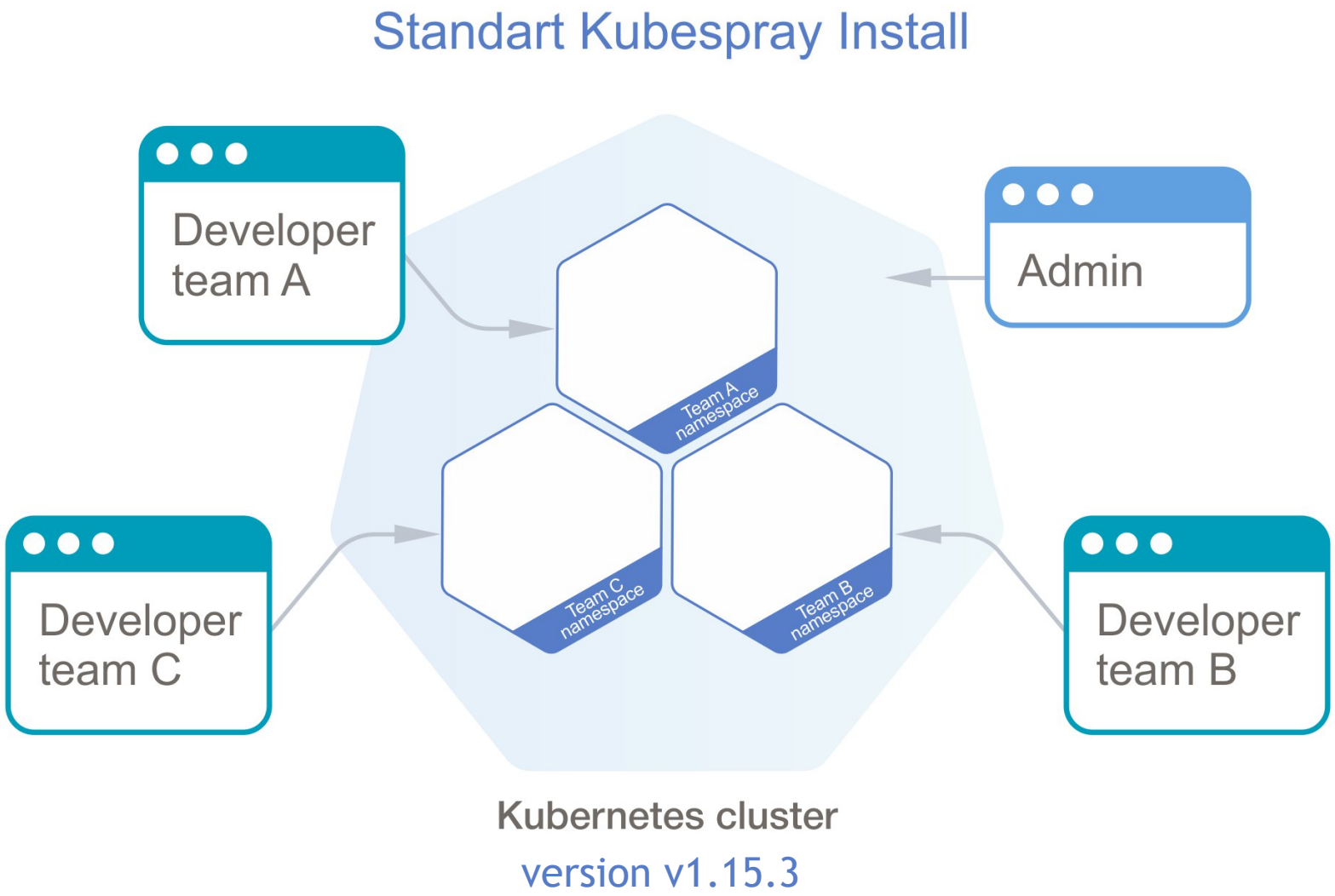
СЛЁРМ

План

- Права Pod’ов vs права пользователей
- Сетевые политики
- Глобальные лимиты для кластера



Сетап


Standart Kubespray Install
Developer team A
Admin
Team A namespace
Developer team C
Team C namespace
Team B namespace
Developer team B
Kubernetes cluster
version v1.15.3

Демо будет!

