УДК 004.451.53

УПРАВЛЕНИЕ ПАРКОМ НЕИЗМЕНЯЕМЫХ СИСТЕМ В КОРПОРАТИВНОЙ И ПРОИЗВОДСТВЕННОЙ СРЕДЕ

В. А. ОВЧИННИКОВ
(Представлено: В. А. МАКАРЫЧЕВА)

В статье рассматривается решение главных задач современной ИТ-инфраструктуры: обеспечение стабильности, безопасности, единообразия рабочих станций с помощью неизменяемых операционных систем на базе libostree.

Введение. Современные корпоративные и образовательные ИТ-инфраструктуры сталкиваются с большим количеством проблем, связанных с управлением парками рабочих станций. Поддержание стабильности, обеспечение безопасности и соблюдение одинаковой конфигурации на сотнях или тысячах компьютеров требует большого количества человеческих ресурсов.

Особенно эти проблемы касаются образовательных учреждений, где компьютерными классами пользуется большое количество человек и необходимо гарантировать одинаковую среду для проведения занятий, а также в корпоративной среде, где простой одного рабочего места может остановить работу всей компании.

В статье будет изучено, как неизменяемая операционная система, контейнеризированная среда Toolbox и изолированные пользовательские приложения (на примере Flatpak) создают устойчивую, безопасную и легко управляемую экосистему, которая сильно снижает стоимость владения парком рабочих станций и повышает отказоустойчивость ИТ-инфраструктуры.

Основная часть. В традиционных Linux дистрибутивах, в которых пакеты динамически обновляются, например, через APT или DNF, неизбежно такое явление, как «дрейф конфигураций». Дрейф конфигураций – ситуация, когда в самом начале идентичные системы через некоторое время имеют различия из-за установки пользовательского программного обеспечения, обновлений или ручных изменений системных файлов [8]. Это приводит к непредсказуемому поведению, сложностям в диагностике проблем и уязвимостям в безопасности.

На предприятиях чаще всего очень важную роль играет старое, но проверенное программное обеспечение, которое требует для своей работы устаревшие версии системных библиотек. В традиционных дистрибутивах это приводит к конфликтам пакетов, что делает невозможным правильную работу специализированного программного обеспечения и остальной системы. Из-за этого на предприятиях часто используются старые операционные системы, что приводит к серьезным угрозам для безопасности всего предприятия.

Универсальным решением становятся неизменяемые операционные системы, построенные на технологии OSTree.

Libostree – альтернативная пакетным менеджерам система, которая обеспечивает поддержку параллельной установки и атомарного обновления операционных систем. OSTree формирует системный образ из Git-подобного хранилища. Такой подход позволяет применять методы версионного контроля к компонентам дистрибутивах [1].

Вместо пакетов и установочных образов OSTree манипулирует готовыми загрузочными деревьями файловой системы и может быть охарактеризован как "Git для бинарных файлов ОС". OSTree имеет многослойную архитектуру и изначально рассчитан на работу с различными наборами деревьев, развёртываемыми поверх базового административного слоя [5].

В результате администратор работает не с большим набором отдельных пакетов, а с эталонными образами, что гарантирует стопроцентную идентичность базовой системы на всех рабочих станциях парка.

Основой управления является золотой снимок. Золотой снимок – это эталонный снимок операционной системы, который включает в себя ядро, системные утилиты и предустановленное программное обеспечение. Этот образ развертывается на всех рабочих станциях заведения, что обеспечивает их стопроцентную идентичность на базовом уровне и последующее атомарное обновление всех узлов парка [8].

Каждый образ представляет собой отдельный коммит в репозитории OSTree, который идентифицируется хэш-суммой. Любое изменение, будь то обновление безопасности или установка нового пакета, приводит к созданию нового, верифицированного образа. Это исключает возможность «дрейфа конфигураций» и неожиданного сбоя системы, после обновления критических пакетов.

Процесс обновления является атомарным. Новый образ системы загружается и проверяется в фоновом режиме, а активируется только при следующей перезагрузке, путем переключения на новую корневую файловую систему. Если новый образ по какой-либо причине не запускается (например, из-за по-

врежденного драйвера), загрузчик автоматически предлагает вернуться к предыдущему, работоспособному состоянию. Это сводит простой рабочих мест к минимуму и полностью исключает возможность получения системы в нерабочем состоянии после обновления системы.

Архитектура неизменяемых систем предлагает четкое разделение ответственности, что упрощает управление и повышает безопасность. Система делится на три независимых слоя, которые управляются по отдельности:

1. Неизменяемая базовая операционная система
2. Пользовательские приложения
3. Среды разработки и администрирования

Неизменяемая базовая ОС – это и есть тот самый «золотой образ», которым администратор управляет через rpm-ostree. Он содержит в себе только базовые компоненты, необходимые для функционирования операционной системы.

