Развёртывание OSTree-образа

1. Общие сведения

1.1 Назначение

Настоящий раздел устанавливает порядок понимания и применения механизма развёртывания НАЙС.ОС на базе **OSTree** (rpm-ostree-подход) с использованием скрипта mk-ostree-host.sh. Цель — получить воспроизводимый загрузочный дисковый образ, пригодный для развёртывания в ВМ/на стендах, где требуется единообразие состава файловой системы и предсказуемость загрузки.

1.2 Ключевые определения (в контексте данного руководства)

- **OSTree** — механизм доставки и хранения коммитов (снимков состояния) файловой системы и управления деплоями (развёртываниями) и откатами.
- **ref** (REPO_REF) — ссылка на ветку/канал в OSTree-репозитории (например, niceos/5.2/x86_64/base), по которой выполняется **pull** и **deploy**.
- **sysroot** — корневой каталог целевой системы, внутри которого OSTree размещает деплои и служебные данные (обычно /ostree и структура /ostree/deploy/...).

1.3 Суть подхода НАЙС.ОС: “развёртывание не установкой, а образом”

В НАЙС.ОС для типовых инфраструктурных сценариев (виртуальные машины, edge-узлы, шаблоны ролей) удобен подход, при котором конечная система получается не “набором ручных действий” после установки, а как **готовый дисковый образ**, внутри которого уже выполнен deploy выбранного OSTree-рефа. Такой образ переносится между средами как единый артефакт, что упрощает контроль, повторяемость и аудит.

1.4 Ожидаемый результат выполнения mk-ostree-host.sh

- Создаётся файл образа: <IMG_NAME>.raw заданного размера (FILE_SIZE, ГБ).
- Внутри образа формируется GPT-разметка (BIOS-ориентированная):
  - p1 — служебный раздел bios_grub (тип GPT ef02);
  - p2 — /boot (ext4);
  - p3 — корневой раздел / (ext4).
- Выполняется **инициализация OSTree**, добавление remote, **pull** заданного рефа и **deploy** в sysroot.
- Выполняется **установка GRUB2** в образ и формирование конфигурации загрузки.
- Производится настройка параметра ядра root= и запись /etc/fstab для / и /boot.

1.5 Принципиальный момент: почему существует параметр --root-dev

В процессе сборки образ подключается как loop-устройство, а разделы доступны через device-mapper (например, /dev/mapper/loop0p3). В целевой среде (после импорта образа в ВМ/на хост) устройство корня обычно будет называться иначе: чаще /dev/sda3 (SATA/SCSI) либо /dev/vda3 (virtio). Поэтому скрипт выполняет приведение загрузочных записей к ожидаемому имени устройства — это обеспечивает предсказуемую загрузку без ручной правки.

1.6 Командная форма применения (справочно)

Развёртывание выполняется запуском mk-ostree-host.sh с указанием размера образа, имени, адреса OSTree-сервера, рефа и точки монтирования sysroot. Параметр --root-dev следует выбирать по типу дискового контроллера целевой среды (см. примечание ниже).

```
sudo ./mk-ostree-host.sh \
 -s 20 \
 -n niceos-5.2-base \
 -i 10.0.0.10 \
 -r niceos/5.2/x86_64/base \
 -m /mnt/niceos-root \
 --root-dev /dev/sda3
```

Примечание. Для virtio (KVM/QEMU с if=virtio) корневой раздел, как правило, будет /dev/vda3; для SATA/SCSI чаще /dev/sda3.

1.7 Ограничения и требования безопасности (обязательные)

- Скрипт выполняется **только от root** и использует losetup, kpartx, монтирование файловых систем и установку загрузчика.
- По умолчанию устанавливается временный пароль root:changeme. После первого запуска образа пароль требуется **сменить немедленно**.
- Проверка подписей OSTree remote отключена (gpg-verify=false). Для эксплуатационных контуров рекомендуется включать верификацию и использовать доверенный ключ/защищённый транспорт.
- Разметка и установка GRUB ориентированы на **BIOS/Legacy** (раздел bios_grub). Для UEFI требуется отдельный профиль (ESP/FAT32, /boot/efi, установка GRUB под EFI).
- Параметр -m/--MOUNT_POINT не должен указывать на / и не должен пересекаться с критическими точками монтирования системы сборки.

