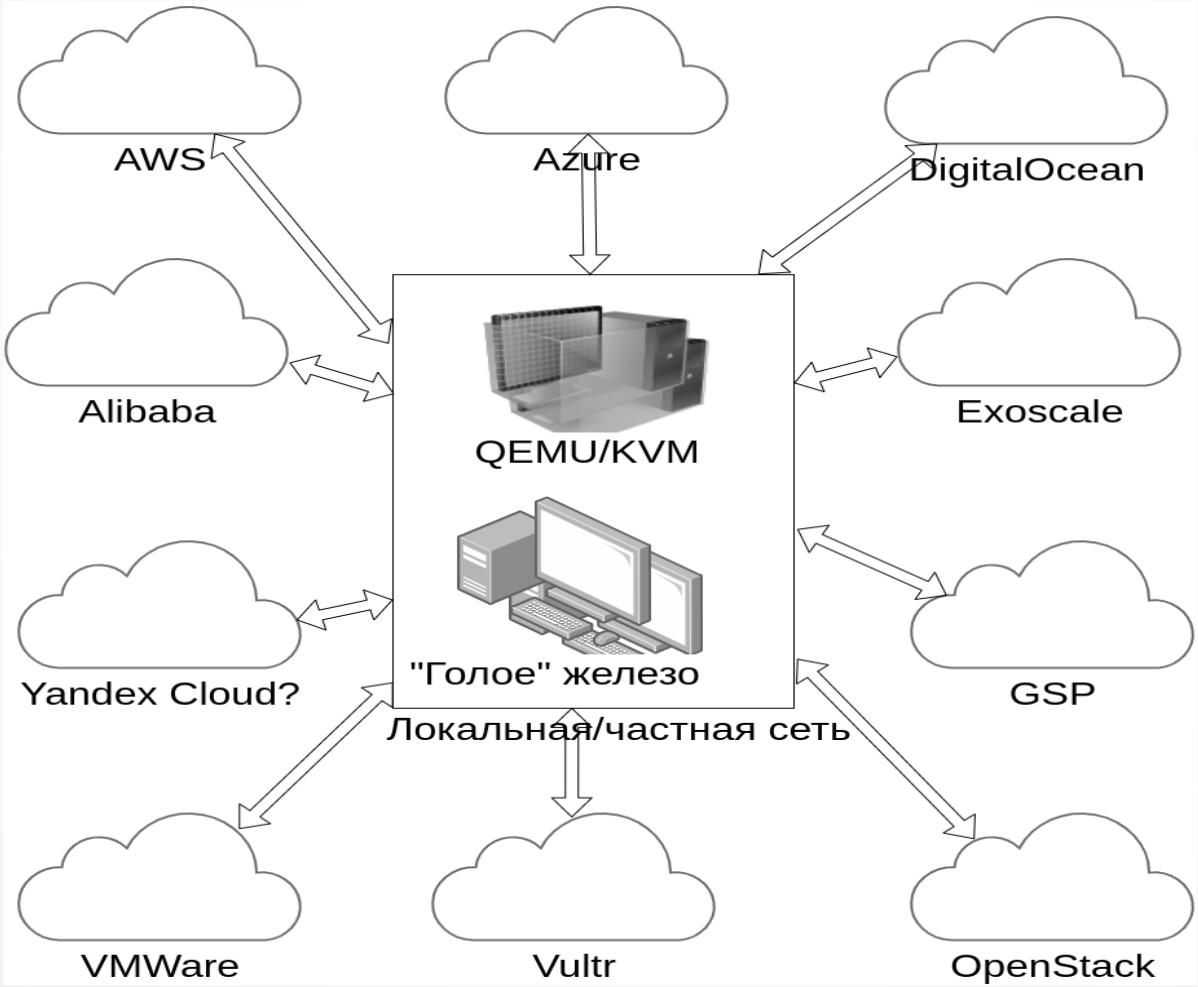
Fedora CoreOS
Мы Федоре не враги

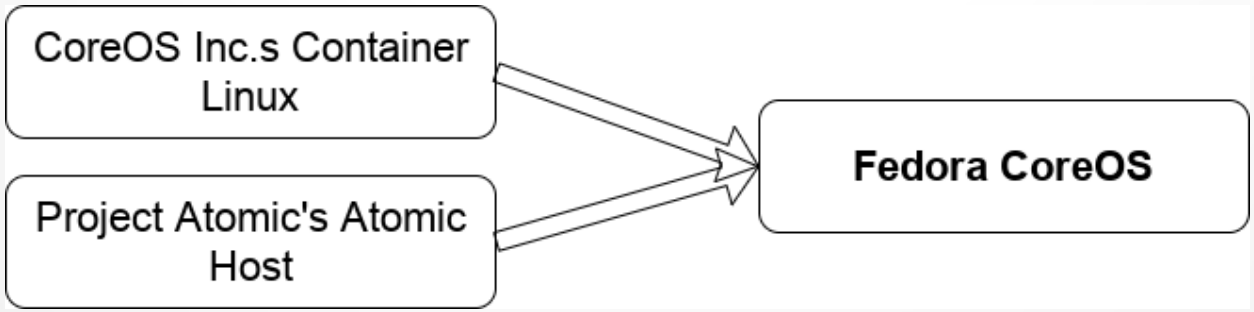
Целевая ниша Fedora Core

- автоматизация разворачивание и обновления узлов мультиоблачного кластера.



Родители

- Заимствования из Container Linux (проект почил в бозе)
  - Философия
  - Стек поддержки (Provision Stack?)
  - Опыт развертывания в облаках различного типа
- Заимствования из Atomic Host
  - Fedora Foundation;
  - Стек обновления дистрибутива;
  - SeLinux Enhanced Security.



Философия Container Linux

- Атомарные обновления
  - автоматическая установка/обновления без вмешательства оператора;
  - автоматическая синхронизация с последней версией дистрибутива (Bug Fixes).
- Все узлы разворачиваются с одной стартовой точки:

  использование ignition (описание конфигурации узла) при разворачивании и обновлении узла, где бы он ни находился
- Неизменная инфрастуктура:
  - Нужны изменения - обновите конфигурация и перегрузитесь.
- Весь пользовательский софт работает в контейнерах, что позволяет более гибко обновлять узлы кластера.

