ООО «Базальт СПО»

Российский разработчик
операционных систем «Альт»

Реализация rootless kubernetes в рамках ALT Linux-пакетов

https://github.com/alt-cloud/podsec

Костарев Алексей kaf@basealt.ru
Степченко Александр stepchenkoas@basealt.ru

Что такое rootless

Изолированное окружение, внутри которого пользователь имеет UID=0.

Изолированное окружение включает:

- Изолированное пространство пользователей (новые UIDs и GIDs)
- Изолированная унаследованная файловая система
- Изолированные новые сетевые интерфейсы
  (включая таблицы netfilter и EPBF ядра).

Повышенная безопасность при запуске rootless контейнеров.

Реализации rootless контейнеров

- Podman 1.0.0 (11.01.2019)
- Docker 20.10.0 (08.12.2020)
- Usernetes Gen1 (06.05.2021)
- Kubernetes 1.28 (08.2023)
- Podsec-k8s (05.2023)

Основа:

- Rootlesskit 1.0.0 (25.03.2022)
- Slirp4netns 1.0.0 (31.03.2020)

kubernetes переход от containerd к CRI-O

Недостатки containerd:

- Наличие единой точки отказа — containerd
- Позволяет получить доступ по TCP/IP извне
- Сложности в реализации совместной работы в rootless/rootfull режимах (для каждого пользователя отдельный демон)

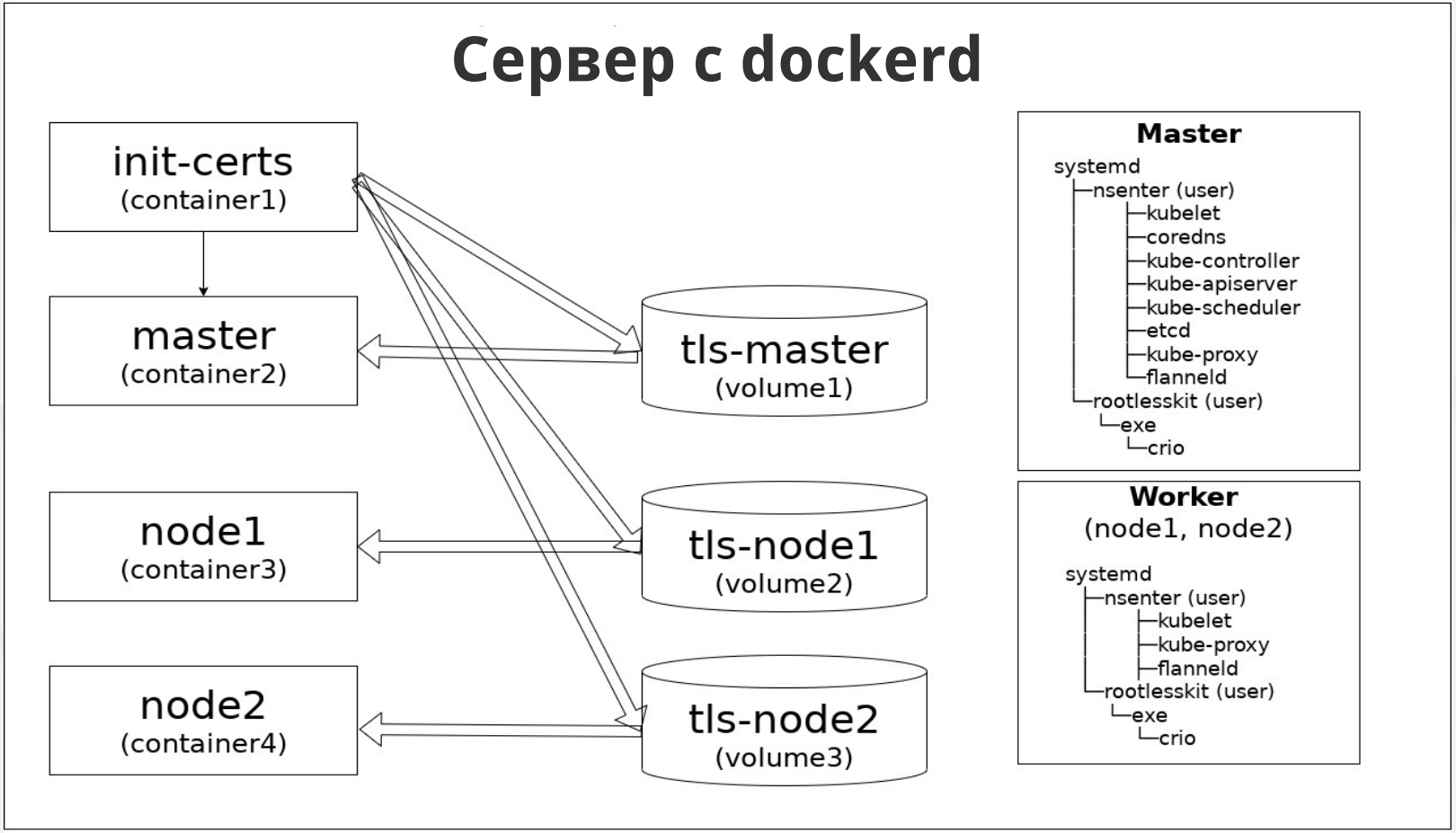
Преимущества CRI-O:

- Непосредственный запуск контейнеров (как и в podman) через fork/exec.
- Поддержка images policy с использованием подписанных (signed) образов

podsec-k8s

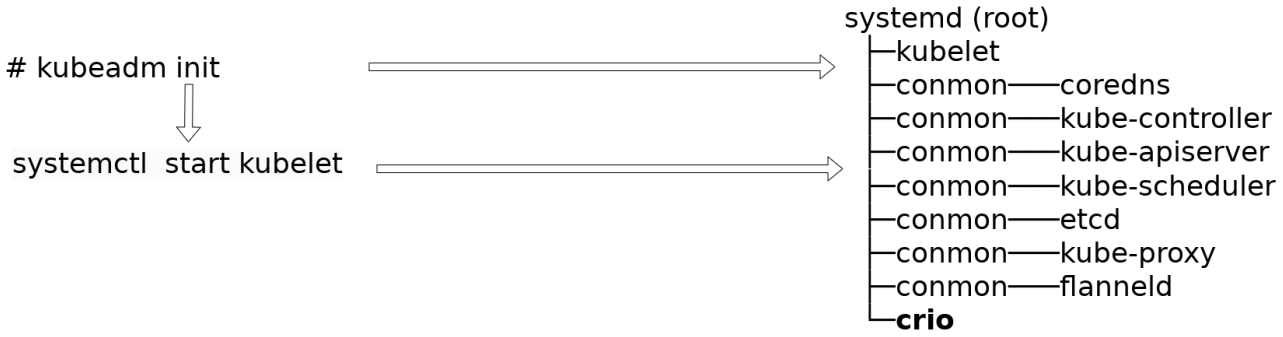
- kubernetes v1.26+ и rootlesskit
- Все POD’ы kubernetes, включая системные, работают в rootless-окружении.
- Локальный репозиторий подписанных образов
- Политики безопасности и мониторинга попыток их нарушения (podsec-k8s-rbac, podsec-k8s-inotify).

