



ASTERCONF
- 2019

DOCKER КОНТЕЙНЕРЫ ДЛЯ ASTERISK



О ЧЕМ ЭТОТ ДОКЛАД?

О запуске PBX в docker

- Краткий экскурс по docker
- PBX на Alpine Linux
- Плюсы-минусы



НЕМНОГО О СЕБЕ



Антон Захаров



anton@fibex.su



antonzakharov.ru



@c0rnoTa



cf.anton



github.com/c0rnoTa



Опыт

- с 2006 года работаю с платформой  Asterisk
- 12 лет опыта разработки сервисов для систем телефонии
 -    PHP, Perl, Go
- с 2015 года со-основатель компании **FIBEX** (<https://fibex.su>)

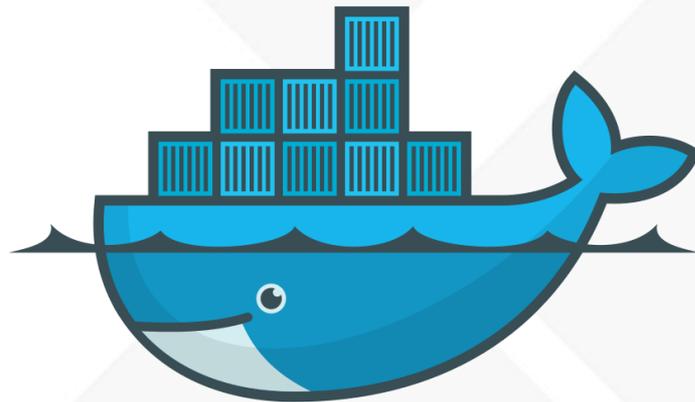
01

ПАРА СЛОВ О DOCKER

ПАРА СЛОВ О DOCKER

Docker technology review

- Виртуализация на уровне ОС Linux
- cgroups и namespaces
- runC (libcontainer)
- AuFS
- Networking
- Docker EE и Docker CE
- <https://docker-curriculum.com>



DOCKER vs VM

Виртуальная машина

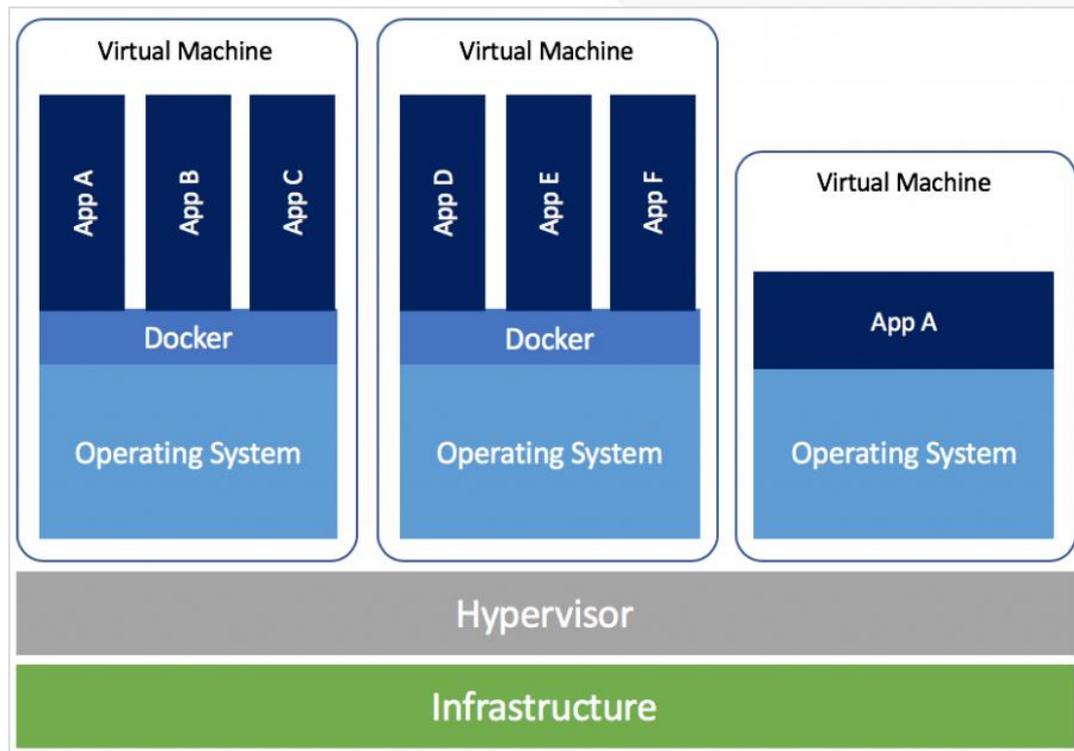
- Несколько экземпляров ПО на 1G HDD требуют 1G * количество экземпляров
- Более изолированная, но тяжелая (ресурсы на ОС)
- Несколько минут на запуск
- Разные окружения 🖱️ painful deploy

Vs

Docker

- Несколько экземпляров ПО на 1G HDD требуют 1G (шарит образ ПО)
- Менее изолированная, но очень лёгкая (сотни контейнеров на одном хосту)
- Меньше секунды на запуск
- Snapshot окружения 🖱️ easy deploy