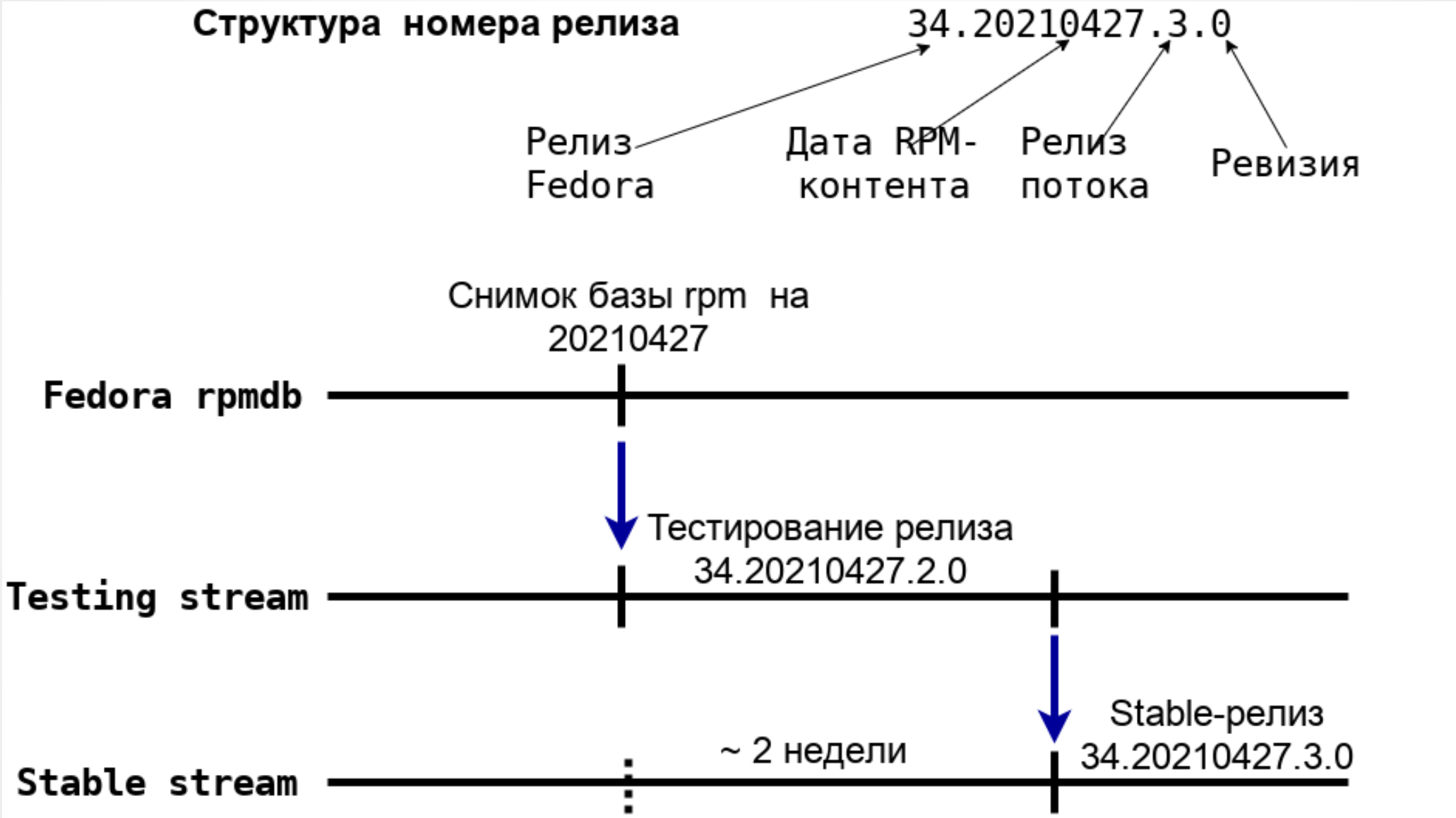
Несколько потоков обновления

- Поддерживается три потока обновления с автоматическим обновлением:
  - **Next** - Эксперементальные фичи мажорных релизов Fedora
  - **Testing** — тестирование следующего релиза **Stable**.
  - **Stable** — наиболее надежный поток на основе фиксации потока **Testing**
- Цели:
  - Публикация новый релизов примерно через 2 недели
  - Фиксация проблем в потоках **Next**, **Testing** до выхода очередного релиза **Stable**

Особенности Fedora CoreOS

- Автоматические обновления == надежные обновление
  - Глубокое тестирование ПО между обновлениями
  - Несколько потоков обновления: **Next**. **Testing**, **Stable** — пользователь может использовать любой
  - Регулярные управляемые релизы (rollouts) через несколько дней, приостановка релиза при обнаружении проблем
  - Возможность отката на предыдущий релиз через rpm-ostree

«Продвижение» релиза



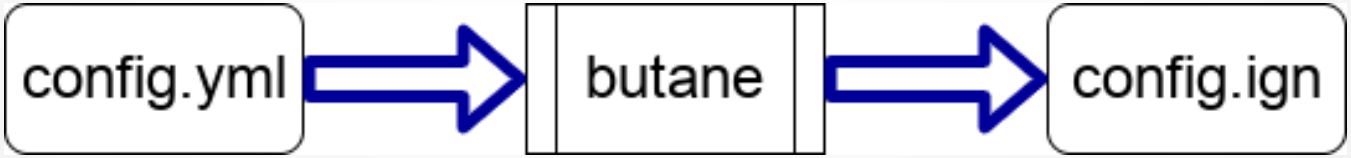
Автоматическое разворачивание ОС

Fedora CoreOS использует сервис **ignition** (зажигание) для автоматического разворачивания ОС:

- Вся конфигурация жизненного цикла (число и разбиение дисков, сетевые интерфейсы, запускаемые сервисы и контейнеры, ...) сервера описаны в конфигурации **ignition**
  - Очень просто переустановить сервер
- Одна стартовая точка для установки как на «голое», виртуальное железо, так и в облачные сервисы
  - Для разворачивания и обновления ОС для всех сред используется единый сервис **ignition**

Ignition: детали

- Ignition-конфигурация:
  - Машинно-читаемый JSON-документ
  - Выполняется только один раз при установке ОС на стадии **initramfs**
  - Может выделять дисковое пространство, RAID-массивы, создавать файловые системы, пользователей, группы, сетевые интерфейсы, systemd юниты и обычные файлы
  - В случае сбоя или ошибки прекращает разворачивание (нет недоустановленных ОС)
- Создание конфигураций:
  - Автоматически или вручную создается человекочитаемый YML-файл
  - Butane конвертирует файл в JSON-формат **ignition**
  - Файл размещается на локальном или сетевом ресурсе