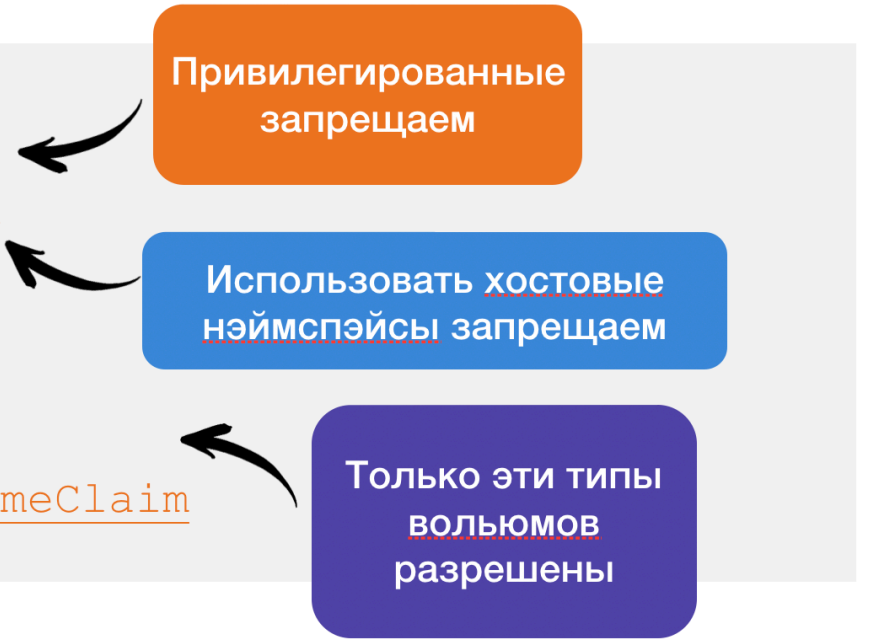
Права Pod’ов

- Privileged
- Root user
- Host namespace
- Host path volume
- …

Pod Security Policy

Контролирует аспекты безопасности в описании Pod’ов

```
spec:
  privileged: false
  hostNetwork: false
  hostPID: false
  volumes:
    - configMap
    - emptyDir
    - secret
    - persistentVolumeClaim
```



Pod Security Policy

Контролирует аспекты безопасности в описании Pod’ов

```
spec:
  privileged: false
  hostNetwork: false
  hostPID: false
  volumes:
    - configMap
    - emptyDir
    - secret
    - persistentVolumeClaim
```

Привилегированные запрещаем

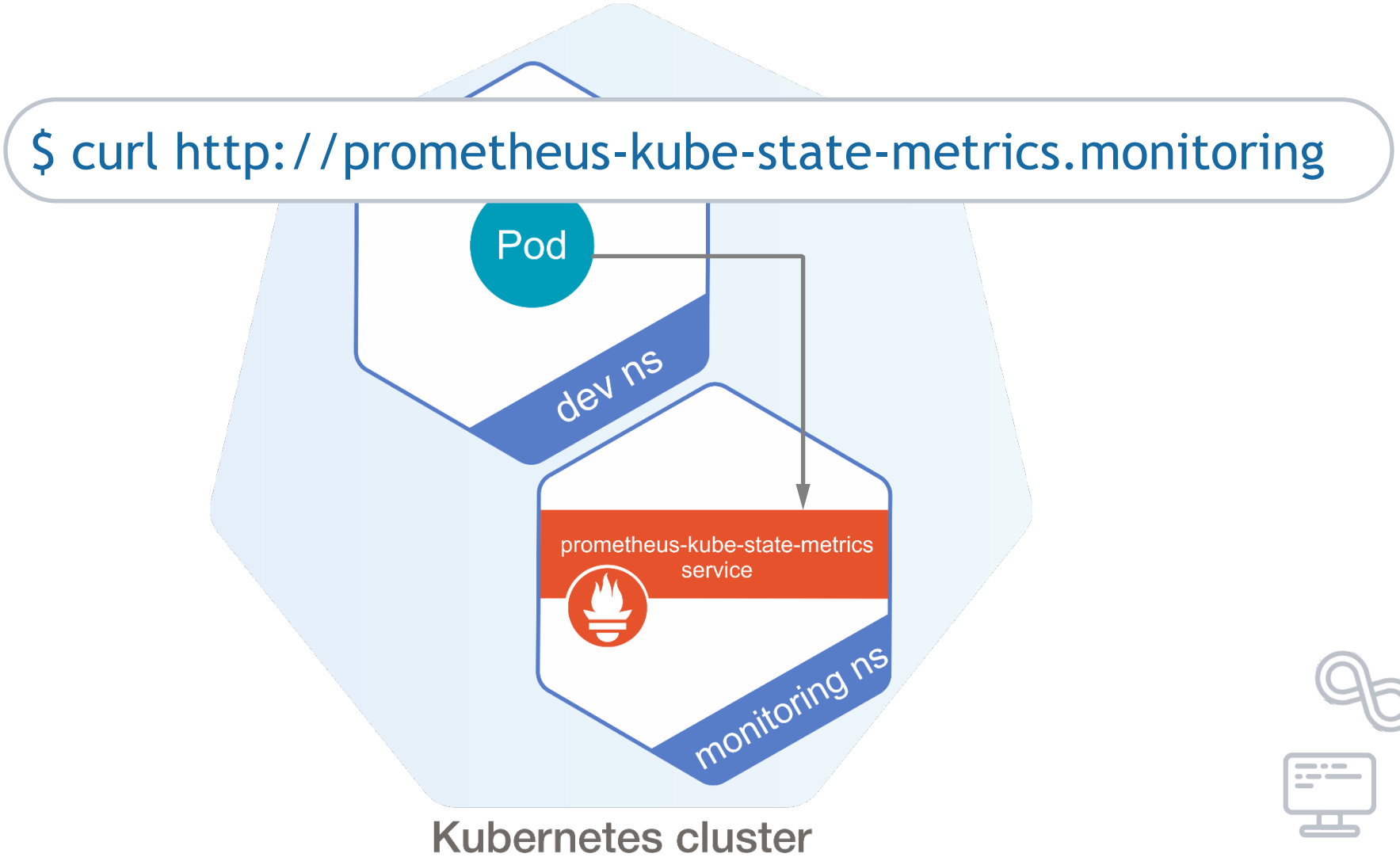
Использовать хостовые нэймспэйсы запрещаем