Базовое решение - Usernetes



Стандартная схема разворачивания через kubeadm

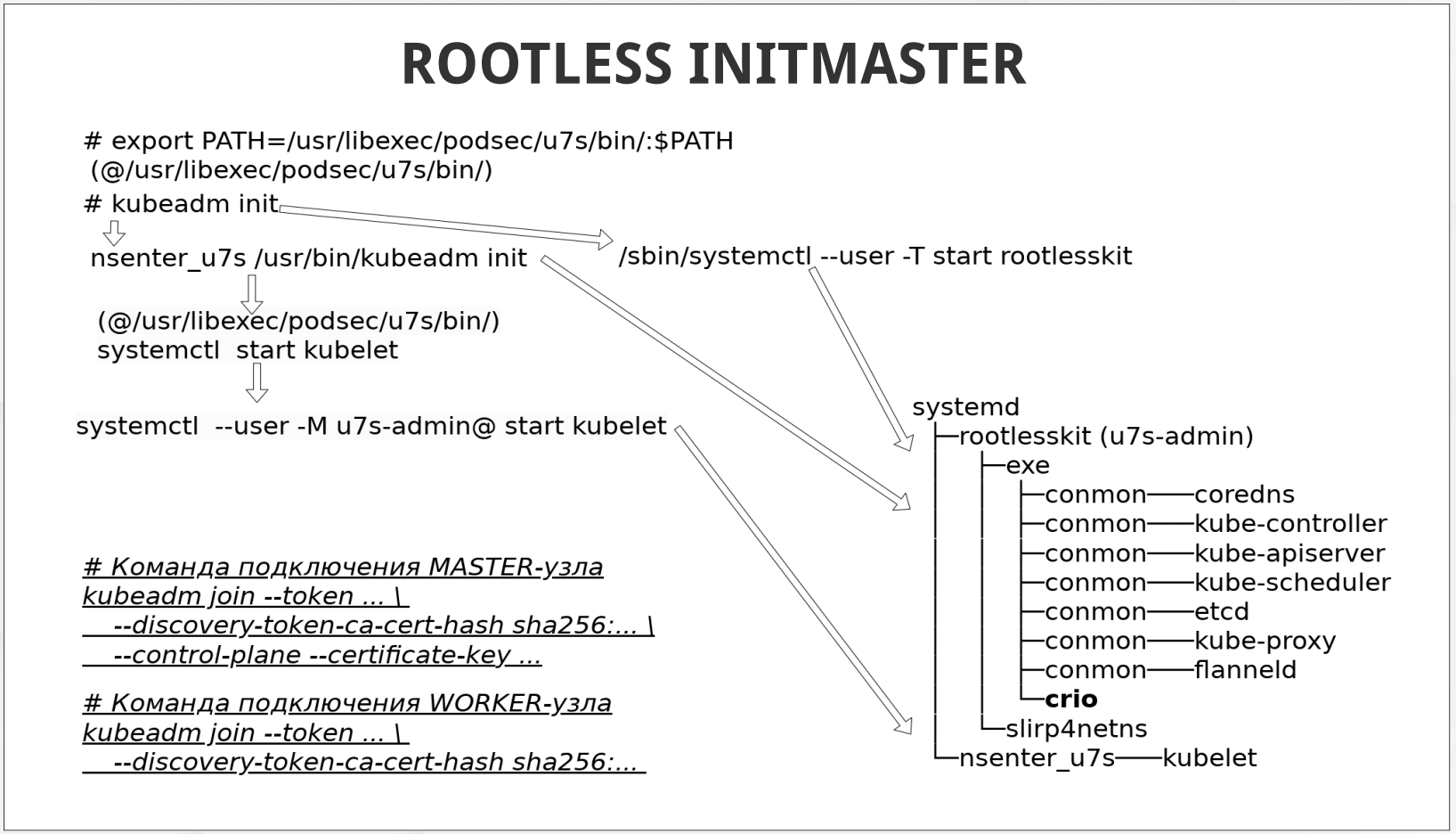
ROOTFULL INITMASTER



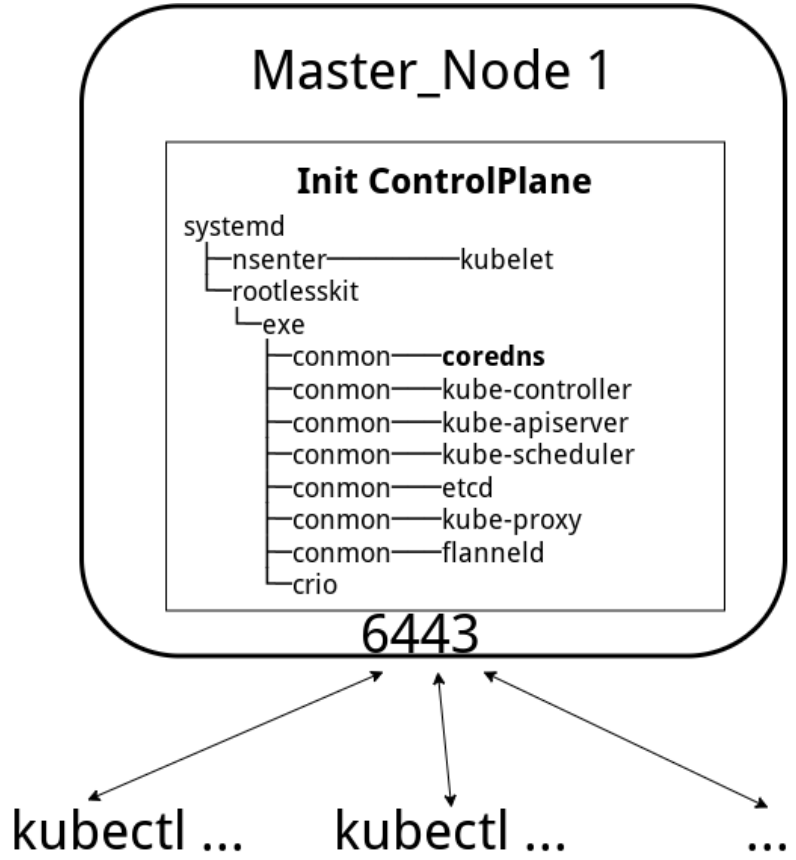
 # Команда подключения MASTER-узла
*kubeadm join --token ... *
