Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Talos Linux: неизменяемая ОС для Kubernetes без SSH

Разворачиваем прод-кластер на Talos 1.13: Image Factory, mTLS-API, A/B-обновления, шифрование

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Kubernetes-ноды на универсальном Linux — это сотни пакетов, SSH и дрейф конфигураций: через год ноды различаются, обновления превращаются в ночные работы, а побег из контейнера даёт shell на хосте. Мы переводим ноды на Talos Linux: образ ~80 МБ, read-only корень, управление только через mTLS-API. Кластер обновляется скриптом за минуты и не деградирует со временем.

Почему это важно бизнесу

- Обновление парка нод сжимается с часов ручной работы до 15–20 минут скриптом — без ночных окон и простоя сервисов
- Минимальная поверхность атаки: нет SSH, shell и пакетного менеджера — типовые сценарии закрепления злоумышленника на ноде не работают
- Идентичные ноды из одного образа: нет «особенных» серверов, отказ любой ноды лечится переустановкой за минуты
- A/B-схема разделов с автооткатом: неудачное обновление не оставляет ноду мёртвой и не требует выезда в серверную

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

1.13.x

Рабочая ветка Talos: ставим только стабильные патч-релизы; в составе ядро Linux 6.18, containe…

Talos Linux 1.13

1.36

Kubernetes в комплекте Talos 1.13; версию кластера двигаем отдельно командой talosctl upgrade-…

по докам Sidero Labs

3+3

Минимум прод-кластера: 3 control-plane (кворум etcd) + 3 worker; workload-ы на CP не пускаем

наш стандарт

80 МБ

Размер образа ОС: монолитный read-only squashfs, ноль пакетов — нечего патчить и нечем «обраст…

по докам Talos

50000

Порт apid: весь менеджмент — gRPC поверх mTLS с сертификатами из talosconfig; SSH на нодах нет

Talos API

30–60 с

Перезагрузка ноды в новый образ при апгрейде: A/B-разделы, при сбое загрузки — автооткат на пр…

по докам Talos

РЕАЛИЗАЦИЯ 1 ИЗ 3

Сборка образа и раскатка кластера с нуля

Что настраиваем

Bare-metal или Proxmox/VMware: 6 нод, собственный schematic в Image Factory

Как мы это делаем

1. Собираем schematic на factory.talos.dev: extensions qemu-guest-agent, iscsi-tools, util-linux-tools; ID схемы фиксируем в репозитории
2. talosctl gen secrets -o secrets.yaml, затем gen config --with-secrets; сам secrets.yaml сразу в сейф — это ключи PKI всего кластера
3. Патчи machine-config: VIP для control-plane (machine.network.interfaces[].vip.ip), NTP, nameservers, kubelet rotate-server-certificates: true
4. talosctl apply-config --insecure на ноды в maintenance-режиме, bootstrap первой CP-ноды, ждём talosctl health до зелёного
5. CNI по умолчанию Flannel; под Cilium ставим cni.name: none и proxy.disabled: true, сам Cilium — helm-ом после bootstrap

РЕЗУЛЬТАТ

Кластер поднимается воспроизводимо за 1–2 часа вместо рабочего дня: каждая нода — функция от образа и machine-config, вся конфигурация в git, «ручных» серверов с уникальной историей не существует.

КЛЮЧЕВОЙ НЮАНС

secrets.yaml генерируется один раз и живёт всю жизнь кластера: потеря = потеря доступа к Talos API, утечка = полный контроль над кластером. Храним отдельно от machine-config и репозитория.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Эксплуатация без SSH: диагностика и апгрейды

Что настраиваем

Все ноды кластера; рабочее место инженера — talosctl + talosconfig с ролью os:admin

Как мы это делаем

1. Диагностика через API: talosctl dashboard, logs kubelet/etcd, dmesg, netstat, processes, mounts — всё read-only, на хост не заходим
2. Апгрейд ОС: talosctl upgrade --image factory.talos.dev/installer/<schematic>:v1.13.x --wait, строго по одной ноде
3. Kubernetes отдельно: talosctl upgrade-k8s --to 1.36.x — последовательно прокатывает apiserver, controller-manager, scheduler, kubelet
4. Перед апгрейдом CP: talosctl etcd snapshot db.snapshot + выгрузка снапшота за пределы кластера; после каждой ноды — talosctl health
5. Отладка приложений: kubectl debug с ephemeral-контейнером (netshoot) внутри pod — без доступа к хост-системе

РЕЗУЛЬТАТ

Плановое обновление 6 нод — 15–20 минут скриптом без окна простоя: pod-ы мигрируют на drain, нода возвращается за 30–60 секунд, при сбое загрузки срабатывает автооткат на предыдущий раздел.

КЛЮЧЕВОЙ НЮАНС

Minor-версии Talos апгрейдим только последовательно (1.12→1.13), а в installer-образе обязан быть наш schematic — стоковый ghcr.io/siderolabs/installer молча выкидывает все extensions.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Безопасность: mTLS, шифрование дисков, восстановление

Что настраиваем

Сетевой периметр кластера + control-plane; регламент восстановления нод и etcd

Как мы это делаем

1. Порты 50000 (apid) и 6443 закрываем на уровне сети: доступ только из админ-VLAN/VPN; talosconfig раздаём по ролям os:admin / os:reader
2. Шифрование разделов STATE и EPHEMERAL через machine.systemDiskEncryption, ключ — в TPM 2.0: извлечённый диск нечитаем
3. Бэкап control-plane: talosctl etcd snapshot db.snapshot по cron + данные PV отдельно (Velero / CSI-снапшоты) — это разные контуры
4. Восстановление ноды: talosctl reset либо переустановка с того же образа + apply-config — 10 минут до статуса Ready

РЕЗУЛЬТАТ

Кража диска или сервера не отдаёт данные, компрометация pod-а не превращается в компрометацию ноды, а сценарий «умер control-plane» отработан: восстановление API кластера из снапшота etcd за 30–40 минут.

