

Virtuozzo

Шаблоны контейнеров

Денис Силаков, ст. системный архитектор

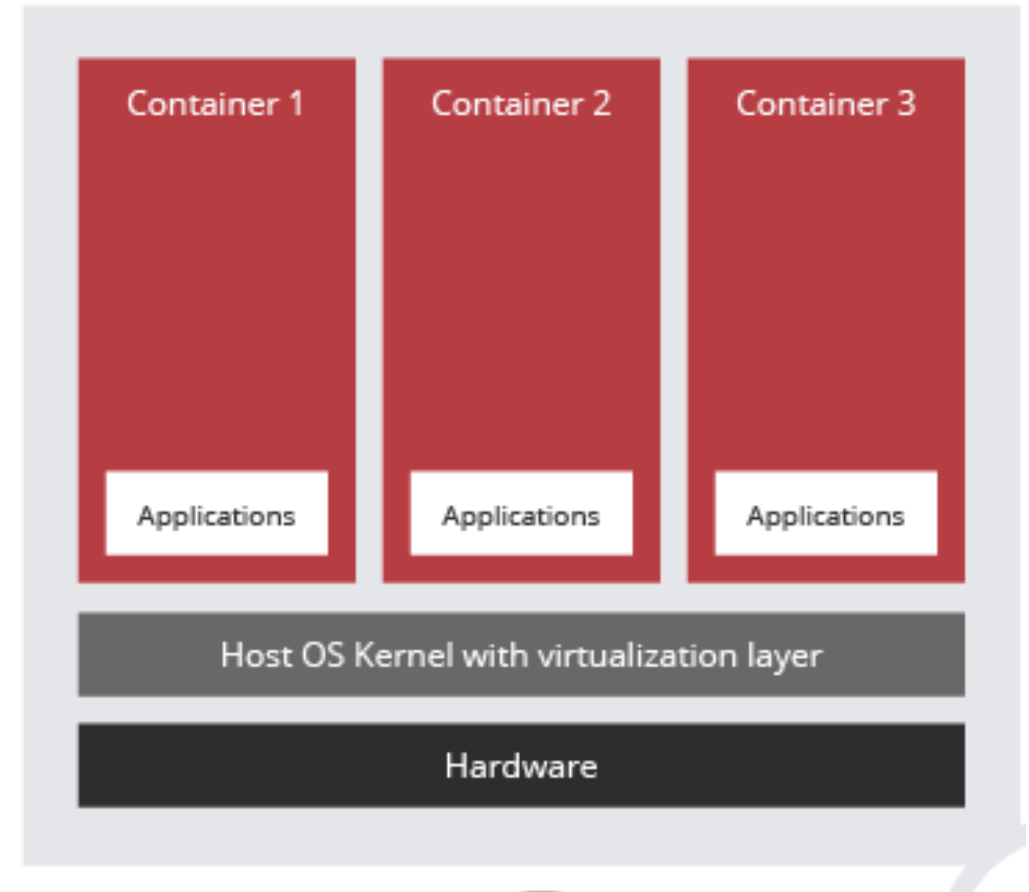
dsilakov@virtuozzo.com



Терминология

- Контейнер – «легковесное» виртуальное окружение
- Внутри гостей –
 - ядро основной ОС

System Containers



Технологии

- Solaris Zones
- FreeBSD Jails
- **Linux:**
 - LXC
 - Virtuozzo/OpenVZ
 - Docker (контейнеры «с наполнением»)

Пустой контейнер – плохой контейнер

Пользователям нужно **наполнение**:

- Операционная система
- Заданный набор приложений

Доставка контента в контейнер

- Использование заранее созданных VM
 - Просто и популярно (Docker)
 - Требуется поддержки
(“30% of Official Images in Docker Hub Contain High Priority Security Vulnerabilities” – BanyanOps, 2015)
- Автоматическая установка ОС/приложений после создания контейнера

Автоматическая установка ОС

- «Родные» программы установки ОС
 - Специфичны для каждого дистрибутива Linux
 - Требуют предварительной конфигурации
 - Ограниченные возможности автоматической установки
- Использование средств хост-системы
 - LXC с ALT Linux можно развернуть только в ALT Linux
- Инструменты установки одной ОС внутри другой
 - Debootstrap, supermin, rosa-bootstrap – ограничены по функционалу

