thin os для управления контейнерами

- основные приколы thinOS
  - минимум пакетов, максимум заявлений о security first: offline сборки для установки/обновления ОС в airgap окружениях, шифрованные диски и вот это вот всё.
  - конфиги для сборки/установки ОС в ассортименте - json/yaml/bash
  - предпочитают установку поверх гипервизора, интересно зачем.
  - новый или обёрнутый в скрипты менеджер пакетов/сервисов для изоляции и версионирования
  - система сужения maintenance window через снимки/откаты, либо на уровне ФС, либо отдельным сервисом пакетов для пакетов.
  - ессно, пачка самых-самых утилит и фреймворков для управления контейнерами docker/podman.
  - итого тихой сапой идёт замещение гипервизоров/виртуализации на thinOS+kubernetes. Ведь по сути экосистемы гипервизоров делают то же самое, что и экосистема kubernetes.
- итого, есть ОС от:
  - vmware - Умеет в realtime kernel. SLES под капотом. tdnf вместо zypper для управления пакетами. Выбор стабильных корпоратов, plugNpray.
  - Fedora не умеет в железо, сборка через rpm-ostree, конфиги ОС на json/yaml. Выбор неопределившихся.
  - suse в основе rpm/zypper+btrfs и bash(!) для конфига ОС(есть UI WYSWYG). Выбор дедов.
  - Ubuntu - snapd пакеты для пакетов, конфиги на json, нужен облачный аккаунт для сборки. Выбор смелых.
  - Flatcar - это gentoo и аналог coreOS/Fedora, но умеет в железо и сборку из исходников kernel.org. Выбор пытливых.
  - Ranch, от него отвалилась ОС, вместо неё теперь Harvester HCI с экосистемой для kuber. Умеет в железо. Под капотом SLES. Выбор любителей кубических форм.

Fedora CoreOS

- один из наследников coreos
- containerd 1.6.23, kernel 6.8.11
- Fedora CoreOS does not have a separate install disk. Instead, every instance starts from a generic disk image which is customized on first boot via Ignition.
- Fedora CoreOS ships with both the docker CLI tool (as provided via Moby) and podman installed.
- https://mobyproject.org/ для управления docker
- два несовместимых формата файлов конфигурации/сборки ОС - ignition(json) и butane(yaml)
- запутанная документация
- rpm-ostree для управления пакетами, версионирования, откатов
- KVM/libvirt
- Currently, the OSTree and SELinux tooling conflict a bit. If you have permanently applied local policy modifications then policy updates delivered by the OS will no longer apply; your policy stays frozen. This means any policy "fixes" needed to enable new functionality will not get applied. See coreos/fedora-coreos-tracker#701 for more details.

Gentoo Flatcar

- аналог fedoraCoreOs, да, тоже наследник
- два конфига - ignition/json + butane/yaml есть конвертер
- A minimum of 2 GB of RAM is required to boot Flatcar Container Linux via ISO
- The Flatcar Linux kernel build is split over multiple `gentoo` ebuild files
- https://www.flatcar.org/docs/latest/reference/developer-guides/sdk-modifying-flatcar/
- https://github.com/flatcar
- подкостыленный systemd-sysext для управления версиями системных сервисов
- https://github.com/flatcar/sysext-bakery
- не умеет в OTA(обновления без перезагрузки)

SuSe MicroOS

- minimum 1 GB physical RAM
- The package list is similar to the SUSE Linux Enterprise Server minimal system.
- MicroOS 5.2 based on Leap 15.3
- kernel 6.9+
- btrfs+snapper - основа, откаты и версионирование пакетов/системы через снимки
- / (root) partition: 5 GB available disk space minimum, 20 GB maximum
- /var partition: 5 GB available disk space minimum, 40 GB or more recommended
- read-only root filesystem to avoid accidental modifications of the OS
- The Transactional Updates technology leverages btrfs snapshots to apply package updates without interfering with the running system
- health-checker to verify the OS is operational after updates. Automatically rolls back in case of trouble.
- cloud-init for initial system configuration during first boot on Cloud (includes OpenStack)
- три конфига для сборки ОС
    - Ignition - has its origins in Fedora CoreOS and is fully supported by openSUSE MicroOS. Best choice for beginners.
    - Combustion - is part of openSUSE's MicroOS project and is more powerful and flexible than Ignition and requires bash programming skills.
    - Cloud-Init - is used only for the OpenStack Cloud variant of openSUSE MicroOS. Learn more from the Cloud-Init Quick Start Documentation.
- UI для конфигов ОС https://opensuse.github.io/fuel-ignition/
- Podman Container Runtime available
- Rolling Release: Every new openSUSE Tumbleweed snapshot also automatically produces a new openSUSE MicroOS release. The Leap based version automatically updates when maintenance updates for Leap are published.
- https://github.com/clearlinux/tallow - fail2ban/lard replacement that uses systemd's native journal API to scan for attempted ssh logins, and issues temporary IP bans for clients that violate certain login patterns