* --discovery-token-ca-cert-hash sha256:... *
* --control-plane --certificate-key ...*

 # Команда подключения WORKER-узла
*kubeadm join --token ... *
* --discovery-token-ca-cert-hash sha256:...*

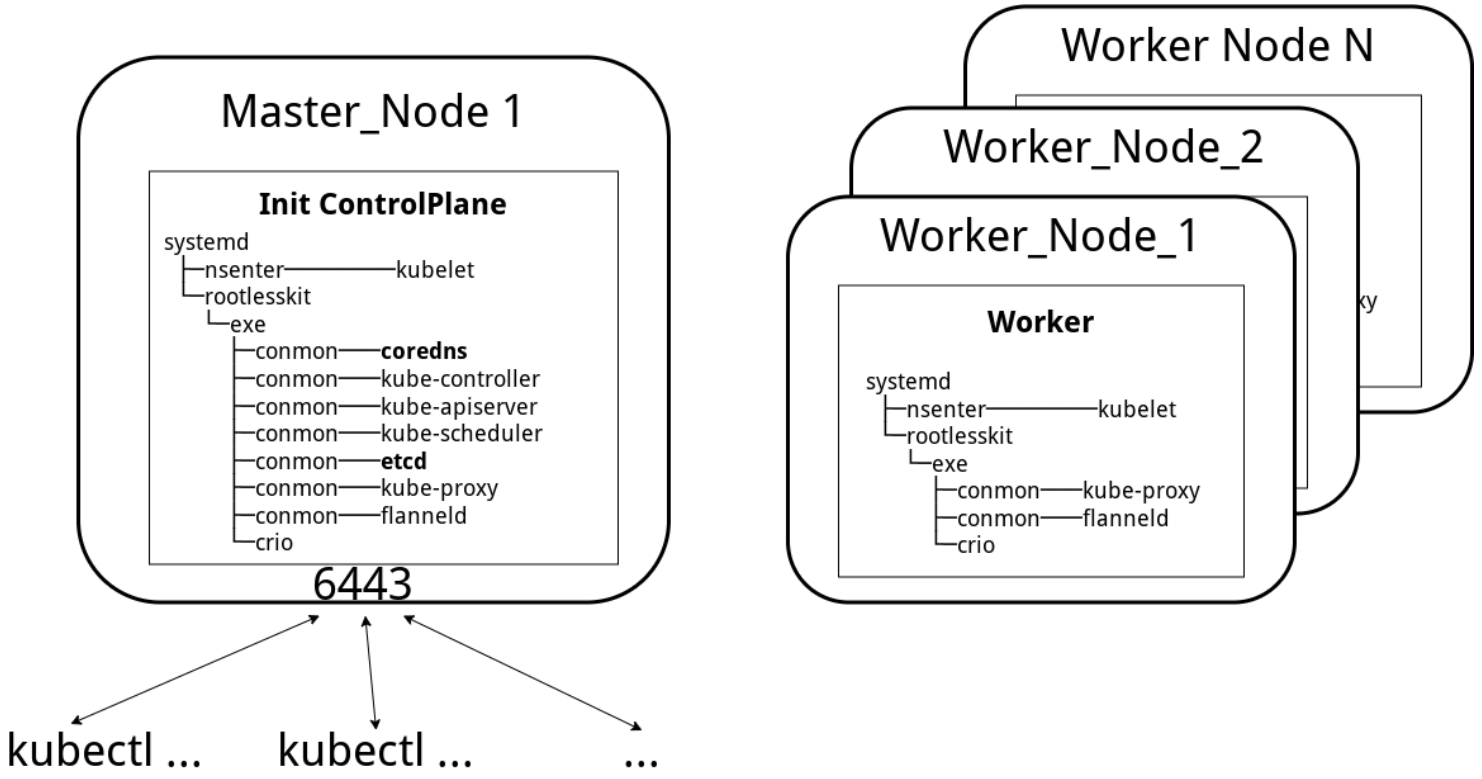
Развертывание rootless кластера в podsec-k8s