Средства управления конфигурацией

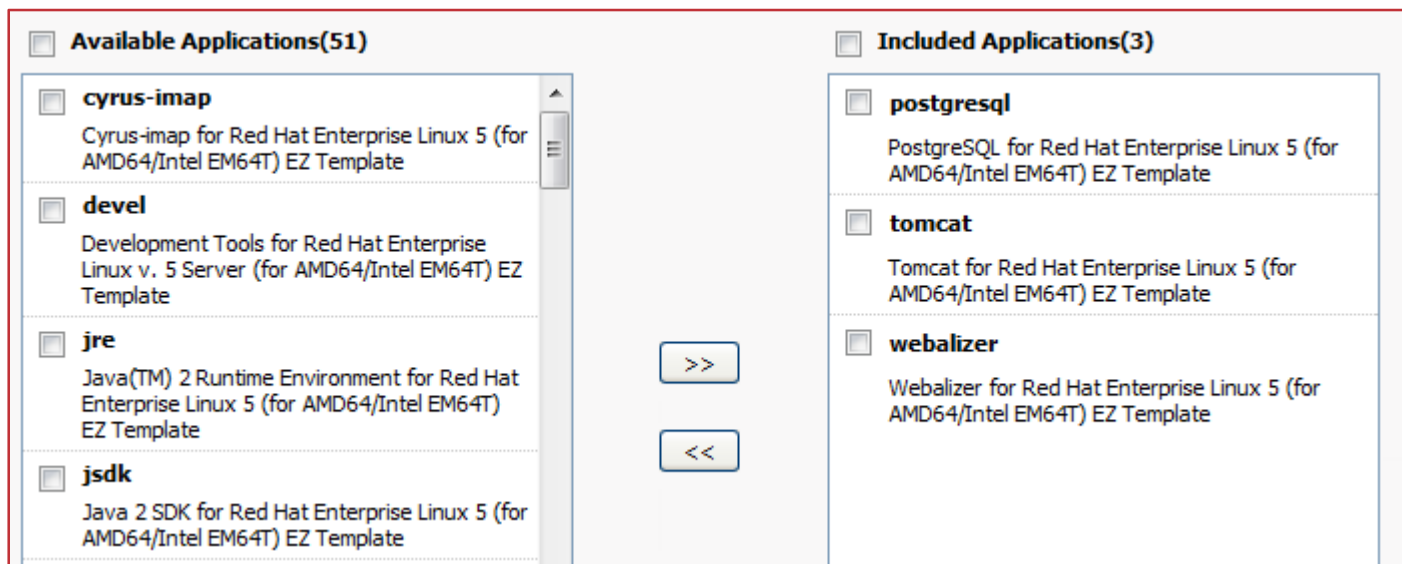
- Ansible, chef, puppet
- ... в совокупности с Vagrant ...

Работает, но требует отдельной настройки

Жизнь после установки

Мало установить систему, ее надо поддерживать

- Устанавливать обновления
- Устанавливать/удалять заданные приложения



Инструменты поддержки

- Docker – манипулирование «слоями» контейнеров
 - Недостаточно гибко
- Системы управления конфигурациями
 - Требуют настройки
 - Многие действия производят изнутри контейнеров
 - ⇒ нужен доступ в интернет, права администратора, специальный агент и т.п.

Шаблоны контейнеров Virtuozzo

- Установка ОС в контейнере «с нуля»
- Установка/удаление/обновление наборов программ
- Унифицированный интерфейс для всех дистрибутивов Linux
- Нет необходимости в модификациях внутри контейнеров (не нужно агентов, ssh-доступа, ...)