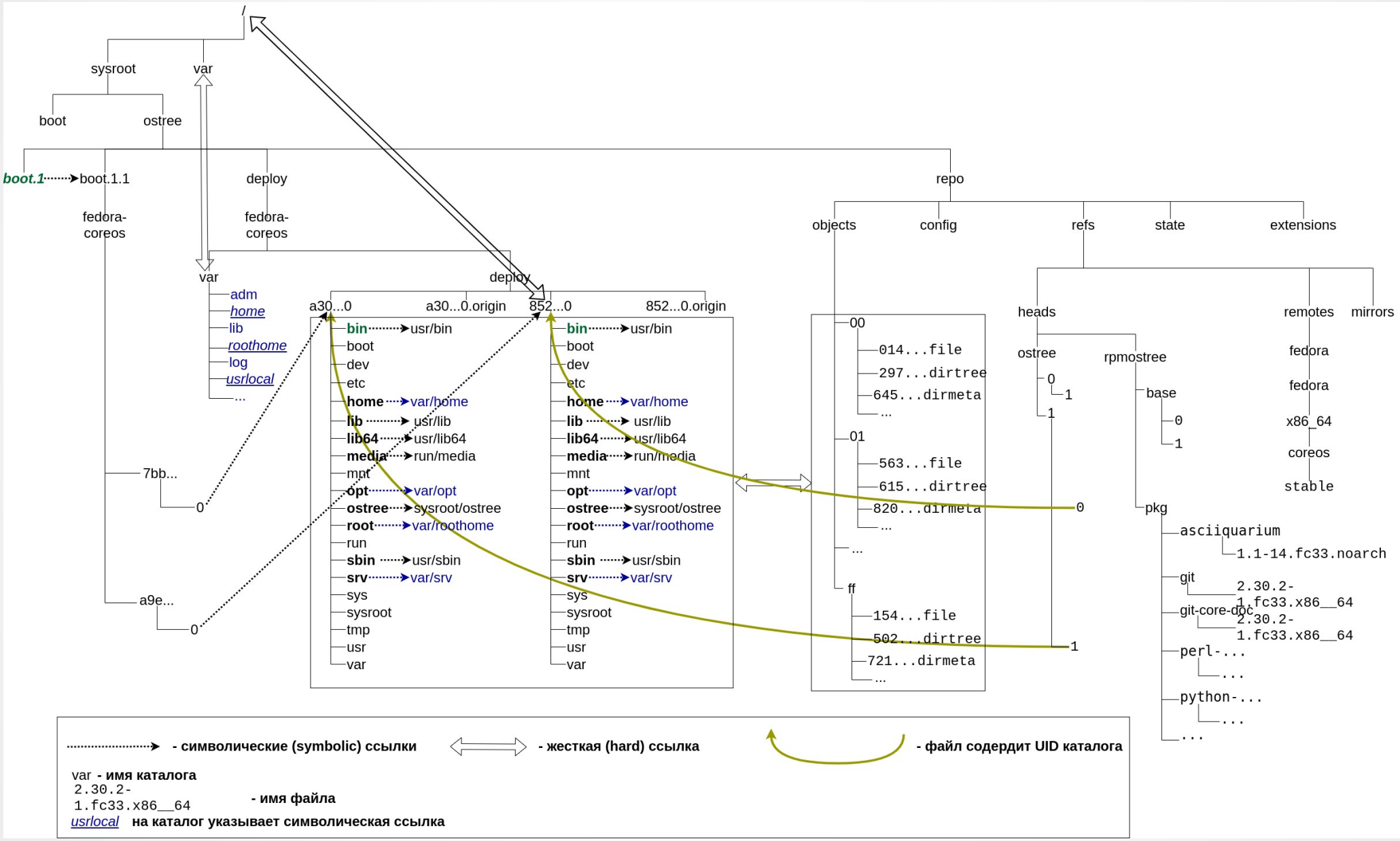
Облачно-ориентированный с фокусом на контейнерах

- Все пользовательское ПО работает в контейнерах
  - В среде podman или docker (moby engine)
- Обеспечивает разворачивание кластеров:
  - За счет ignition-конфигураций разворачивание сотен узлов и объединение их в кластер
  - Вывод из кластера ненужных в данный момент узлов
  - Добавление их при увеличении нагрузки
- Поддерживает множество cloud/virt платформ:
  - Alibaba, AWS, Azure, DigitalOcean, Exoscale, GCP, Openstack, Vultr, WMWare, QEMU/KVM

Версионирование ОС и защита

- Fedora CoreOS использует технологию (rpm-)ostree
  - A“la git для всей ОС — единственный идентификатор релиза определят ВСЕ системное ПО
  - Системные каталоги (/usr/) монтирутся только на чтение — защита от злоумышленников и новичков
- Режим SELinux включен по умолчанию — защита от доступа к важным ресурсам из скомпроментированного ПО