Только эти типы вольюмов разрешены

https://kubernetes.io/docs/concepts/policy/pod-security-policy/

Мониторинг – самая большая дыра ~~во Вселенной~~ в Вашем кластере

Prometheus в кластере



Версия кластера из мониторинга

kube_pod_container_info{namespace=«kube-system",pod="kube-apiserver-k8s-1",container="kube-apiserver",image=

"gcr.io/google-containers/kube-apiserver:v1.14.5"

,image_id="docker-pullable://gcr.io/google-containers/kube-apiserver@sha256:e29561119a52adad9edc72bfe0e7fcab308501313b09bf99df4a9638ee634989",container_id="docker://7cbe7b1fea33f811fdd8f7e0e079191110268f2853397d7daf08e72c22d3cf8b"} 1

Как закрывать Prometheus

- Network Policy (https://kubernetes.io/docs/concepts/services-networking/network-policies/)
  - Нет доступа – нет проблем

Как закрывать Prometheus

- Network Policy (https://kubernetes.io/docs/concepts/services-networking/network-policies/)
  - Нет доступа – нет проблем
  - Можно включить просто в чартах
- Kube-RBAC-Proxy (https://github.com/brancz/kube-rbac-proxy)
  - Добавляем авторизацию
  - Придется переписать чарты