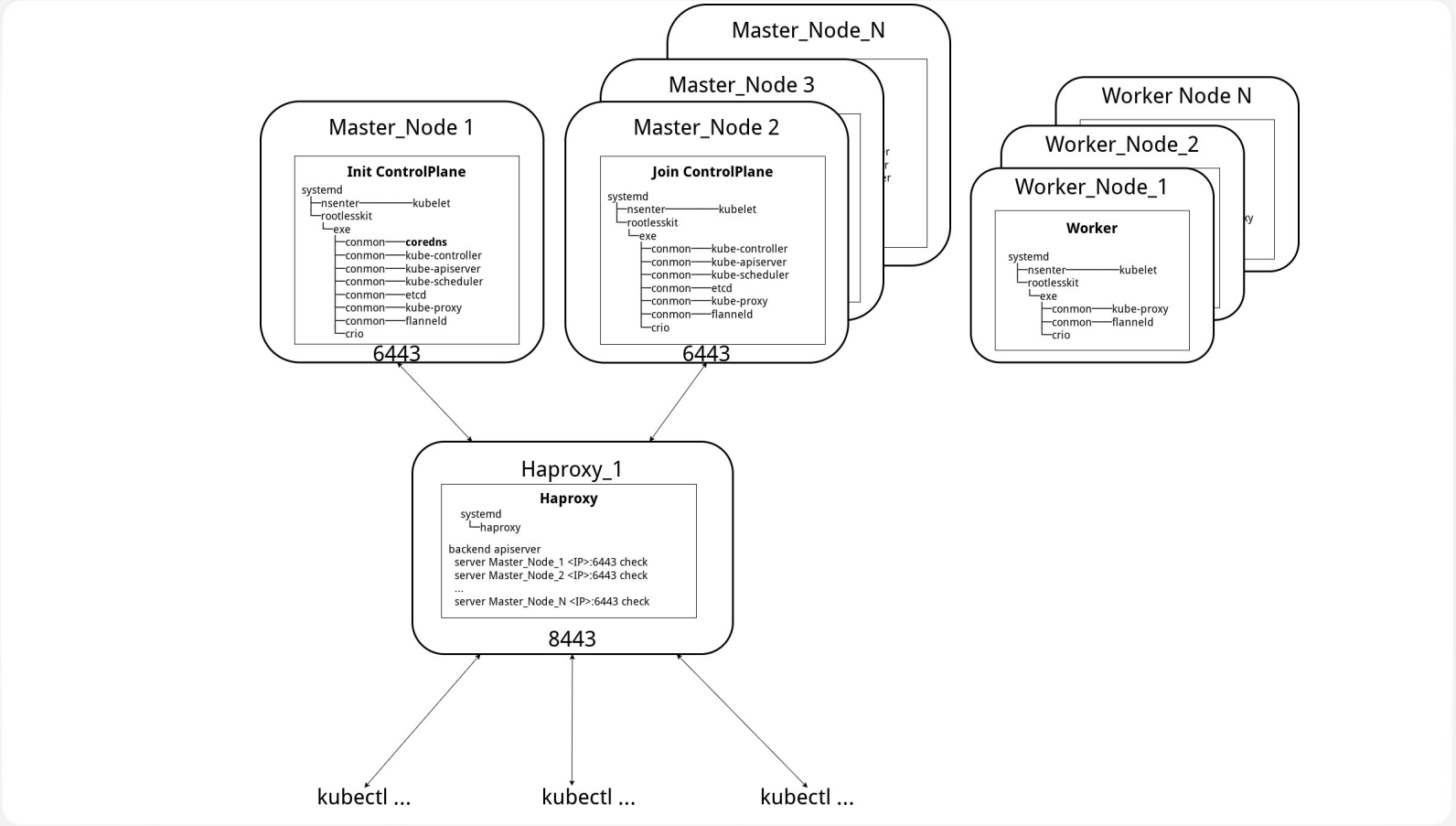
Вариант развертывания Only Master