Структура файловой системы



Что внутри Fedora Core

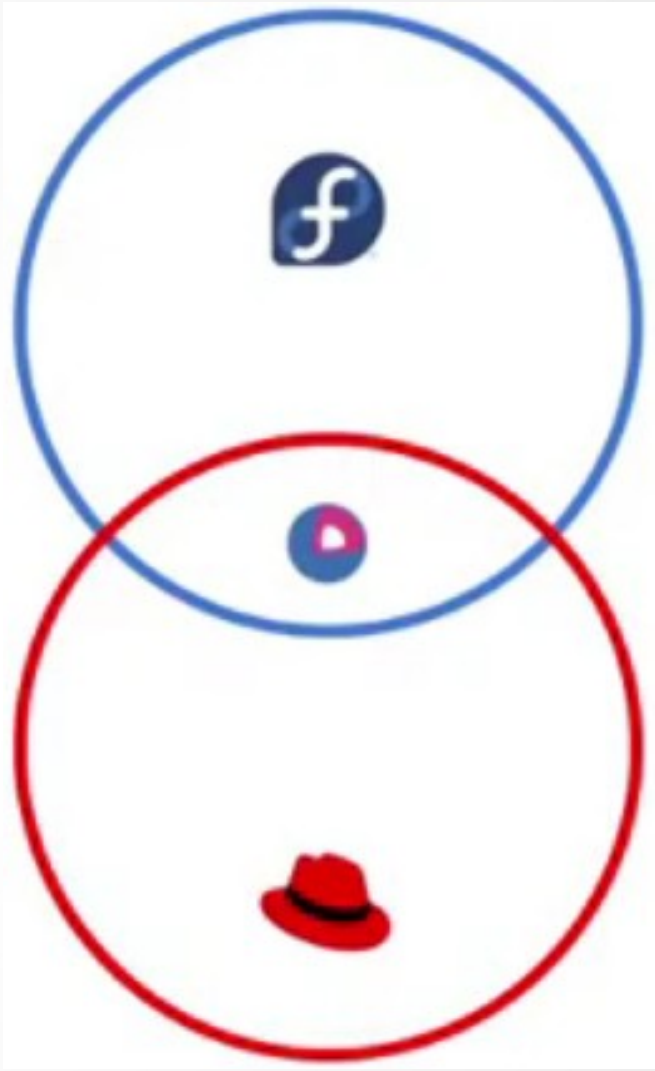
- Свежие компоненты (RPM-пакеты)
- Поддержка оборудования
- Основные административные инструменты (команды)
- Контейнерные движки — podman, docker (moby engine)
- Без«питоновость»

Вскоре ожидаются

- Большее число поддерживаемых облачных сред;
- Многоплатформенность (aarch64, ppc64le, s360x)
- Больше удобочитаемых вспомогательных функций в FCCT (Butane)
- Расширения хостов (более гибкая раскладка пакетов по уровням)
- Больше (улучшенной) документации
- Плотная интеграция с OKD

Fedora CoreOS & RHEL CoreOS

Общие инструменты и компоненты / разные цели и сферы



- RHEL CoreOS не предназначена для stanalone решений
  - Пакетная база RHEL
  - Включает компоненты OpenShift
  - Конфигурация и обновления производятся вручную Cloud-оператором
- Fedora CoreOS
  - Пакетная база Fedora
  - Разделяет общие инструменты и компоненты с RHEL CoreOS
  - StandAlone ОС с автообновлением

OKD на Fedora CoreOS

- Устанавливается через OKD-инсталлер (openshift-install)
- Кластер контролирует обновление ОС через machine-config-operator
- Обновления ПО поддерживаются machine-os-content контейнеры
- Кластер может управляться и принимать новые узлы автоматически

Fedora IoT vs Fedora Core

Сходства дистрибутивов:

- Использование `ostree`, `rpm-ostree` для поддержания неизменяемой операционной системы с атомарными изменениями.
- Использование `ignition` для автоматического разворачивания на множество аппаратных устройств.
- Пользовательские приложения разворачиваются в контейнерной среде.
- Поддержка `TPM2`, `SecureBoot` и автоматического расшифровки данных с устройств хранения с помощью `Clevis`.