Ubuntu Core

- мы не CoreOS, мы - Core!!!
- минимальная установка, остальное через snapcraft
- kernel 5.15 Ubuntu 22.04 Jammy
- new: Ubintu 24 Noble https://ubuntu.com/core/docs/uc24

- https://ubuntu.com/core/docs/build-an-image
- конфиг ОС на json https://ubuntu.com/core/docs/create-model-assertion
- умеет в железо

Rancher

- SUSE
- https://github.com/docker/machine - устарел, но используется для управления в простых окружениях workstation
- https://github.com/rancher/os сдох 5 лет назад, его не поддержали разработчики linux
    - all is docker
    - ext4
    - virtualbox, vmware, aws
    - docker+system docker
- https://docs.k3s.io/ - kuber IoT
- https://docs.harvesterhci.io/v1.3
    - bare metal. provides virtualization and distributed storage capabilities. In addition to traditional virtual machines (VMs), Harvester supports containerized environments automatically through integration with Rancher.
    - Linux OS. Elemental for SLE-Micro 5.3 is at the core of Harvester and is an immutable Linux distribution designed to remove as much OS maintenance as possible in a Kubernetes cluster.
    - Harvester is an HCI solution with Kubernetes under the hood.
    - KubeVirt provides virtualization management using KVM on top of Kubernetes.
    - Longhorn provides distributed block storage and tiering.
    - Grafana and Prometheus provide robust monitoring and logging.
- https://longhorn.io/docs/1.6.2/what-is-longhorn/
    - DFS для kubernetes volumes, платформонезависимый
    - The Longhorn CSI driver takes the block device, formats it, and mounts it on the node. Then the kubelet bind-mounts the device inside a Kubernetes Pod. This allows the Pod to access the Longhorn volume.
    - Ubuntu 22.04, SLES 15 SP5, RHEL 9.3
    - Minimum Recommended Hardware
    - 3 nodes
    - 4 vCPUs per node
    - 4 GiB per node
    - 10 Gbps network bandwidth between nodes
    - SSD/NVMe or similar performance block device on the node for storage (recommended)
    - 500/250 max IOPS per volume (1 MiB I/O)
    - 500/250 max throughput per volume (MiB/s)
    - periodically delete all types of snapshots, trim the filesystem
    - A Longhorn volume itself cannot shrink in size if you've removed content from your volume. This happens because Longhorn operates on the block level, not the filesystem level.

VMware Photon OS

- https://vmware.github.io/photon/
- Photon OS 5.0 contains: Linux kernel 6.1.10, Gcc : 12.2, Glibc 2.36

- дружит с VMWare ESXi и Vagrant
- Open virtualization
- Real Time Kernel Support
- умеет в железо
- для сборки образа ОС зачем-то требует Ubuntu 14+
- works with the most common container formats, including Docker, Rocket, and Garden
- Deployment using RPM-OStree. OSTree is a tool to manage bootable, immutable, versioned filesystem trees. Unlike traditional package managers like rpm or dpkg that know how to install, uninstall, configure packages, OSTree has no knowledge of the relationship between files. But when you add rpm capabilities on top of OSTree, it becomes RPM-OSTree, meaning a filetree replication system that is also package-aware.
- управление пакетами через новое поколение yum/dnf - tdnf - tiny dandified yum. It is a C implementation of the DNF package manager without Python dependencies.
- управление сервисами через systemd
- https://github.com/vmware/pmd-next-gen photon-mgmt для управления/мониторинга сервисов
- cntrctl для управления контейнерами

образ ОС для контейнера

- Alpine
  - наименьший размер, однако там musl libc вместо стандартной glibc. Поэтому некоторое старое ПО может глючить из-за недостаточных libc зависимостей.
  - See this Hacker News comment thread for more discussion of the issues that might arise and some pro/con comparisons of using Alpine-based images.
  - `alpine` image description
  - https://wiki.alpinelinux.org/wiki/Running_glibc_programs
  - https://stackoverflow.com/questions/70243938/use-shared-library-that-uses-glibc-on-alpinelinux
  - MUSL is lighter and doesn't drag a legacy with it. This is a problem when applications depend on the legacy, like when they want to use pthread.
  - Comparison of C/POSIX standard library implementations for Linux
- oracle linux
  - Ksplice for zero-downtime kernel patching, DTrace for real-time diagnostics, Btrfs file system
- ubuntu
  - This is the defacto image. If you are unsure about what your needs are, you probably want to use this one. It is designed to be used both as a throw away container (mount your source code and start the container to start your app), as well as the base to build other images off of.