КЛЮЧЕВОЙ НЮАНС

Шифрование включаем ДО установки: конвертация занятых STATE/EPHEMERAL на лету не поддерживается — только через reset ноды. Наличие и версию TPM 2.0 на bare-metal проверяем заранее.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Longhorn/iSCSI без extensions**
  В базовом образе нет iscsid и nsenter-утилит — CSI молча не монтирует тома. Заранее включаем iscsi-tools и util-linux-tools в schematic
- ✕ **Апгрейд стоковым installer**
  talosctl upgrade с образом ghcr.io/siderolabs/installer теряет все extensions; используем только factory.talos.dev/installer/<schematic-id>
- ✕ **Данные на EPHEMERAL-разделе**
  hostPath на системном диске стирается при reset и переустановке; PV размещаем только на отдельных дисках через UserVolumeConfig или CSI
- ✕ **apid доступен из общей сети**
  Порт 50000 защищён mTLS, но наружу его не публикуем: только админ-VLAN/VPN. Режим --insecure допустим лишь в maintenance до применения конфига
- ✕ **Прыжок через minor-версии**
  Upgrade поддержан только на соседний minor: 1.11→1.13 напрямую ломается — идём 1.11→1.12→1.13, по одной ноде с --wait
- ✕ **Kubernetes отстал от Talos**
  talosctl upgrade не трогает K8s: следим за version skew kubelet/apiserver и сразу катим talosctl upgrade-k8s следом за ОС
- ✕ **DHCP без резервации на нодах**
  Смена IP рушит endpoints в talosconfig и SAN сертификатов API; ставим static lease или фиксируем machine.network.addresses
- ✕ **Один control-plane «для экономии»**
  etcd без кворума: любой ребут CP — недоступный API кластера. Для прода только 3 CP; на стенде — хотя бы регулярный etcd snapshot

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- 3 CP + 2–3 worker, свой schematic в Image Factory, secrets.yaml в сейфе
- Порты 50000 и 6443 только из админ-сети, talosconfig не раздаём общим файлом
- Cron: talosctl etcd snapshot db.snapshot + выгрузка снапшота за пределы кластера

НОРМАЛЬНО

- VIP на control-plane, rotate-server-certificates + kubelet-serving-cert-approver
- Патч-релизы Talos ежемесячно скриптом: по одной ноде, --wait и health-гейт
- Шифрование STATE/EPHEMERAL с ключом в TPM 2.0 на bare-metal
- Мониторинг kube-prometheus-stack + метрики etcd и статусы апгрейдов

ХОРОШО

- GitOps на machine-config: патчи в git, применение через CI, либо Sidero Omni
- KubeSpan (WireGuard-mesh) для нод на разных площадках без ручных туннелей
- Учения по DR: восстановление control-plane из снапшота etcd на стенде
- SecureBoot: подписанные UKI-образы из Image Factory, ключи в UEFI

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Schematic образа зафиксирован (ID в репозитории), список extensions описан явно?
- [ ] secrets.yaml хранится вне репозитория конфигов и доступен минимум двум ответственным?
- [ ] Порты 50000 (apid) и 6443 недоступны из пользовательской сети и интернета?
- [ ] Снапшот etcd снимается по расписанию и уезжает за пределы кластера?
- [ ] Installer-образ для апгрейда берётся из Image Factory с вашим schematic, не стоковый?
- [ ] Версия Kubernetes обновляется вслед за Talos (upgrade-k8s), version skew в норме?
- [ ] PV лежат на отдельных дисках, а не на системном разделе EPHEMERAL?
- [ ] IP нод статичны (static lease), VIP для control-plane настроен?
- [ ] Есть замер: сколько минут занимает пересоздание умершей ноды до Ready?
- [ ] Диски STATE/EPHEMERAL зашифрованы, ключ в TPM 2.0 проверен на вашем железе?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Проектируем и разворачиваем кластер Talos под ключ: bare-metal, Proxmox, VMware — от schematic до Ready
- Мигрируем работающий кластер с Ubuntu/kubeadm на Talos без простоя: сначала worker-ы, затем control-plane
- Настраиваем эксплуатацию: бэкап etcd, мониторинг, регламент апгрейдов, шифрование дисков
- Обучаем команду заказчика работе через talosctl и берём кластер на поддержку 24/7

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Talos Linux Docs — Getting Started / Production Cluster (talos.dev — v1.13)

02 What's New in Talos 1.13 (Sidero Documentation) (docs.siderolabs.com — v1.13)

03 Image Factory: boot assets и system extensions (factory.talos.dev — 2026)

04 Talos Docs — Upgrading Talos / Upgrading Kubernetes (talos.dev — v1.13)

05 Talos Docs — Disk Encryption (STATE/EPHEMERAL, TPM 2.0) (talos.dev — v1.13)

06 Наш шаблон machine-config патчей: VIP, NTP, sysctl, kubelet (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.