DOCKER + VM



Источник: <https://blog.docker.com/2018/08/containers-replacing-virtual-machines/>

ПАРА СЛОВ О DOCKER

Принципы Docker

- Docker контейнер пакует приложение с файловой системой в единый образ со всем необходимым окружением для запуска этого приложения
- Основа Docker-контейнера – это образ (image). Можно скачать из репозитория или собрать свой на базе существующего
- Одно приложение - один контейнер
- Persistent data на volume, один volume может монтироваться в несколько контейнеров
- Overlay network для контейнеров, порты пробрасываются в хост
- Свой DNS для service discovery
- Интерактивный режим для работы в shell контейнера

ПАРА СЛОВ О DOCKER

Dockerfile

- Текстовый файл, который содержит команды по сборке контейнера
- Одна строка – один слой файловой системы
- Запуск приложения через ENTRYPOINT и CMD
- Компиляция, теги, вот это вот всё

```
Dockerfile x
1  FROM php:fpm-alpine
2
3  WORKDIR /var/www/html
4
5  RUN apk add \
6      sox \
7      lame
8
9  RUN apk add --no-cache --virtual .build-deps \
10     $PHPIZE_DEPS \
11     imagemagick-dev \
12     && pecl install imagick \
13     && docker-php-ext-enable imagick \
14     && apk del .build-deps
15
16  CMD ["php-fpm"]
```

ПАРА СЛОВ О DOCKER

Toolkit

- `docker-compose` – описание и запуск мультиконтейнерных приложений
- `Docker Swarm` – кластеризация хостов с Docker
- `stop` – утилита типа ``top`` для realtime метрик контейнеров
- `portainer` – web UI для docker-a