Для пользовательских приложений предлагается использовать систему универсальных пакетов Flatpak. Приложения устанавливаются в изолированные среды (sandbox) и не имеют возможности влиять на базовую ОС. Администратор может централизованно управлять корпоративным репозиторием Flatpak, утверждая и распространяя только необходимые версии программ. Это решает проблему конфликта зависимостей, так как разные приложения используют свои собственные, изолированные версии библиотек.

Для задач, требующих гибкости (установка компиляторов, отладочных инструментов, специфического CLI программного обеспечения), используются контейнеризированные среды. Они предоставляют пользователям полную свободу действий в изолированном пространстве, не ставя под угрозу целостность основной операционной системы. Данный подход идеален для ИТ-отделов и учебных классов, где требуется быстрая подготовка различных сред для разных проектов или дисциплин.

Данная архитектура кардинально упрощает такие рутинные, но критически важные операции, как массовое развертывание и восстановление после сбоев.

Новая рабочая станция подготавливается не последовательной установкой сотен пакетов, а развертыванием готового образа.

В случае критического сбоя, вызванного, например, экспериментами пользователя или повреждением данных, систему можно мгновенно вернуть в рабочее состояние. Команда rpm-ostree rollback выполняет откат к предыдущему системному образу, а сброс пользовательского пространства через rpm-ostree reset позволяет очистить изменяемые разделы до эталонного состояния, заданного администратором.

Для создания «золотых образов» используется утилита rpm-ostree. Команда rpm-ostree compose tree позволяет администраторам описывать конфигурацию базовой системы в виде декларативного манифеста (часто в формате YAML или JSON) [3]. В манифесте указываются: базовый дистрибутив, список предустановленных пакетов, настройки по умолчанию для загрузчика.

Для полного контроля и безопасности эталонные образы должны храниться на внутреннем сервере. Стандартная утилита ostree serve позволяет легко поднять такой репозиторий. Это дает администраторам возможность выкладывать новые образы в канал «staging» для проверки на контрольной группе устройств перед массовым развертыванием, поддерживать разные версии образов для разных филиалов или проектов, обеспечивать обновления в изолированных средах без доступа к интернету.

Развертывание собственного репозитория Flatpak, наподобие Flathub, например, с помощью flatpak-repo-build позволяет собирать, подписывать и распространять только проверенные версии программного обеспечения в корпоративной среде.

Заключение. Неизменяемые операционные системы – это не просто технологический эксперимент, а важный этап в эволюции ИТ-инфраструктур. Они являются эффективным решением основных проблем администрирования: обеспечение стабильности, безопасности и единообразия на большом парке развернутых систем. Администратор получает возможность работать не с последствиями бесконечных изменений в динамической системе, а с неизменяемой операционной системой. Атомарность обновлений и мгновенный откат сводят к минимуму простои, а принцип разделения ответственности между неизменяемой базой ОС, изолированными приложениями и контейнеризированными средами создает устойчивую и безопасную архитектуру.

ЛИТЕРАТУРА

1. OSTree [Электронный ресурс] // Wikipedia. – Режим доступа: https://en.wikipedia.org/wiki/OSTree. – Дата доступа: 17.04.2025.
2. OSTree – атомарные обновления ОС в стиле git [Электронный ресурс] // Habr. – Режим доступа: https://habr.com/ru/companies/flant/articles/522234/. – Дата доступа: 17.04.2025.

3. Fedora Kinoite User Guide [Электронный ресурс] // Fedora Project. – Режим доступа: https://docs.fedoraproject.org/en-US/fedora-kinoite/. – Дата доступа: 18.04.2025.
4. Fedora Kinoite User Guide. Getting Started [Электронный ресурс] // Fedora Project. – Режим доступа: https://docs.fedoraproject.org/en-US/fedora-kinoite/getting-started/. – Дата доступа: 18.04.2025.
5. OSTree Documentation [Электронный ресурс] // OSTree Project. – Режим доступа: https://ostreedev.github.io/ostree/. – Дата доступа: 18.04.2025.
6. Managing containerized applications with Flatpak [Электронный ресурс] // Red Hat Customer Portal. – Режим доступа: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/managing_containerized_applications_with_flatpak/index. – Дата доступа: 18.04.2025.
7. Silverblue: The Future of Desktop? [Электронный ресурс] // Fedora Magazine. – Режим доступа: https://fedoramagazine.org/silverblue-the-future-of-desktop/. – Дата доступа: 18.04.2025.
8. What is an immutable OS? [Электронный ресурс] // Ubuntu Blog. – Режим доступа: https://ubuntu.com/blog/what-is-an-immutable-os. – Дата доступа: 18.04.2025.
9. Toolbox: Introduction and Use Cases [Электронный ресурс] // Fedora Magazine. – Режим доступа: https://fedoramagazine.org/toolbox-introduction-and-use-cases/. – Дата доступа: 18.04.2025.