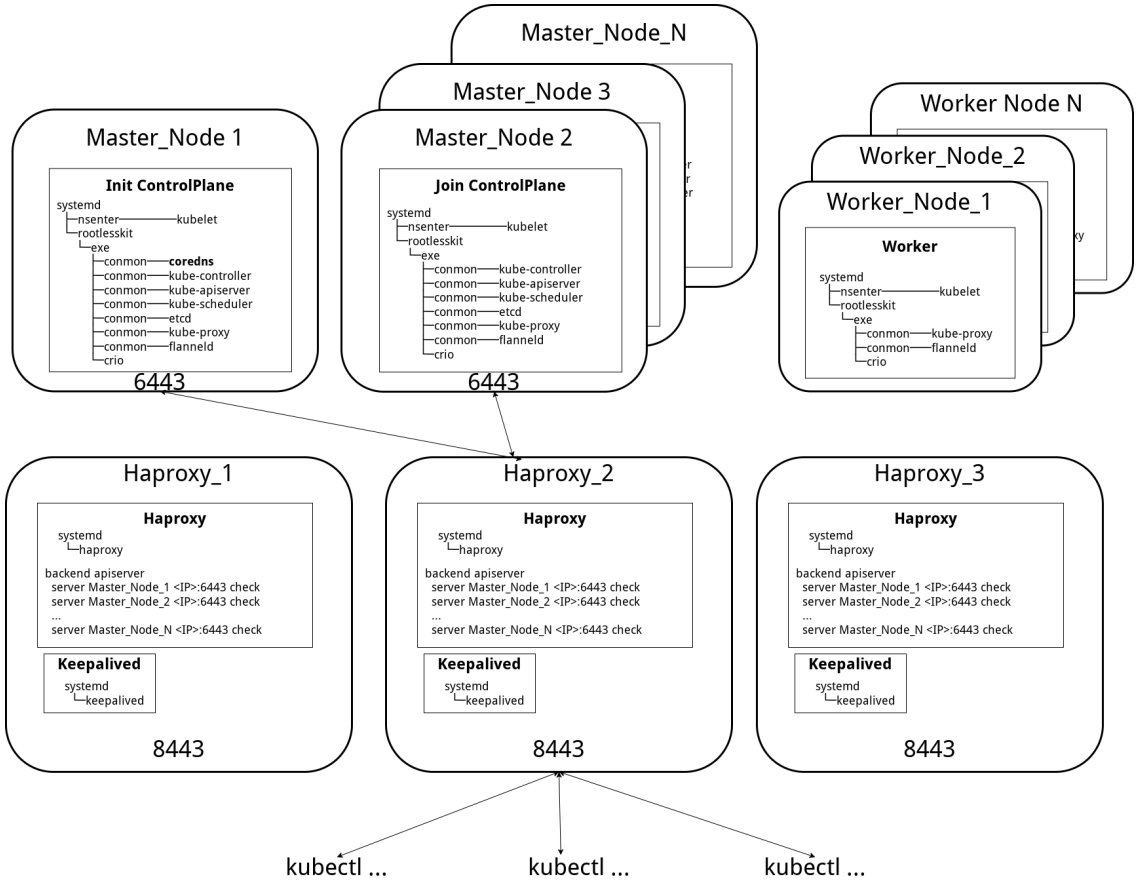
Вариант развертывания Master - Workers