Дистрибутив Linux

== набор пакетов:

- Архив с файлами программ
- Скрипты

Менеджер пакетов:

- Распаковка архивов
- Выполнение скриптов из пакетов
- Выполнение системных триггеров



Управление пакетами

Установка ОС или набора программ == установка нужных пакетов в нужном порядке

Простой распаковки недостаточно:

- Скрипты и триггеры
- Зависимости между пакетами
 - Скрипт из пакета А требует утилиту из пакета В
- Нюансы, о которых знают только менеджеры пакетов конкретного дистрибутива

Virtuozzo vzpkg*

Модифицированные версии менеджеров пакетов для разных дистрибутивов Linux

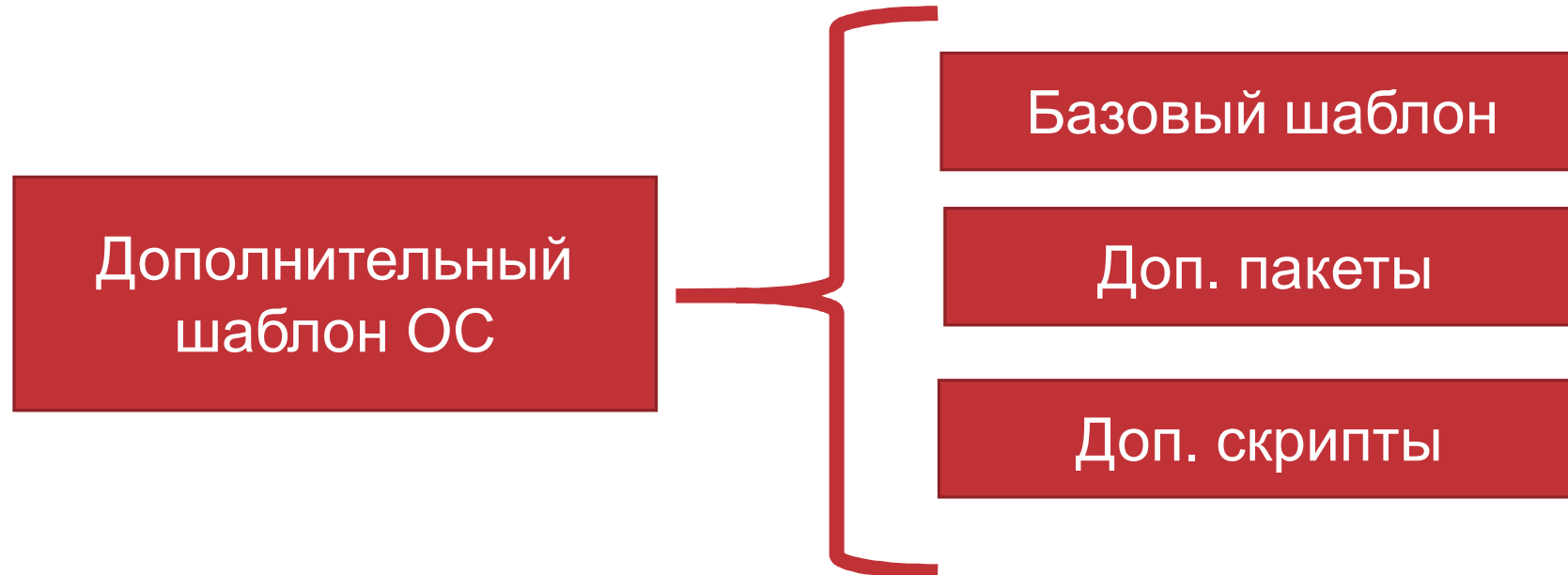
- Заточены на развертывание ОС «с нуля» и ее последующее обслуживание извне контейнера
- Способны взаимодействовать с инструментами управления контейнерами

Виды шаблонов

- Шаблон ОС
 - Базовый
 - Дополнительные вариации
CentOS Minimal, CentOS WebServer, ...
- Шаблоны приложений
 - PHP, Apache, MySQL, ...

Шаблон ОС

- Списки пакетов, замкнутые по зависимостям
- Скрипты, выполняемые программами установки ОС
 - Настройка сети, часового пояса, ...



