МЕГА СЛЁРМ

+

Southbridge

Безопасные и высокодоступные приложения в кластере

slurm.io

План

- Безопасность Docker контейнера
- Pod security policies
- Применение сетевых абстракций
- Pod Disruption Budgets
- Limitrage / Resourcequota

Docker

Что есть Docker?

Docker

Не система контейнеризации

Безопасность Docker контейнера

Возможности доступные "by-design" контейнерам

Безопасность Docker контейнера

Возможности доступные "by-design" контейнерам

Изоляция namespace

Безопасность Docker контейнера

Возможности доступные "by-design" контейнерам

- Изоляция namespace
- Изоляция ресурсов (CGroup)

Безопасность Docker контейнера

Возможности доступные "by-design" контейнерам

Изоляция namespace

Изоляция ресурсов (CGroup)

GID/UID

Безопасность Docker контейнера

Безопасность Docker контейнера

Возможности доступные "by-design" контейнерам

Изоляция namespace

Изоляция ресурсов (CGroup)

Kernel capabilities

GID/UID

Безопасность image

(https://github.com/anchore/anchore-engine)

Уязвимости в K8S pod

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

Pod Security Policies

- Контролирует аспекты безопасности в описании Pod’ов

- Включается как admission controller plugin "PodSecurityPolicy"

При включении запрещает запуск Podов без PSP

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

PSP

```
kubectl create serviceaccount user --namespace=default
```

```
kubectl create rolebinding user --clusterrole=edit
--serviceaccount=default:user
```

```
kubectl get po --as=system:serviceaccount:default:
user --all-namespaces
```

```
kubectl create -f hackers-pod.yaml --as=system:
serviceaccount:default:user
```

Доступность приложения в K8S

Выход из строя ноды

Работы на кластере

Удаление приложения

Доступность приложения в K8S

Service vs. Ingress

Service vs. Ingress

Просто iptables (?)

Базовый механизм service discovery на основе DNS (?)

Service vs. Ingress

Просто iptables (?)

Базовый механизм service discovery на основе DNS (?)

Service vs. Ingress

SERVICE

- Просто iptables (?)
- Базовый механизм service discovery на основе DNS (?)

INGRESS

- Next upstream
  - SIGTERM trap

Pod Disruption Budget

Ограничивает количество инстансов, которые могут быть недоступны одновременно

Администратор должен использовать "Eviction API"

https://kubernetes.io/docs/tasks/run-application/configure-pdb/

Limitrange

Устанавливает ресурсы для объектов кластера

Дефолтные | Максимальные | Минимальные

- Для контейнеров
- Для подов
- Для PVC

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

Resourcequota

Устанавливает количество доступных ресурсов и объектов для нэймспэйса в кластере

Реквесты

Лимиты

Сервисы

Поды

...

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

Обеспечение отказоустойчивости приложений

- Использование ingress при невозможности повторять неуспешные запросы при межсервисном взаимодействии
- Запуск приложений в несколько реплик

- Использование Pod Disruption Budget
- Контроль доступа и ограничений в кластере

МЕГА СЛЁРМ + Southbridge

Перерыв

slurm.io