2. Подготовка и сборка образа

2.1 Условия выполнения

- Операционная система: НАЙС.ОС (с доступом к tdnf).
- Права: выполнение от **root** (или через sudo).
- Доступность OSTree-репозитория: сетевой доступ к http://IP_ADDR.
- Свободное место: не менее FILE_SIZE ГБ под файл образа + запас на служебные операции.
- Комплект файлов: mk-ostree-host.sh и function.inc должны находиться в одном каталоге.

2.2 Подготовка каталога со скриптом

Перед запуском необходимо убедиться, что установлен пакет rpm-ostree-host.

2.3 Проверка исходных параметров и назначение

ключей

Для формирования образа необходимо определить значения параметров, приведённых ниже. Параметры передаются в скрипт в командной строке; все значения должны быть заданы явно.

2.3.1 Параметры запуска (обязательные)

- **-s / --FILE_SIZE** — размер образа (в гигабайтах), целое число > 0.
- **-n / --IMG_NAME** — имя образа без расширения. Итоговый файл будет <IMG_NAME>.raw.
- **-i / --IP_ADDR** — адрес сервера, публикующего OSTree-репозиторий по HTTP.
- **-r / --REPO_REF** — ref в OSTree-репозитории (пример: niceos/5.2/x86_64/base).
- **-m / --MOUNT_POINT** — временная точка монтирования sysroot при сборке (пример: /mnt/niceos-root).

2.3.2 Параметр согласования с целевой средой

- **--root-dev** — устройство, которое должно быть указано в параметре root= для загрузки после переноса образа. По умолчанию используется /dev/sda3. Для virtio обычно требуется /dev/vda3.

2.4 Проверка доступности OSTree-сервера

До запуска рекомендуется проверить сетевую связность с сервером репозитория. Проверка не подтверждает наличие конкретного рефа, но позволяет исключить ошибки маршрутизации и блокировки по сети.

```
# минимальная проверка доступности по HTTP
curl -I "http://10.0.0.10/" || true
```

2.5 Запуск сборки образа

Запуск выполняется одной командой. Скрипт самостоятельно установит необходимые служебные пакеты (через tdnf), создаст образ, разметит его, выполнит deploy OSTree и подготовит загрузку.

```
sudo ./mk-ostree-host.sh \
 -s 20 \
```

```
-n niceos-5.2-base \
-i 10.0.0.10 \
-r niceos/5.2/x86_64/base \
-m /mnt/niceos-root \
--root-dev /dev/sda3
```

2.6 Контроль хода выполнения и логирование

При выполнении скрипт пишет подробный лог в файл вида: /var/log/mk-ostree-host.sh-YYYY-MM-DD.log. Рекомендуется проверять лог при любом отклонении от ожидаемого хода выполнения (ошибка, аварийная остановка, нестандартная длительность операций).

```
# просмотр последних строк лога
sudo tail -n 200 "/var/log/mk-ostree-host.sh-$(date +%Y-%m-%d).log"
```

2.7 Ожидаемые действия скрипта (для понимания процесса)

В ходе выполнения последовательно выполняются операции: создание sparse RAW, подключение loop, разметка GPT, создание mapper-устройств для разделов, форматирование ext4, монтирование sysroot и /boot, ostree init, добавление remote, ostree pull, ostree admin deploy, подготовка окружения chroot, установка GRUB2, корректировка root= и запись fstab, затем размонтирование и снятие loop/mapper.