Установка ОС

== подготовка образа диска с установленной ОС

- Распаковка минимального окружения с модифицированным менеджером пакетов
- Скачивание и распаковка пакетов ОС
- Выполнение скриптов из пакетов
- Выполнение скриптов установки ОС

Шаблоны приложений

- Предназначены для установки поверх конкретного шаблона ОС
 - Centos-7-x86_64-php
- Содержат список пакетов для установки и дополнительные скрипты

Работа с шаблонами

Утилита командной строки **vzpkg**

- Создание и обновление **кэша** шаблонов
 - Во избежание повторной распаковки набора пакетов
- **Установка/удаление** шаблонов приложений в контейнерах
- **Обновление** пакетов, относящихся к шаблону

Challenges

- Поддержка разных пакетных менеджеров
 - Различные кодовые базы (yum, zypper, dpkg/apt)
 - Различные условия сборки
 - Обновления при обновлении ОС
- Скрипты установки ОС

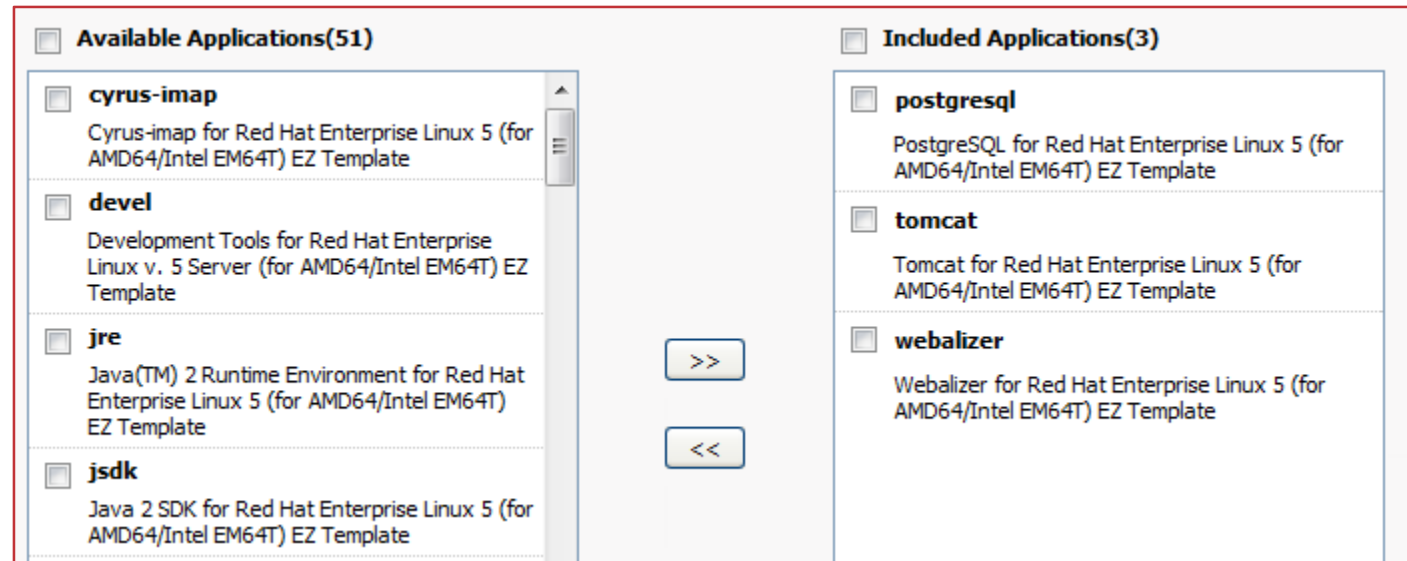
Изменения в пакетных менеджерах

- Установка пакетов в заданный контейнер
- Работа с идентификаторами пользователей/групп
- Обработка зависимостей
- ...
- Работа с VZFS
 - «Слияние» одинаковых файлов из разных контейнеров
 - Больше не нужна (в Virtuozzo 7 заменена на rfcache)

Размер: 1-3KLoC (50% - поддержка VZFS)

Использование

- Командная строка
 - Шаблон – параметр при создании контейнера
 - Vzpkg – «пакетный менеджер» для шаблонов
- GUI – Virtuozzo Automator



Командная строка

```
# prlctl create c1 --ostemplate ubuntu-16.04-x86_64 --vmtype=ct
# vzpkg install c1 php
# vzpkg update c1 ubuntu-16.04-x86_64
# vzpkg remove c1 php
```

Настройки vzpkg

- Списки пакетов, скрипты – в текстовом виде
- Репозитории-источники пакетов
- Ключи для доступа к закрытым репозиториям по подписке

Ресурсы

- Шаблоны Virtuozzo

<https://src.openvz.org/projects/OVZT>

- Инструментарий управления шаблонами

<https://src.openvz.org/projects/OVZ/repos/vztt>