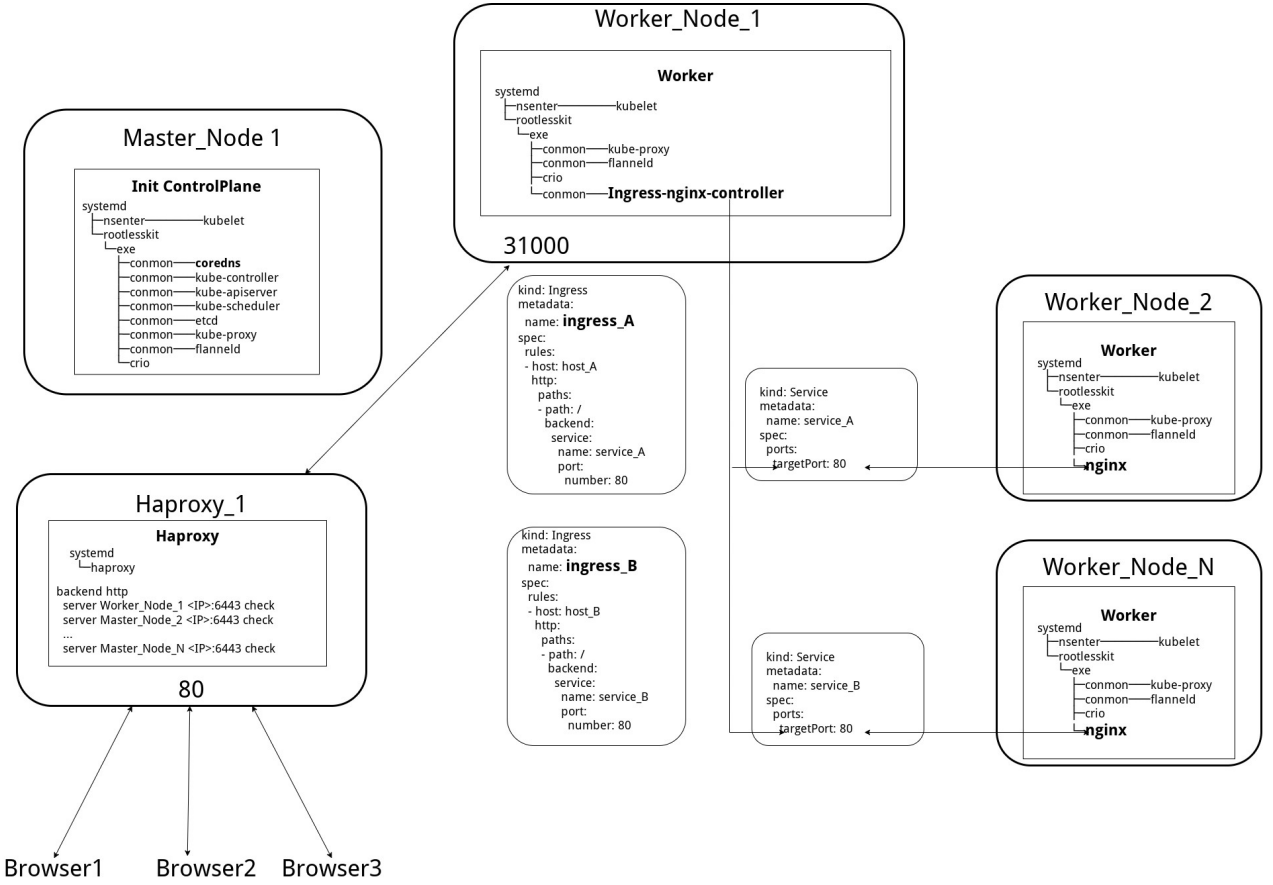
Вариант разворачивания Haproxy - Masters - Workers