2.8 Требования к корректному запуску (типовые ошибки)

- **--FILE_SIZE** должен быть целым числом > 0; значение вида 20.5 не допускается.
- **--MOUNT_POINT** не должен быть равен / и не должен указывать на используемые системой каталоги (рекомендуется отдельный путь вида /mnt/niceos-root).
- При использовании virtio-диска в целевой ВМ следует задавать **--root-dev /dev/vda3**; при SATA/SCSI — чаще **--root-dev /dev/sda3**.
- При отсутствии function.inc скрипт завершится немедленно. Файл должен располагаться рядом со скриптом.
- При сетевой недоступности IP_ADDR или при неверном REPO_REF операция ostree pull завершится ошибкой. В этом случае первично анализируется лог.

3. Использование образа и контроль результата

3.1 Назначение этапа

Настоящий раздел устанавливает порядок использования полученного файла <IMG_NAME>.raw после завершения работы mk-ostree-host.sh: импорт в целевую среду (виртуализация/стенд), выполнение первичных действий после первого запуска и контроль того, что deploy OSTree и загрузка настроены корректно.

3.2 Проверка артефакта на сборочной машине (до импорта)

Перед переносом/импортом образа рекомендуется выполнить базовые проверки: наличие файла, его размер, права доступа, а также убедиться, что в ходе сборки не осталось подключенных loop/devicemapper устройств (это косвенно подтверждает корректную работу процедуры очистки).

```
# 1) проверить наличие и размер файла
ls -lh ./niceos-5.2-base.raw

# 2) убедиться, что loop-устройства не "висят" от прошлой сборки
losetup -a || true

# 3) убедиться, что mapper-устройства не остались (примерный просмотр)
ls /dev/mapper/ | head -n 20
```

3.2.1 Признаки корректно подготовленного образа

- Файл *.raw присутствует и соответствует заданному FILE_SIZE.
- Скрипт завершился сообщением об успешном завершении.
- В логе отсутствуют ошибки на шагах: ostree pull, ostree admin deploy, grub2-install.
- Отсутствуют “подвисшие” mountpoint’ы и loop/mapper устройства, связанные со сборкой.

3.3 Импорт и запуск в целевой среде

Образ RAW может использоваться напрямую или предварительно конвертироваться

в формат, предпочтительный для вашей платформы виртуализации. На практике для KVM/QEMU чаще применяют конвертацию в qcow2; для других платформ — конвертацию в vmdk/vdi штатными инструментами.

3.3.1 KVM/QEMU: рекомендуемая конвертация и тестовый запуск

При использовании KVM/QEMU рекомендуется конвертировать образ в qcow2 для поддержки снапшотов, тонкого выделения места и ускорения некоторых операций.

```
# конвертация RAW -> qcow2
qemu-img convert -f raw -O qcow2 niceos-5.2-base.raw niceos-5.2-base.qcow2

# тестовый запуск (пример, BIOS/Legacy)
# ВАЖНО: тип интерфейса диска влияет на имя устройства в системе (sda vs vda)
qemu-system-x86_64 \
 -m 2048 -smp 2 \
 -drive file=niceos-5.2-base.qcow2,if=virtio,format=qcow2 \
 -net nic -net user \
 -serial mon:stdio
```

3.3.2 Критическое соответствие --root-dev и типа диска в ВМ

Наиболее частая причина неуспешной загрузки — несоответствие параметра root= ожидаемому устройству корневого раздела. Если при импорте/запуске образа вы меняете тип дискового интерфейса, вы меняете и имя устройства в гостевой ОС:

- virtio-диск: как правило /dev/vda, корень /dev/vda3;
- SATA/SCSI: как правило /dev/sda, корень /dev/sda3.

Следовательно, образ следует собирать под целевую конфигурацию ВМ заранее (через корректный --root-dev), либо быть готовым к правке загрузочных записей/параметров в аварийном режиме.