Как закрывать Prometheus

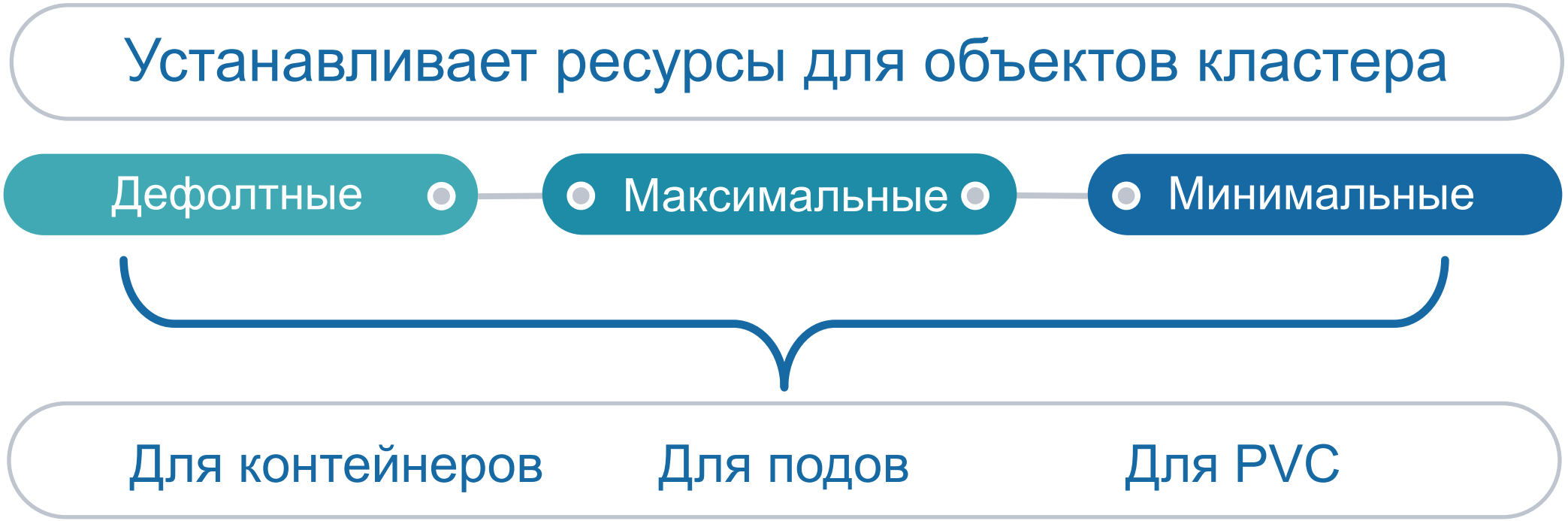
- Network Policy (https://kubernetes.io/docs/concepts/services-networking/network-policies/)
  - Нет доступа – нет проблем
  - Можно включить просто в чартах
- Kube-RBAC-Proxy (https://github.com/brancz/kube-rbac-proxy)
  - Добавляем авторизацию
  - Придется переписать чарты
- На самом деле не только Prometheus
  - Scheduler
  - Controller-manager
  - etc…


DoS
Способ простой – исчерпание ресурсов

Limit Range

Устанавливает ресурсы для объектов кластера

Limit Range


Устанавливает ресурсы для объектов кластера
Дефолтные
Максимальные
Минимальные
Для контейнеров
Для подов
Для PVC

Limit Range

Устанавливает ресурсы для объектов кластера

Дефолтные

Максимальные

Минимальные

Для контейнеров

Для подов

Для PVC

https://kubernetes.io/docs/concepts/policy/limit-range/


Способ мастеров – запускаем 111111111 подов
DOS

Resource Quota

Устанавливает количество доступных ресурсов и объектов для нэймспэйса в кластере

Resource Quota

Устанавливает количество доступных ресурсов и объектов для нэймспэйса в кластере

Реквесты

Лимиты

Сервисы

Поды

…

Resource Quota

Устанавливает количество доступных ресурсов и объектов для нэймспэйса в кластере

Реквесты

Лимиты

Сервисы

Поды

…

https://kubernetes.io/docs/concepts/policy/resource-quotas/

Воркфлоу создания нэймспэйса

- Создаем namespace
- Создаем внутри limitrange
- Создаем внутри resourcequota
- Создаем serviceaccount для CI
- Создаем rolebinding для CI и пользователей
- Опционально запускаем нужные служебные поды

Воркфлоу создания нэймспэйса

- Создаем namespace
- Создаем внутри limitrange
- Создаем внутри resourcequota
- Создаем serviceaccount для CI
- Создаем rolebinding для CI и пользователей
- Опционально запускаем нужные служебные поды

https://github.com/pauljamm/team-operator

Что делать?

- Pod Security Policy – это хорошо

Что делать?

- Pod Security Policy – это хорошо
- Network Policy – это не какая-то еще одна ненужная фича

Что делать?

- Pod Security Policy – это хорошо
- Network Policy – это не какая-то еще одна ненужная фича
- LimitRange/ResourceQuota – пора бы заглянуть в документацию

Что делать?

- Pod Security Policy – это хорошо
- Network Policy – это не какая-то еще одна ненужная фича
- LimitRange/ResourceQuota – пора бы заглянуть в документацию

https://github.com/kubernetes/community/blob/master/wg-security-audit/findings/Kubernetes%20Final%20Report.pdf

Записываться на Слёрм!