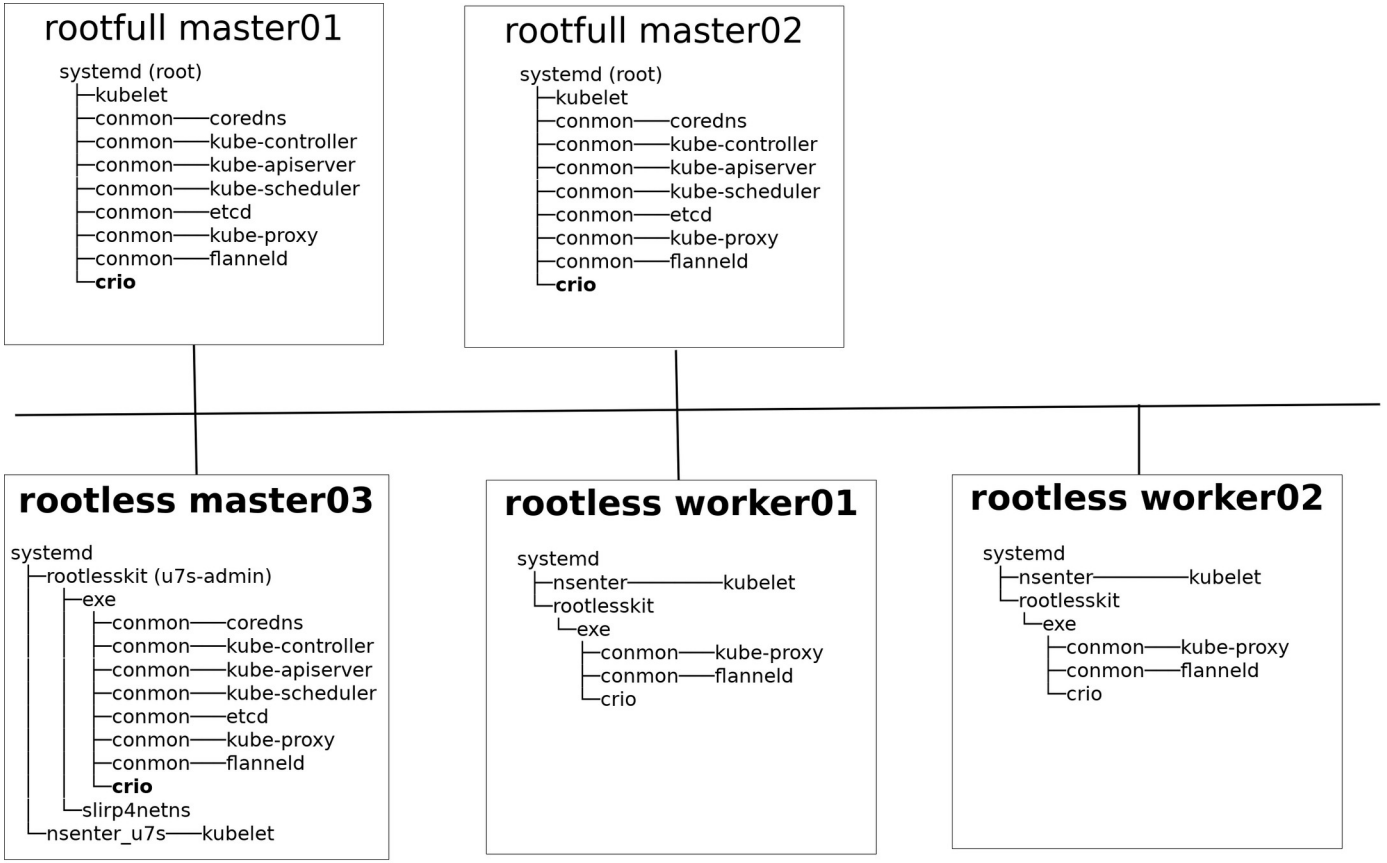
Вариант разворачивания Haproxies - Masters - Workers



Вариант разворачивания Masters — Workers + ingress nginx



RootFullLess кластера kubernetes



Поддерживаемые CNI plugins

- Поддерживается flannel.
- Остальные plugin’ы (cillium, calico и др.) пока что не поддерживаются.

Группа пакетов podsec

Rootless kubernetes входит в состав ALT Linux пакета podsec-k8s.

Кроме этого группа пакетов podsec включает пакеты:

- podsec — настройка политик работы с подписанными на локальном регистраторе образами.
- podsec-k8s-rbac — настройка политик доступа по протоколу kubernetes RBAC;
- podsec-inotify — мониторинг настроенных политик безопастности.

Вопросы