3.3.3 VMware/VirtualBox и иные платформы (общие требования)

Для платформ, где RAW не используется напрямую, необходимо выполнить конвертацию в поддерживаемый формат и импортировать образ как существующий диск. Поскольку разметка и установка GRUB ориентированы на BIOS/Legacy, в

настройках ВМ следует использовать режим загрузки **BIOS/Legacy**. При выборе UEFI загрузка не гарантируется без переработки схемы (см. предупреждение ниже).

3.3.4 Ограничение по UEFI

Образ, подготовленный текущим скриптом, создаёт раздел bios_grub и устанавливает GRUB2 для BIOS/Legacy. Для UEFI требуется ESP-раздел (FAT32, GPT type ef00), монтирование в /boot/efi и установка GRUB2 под EFI. При необходимости использования UEFI следует применять отдельный профиль сборки.

3.4 Действия при первом запуске системы

После первой загрузки целевой системы необходимо выполнить первичные действия: сменить временный пароль, убедиться в корректности deploy OSTree, проверить монтирование разделов и параметры загрузки.

```
# 1) немедленно сменить временный пароль root
passwd

# 2) проверить, какой деплой активен
ostree admin status

# 3) проверить смонтированные разделы / и /boot
mount | egrep ' on / | on /boot '

# 4) проверить fstab
cat /etc/fstab
```

3.4.1 Контрольный перечень (после первого старта)

- Пароль root изменён (исключена возможность входа по root:changeme).
- Команда ostree admin status отображает активный deploy (без ошибок чтения sysroot).
- Разделы / и /boot смонтированы и соответствуют ожидаемым устройствам.
- Файл /etc/fstab содержит строки для / и /boot и соответствует вашей платформе (SATA/SCSI vs virtio).
- Загрузочные записи присутствуют в /boot/loader/entries/; при необходимости доступен /boot/loader/grub.cfg и симлинк в /boot/grub2/grub.cfg.

3.5 Типовые неисправности при загрузке и порядок действий

При возникновении отказов следует различать: (а) проблемы переноса/импорта образа, (б) несоответствие параметров загрузки (root=), (в) проблемы доступа к разделам (fstab/драйвер), (г) неполный/ошибочный deploy. Первичный источник информации — консоль загрузки (ошибка GRUB/kernel panic) и лог сборки на машине, где запускался скрипт.

3.5.1 Сценарий: “Kernel panic / cannot mount root”

Симптом: система доходит до загрузки ядра, после чего сообщает невозможность смонтировать корневой раздел. Наиболее вероятная причина — неверное значение root= (ожидали /dev/sda3, а фактически корень стал /dev/vda3, либо наоборот).

Основной корректирующий метод — пересборка образа с правильным --root-dev. Временное решение (на стенде) — вручную поправить загрузочные записи в /boot/loader/entries/ и/или /boot/loader/grub.cfg, приведя root= к фактическому устройству.

3.6 Аварийная очистка на сборочной машине (при прерывании сборки)

Если сборка была прервана аварийно и автоматическая очистка не сняла loop/mapper устройства, необходимо выполнить ручную очистку. Порядок: размонтировать точки, удалить mapper-карты, затем снять loop-устройство. Команды ниже приведены как типовой пример; конкретные значения путей и устройств следует определить по выводу losetup -a.

```
# 1) определить loop-устройство, связанное с образом
losetup -a

# 2) размонтировать точки (пример)
umount -l /mnt/niceos-root/boot || true
umount -l /mnt/niceos-root || true

# 3) удалить mapper-карты (пример: если образ был на /dev/loop0)
kpartx -d /dev/loop0 || true

# 4) снять loop-устройство
```

```
losetup -d /dev/loop0 || true
```

3.7 Рекомендация по эксплуатационной практике

Для инфраструктурного использования целесообразно фиксировать: (а) используемый ref (REPO_REF), (б) целевую схему диска (virtio/SATA), (в) значение --root-dev, (г) режим загрузки (BIOS/UEFI), (д) требования к верификации (GPG/HTTPS). Это обеспечивает воспроизводимость и облегчает разбор инцидентов при миграциях между средами.