Отличия дистрибутива *Fedora IoT* от *Fedora Core*:

- Поддержка различных аппаратных платформ: `x86_64`, `aarch64`, `armhfp`.
- Упор на поддержку интернет-устройств и драйвером к ним.
- Меньший объем дискового прострнства `~1.5GB` .
- Контейнеризация осуществляется через `podman`, поддержка клиент-серверной модели `moby engine` (`docker`) отсутствует;`
- Веб-служба `Zezere` с помощью которого администраторы могут развертывать и настраивать *Fedora IoT* масштабируемым образом без физической консоли.

Включайтесь

- Web: https://getfedora.org/coreos
- Вопросы: https://github.com/coreos/fedora-coreos-tracker/issues
- Форум: https://discussion.fedoraproject.org/c/server/coreos/
- Mailing list: coreos@lists.fedoraproject.org
- IRC: freenode #fedora-coreos
- Devconf.cz
  - Up and running with Fedora CoreOS (Friday Feb 19)
  - Getting started with Fedora CoreOS. A Hands-on lab (Saturday Feb 20)

ALT CoreOs
Альт ЯдрёнаОСь

Пакет	Описание	Sisyphus	Примечание
ostree	Система обновления версий операционных систем на базе Linux	**портирована**	
ignition	Утилита для управления дисками во время начальной установки системы	**портирована**	
dracut	Инструментарий создания файловой системы начальной загрузки `initramfs`	**портирована**	В рамках `ALTLinux` используется собственный технологический процесс создания `initrams`
`butane`	Утилита конвертации файлов описания конфигурации из формата `YAML` в формат `JSON Ignition`	-	Достаточно простая утилита
`coreos-installer`	Программа установки `CoreOs`	-	Возможно создание собственной программы
`rpm-ostree`	Аналог программы `apt-get` установки `RPM`-пакетов в файловую систему `ostree`	-	Возможно потребуется не весь функционал
`zincati`	Агент автообновления между текущей и предыдущей версией	-	Достаточно простая утилита
`bootupd`	Сервис обновления начальных загрузчиков	-	Достаточно простая утилита, но возможны конфликты с текущей архитектурой

Сравнение CoreOS“ов

Дистрибутив	Fedora CoreOS	Fedora IoT	FlatCar (CoreOS) Container Linux	Ubuntu Core	Chrome OS	GNOME OS	Endless OS	TorizonCore
Пакетная база	Fedora	Fedora	Gentoo	Ubuntu	Gentoo		Debian	Yocto Project (Poky)
Потоки(Streams)	Next, Testing, Stable	Stable	Alpha, Beta, Stable, LTS	Releases			Edge, Beta, Alpha, Stable	
Платформа	x86_64	x86_64, aarch64, armhfp	amd64. arm64	amd64. arm64	x86_64, arm64		x86_64	arm64
Ниша	Cloud, VM, BM	ED	Cloud, VM, BM	ED	D	D	D	ED
Контейнеризация	podman, mobyengine	podman	docker, rkt			flatpak	flatpak	docker (debian images)
ПО мультидеплоя	ostree	ostree	lvm - (две партиции USRA, USRB)	snap		ostree	ostree	ostree, Uptane
Пакетный менеджер	rpm-ostree	rpm-ostree	-	Snappy	portage, chroot		deb-ostree-builder, apt, dpkg	
Ignition	Да	Да	Да	Нет	Нет	Нет	Нет	?
Атомарность	развертывания	развертывания	развертывания	Ядро?	?	Да	Да	?
Автообновление	Да	Нет	Да	Да	Да	Да	Да	?
Хранение развертываний	HL	HL	PS(USR-A, USR-B)	SNAP	PS	HL	HL	HL
Откат(rollback)	Да	Да	Да	Да	?	Да	Да	?
ReadOnly дерево	/usr	/usr	/usr	/snap	?	/usr	/usr	/usr
Шифрование диска	Да	Да	?	Да	?	?	?	?
Системные сервисы	systemd, sssd , zincati, podman, docker	systemd, parces, zezere, podman	systemd, etcd, docker, rtk, fleet	snapd		flatpak, ostree	eos-stage-ostree, eos-autoupdater, ostree	portainer, systemd, docker, podman
Сборка образа	dracut	dracut					dracut	bitbake
kexec	Да?	Да?	Да	?	?	Да?	Да?	Да?

Спасибо за внимание

Костарев А.Ф.

ООО «Новая платформа»
kaf@neoplatform.ru
kaf@nevod.ru

«Базальт СПО»
kaf@basealt.ru