02

ПАКУЕМ РВХ В КОНТЕЙНЕРЫ

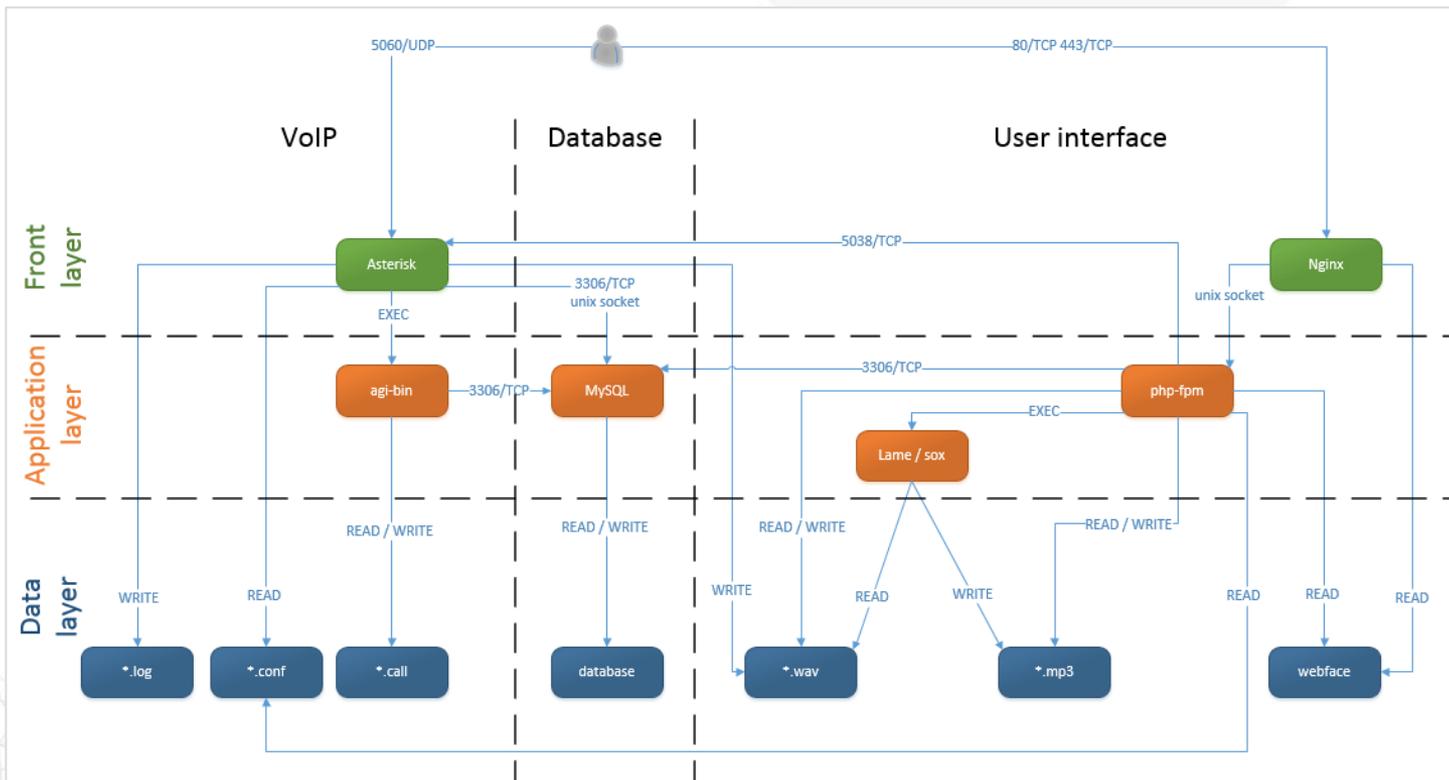
ПАКУЕМ PBX В КОНТЕЙНЕРЫ

Задачи на входе

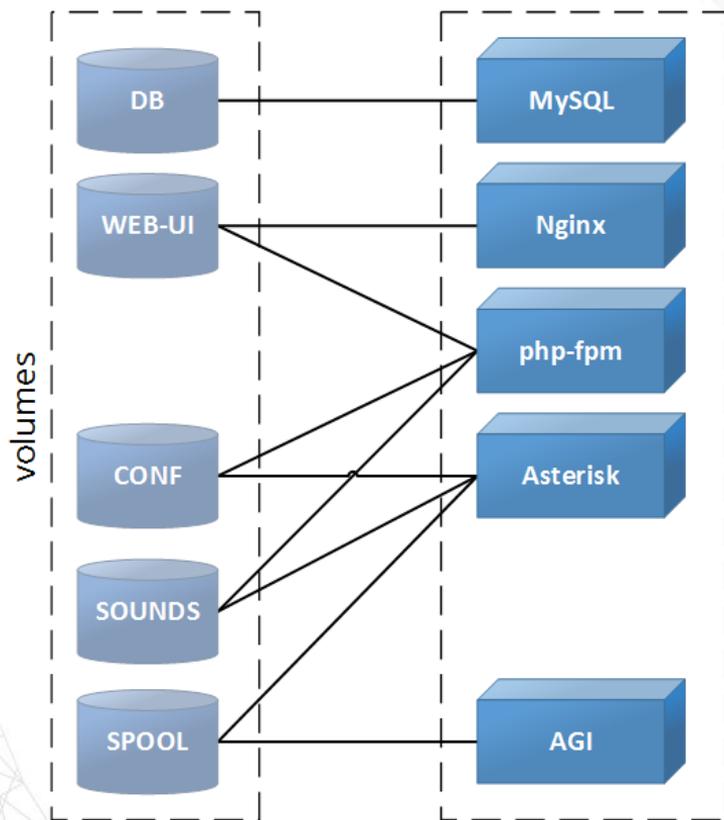
- Архитектура PBX
- Контейнер с Asterisk
- Networking
- Конфигурация



АРХИТЕКТУРА PBX AS-IS



АРХИТЕКТУРА PBX TO-BE



```
docker run -d mysql:5
```



```
docker run -d nginx:alpine
```



```
FROM php:fpm-alpine
RUN apk add \
    # lot's of packages here
CMD ["php-fpm"]
```



docker containers



```
FROM perl:5.20
COPY . /opt/fibex/fbxagi
WORKDIR /opt/fibex/fbxagi
RUN cpanm Module::Install Asterisk::FastAGI
EXPOSE 4573
CMD [ "perl", "./fbxagi.pl" ]
```

ПАКУЕМ РВХ В КОНТЕЙНЕРЫ

Asterisk build под Alpine Linux

- musl libc patches (thx to Timo Teräs)
musl-mutex-init.patch
musl-astmm-fix.patch
- Alpine MySQL ODBC driver (pre-build by c0rnoTa)
<https://github.com/c0rnoTa/mariadb-connector-odbc-alpine>
- Разделять runtime библиотеки от build dependencies
- Bundled PJSIP?

ПАКУЕМ РВХ В КОНТЕЙНЕРЫ

Конфигурационные файлы Asterisk

- Параметризация через переменные окружения
- dockerize – <https://github.com/jwilder/dockerize>

*.tmpl  *.conf

```
docker run -e SIP_UDP=5060 image:tag
```

```
docker-compose.yml x
1  version: "3.7"
2
3  >> services:
4
5  > asterisk:
6     environment:
7       - SIP_UDP_PORT=5060
8       - RTP_START=10000
9       - RTP_END=20000
```

ASTERISK NETWORKING



Требуется много портов для RTP трафика
Docker не пробрасывает диапазоны портов в контейнер

Host mode

- Прямой доступ к сетевой подсистеме
- Нет ограничений по портам
- Нет доступа в overlay network и service discovery

```
docker run --net=host image:tag
```

```
docker-compose.yml x
1  version: "3.7"
2
3  >> services:
4
5  > asterisk:
6     build: ./
7     network_mode: "host"
```

ASTERISK NETWORKING



Требуется много портов для RTP трафика
Docker не пробрасывает диапазоны портов в контейнер

Overlay mode

- Не забыть явно указать default-address-pools в /etc/docker/daemon.json
- Полный доступ к сетям docker и service discovery
- Проброс не более сотни портов

```
docker run -p 10000-10100:10000-10100/udp image:tag
```

ASTERISK NETWORKING



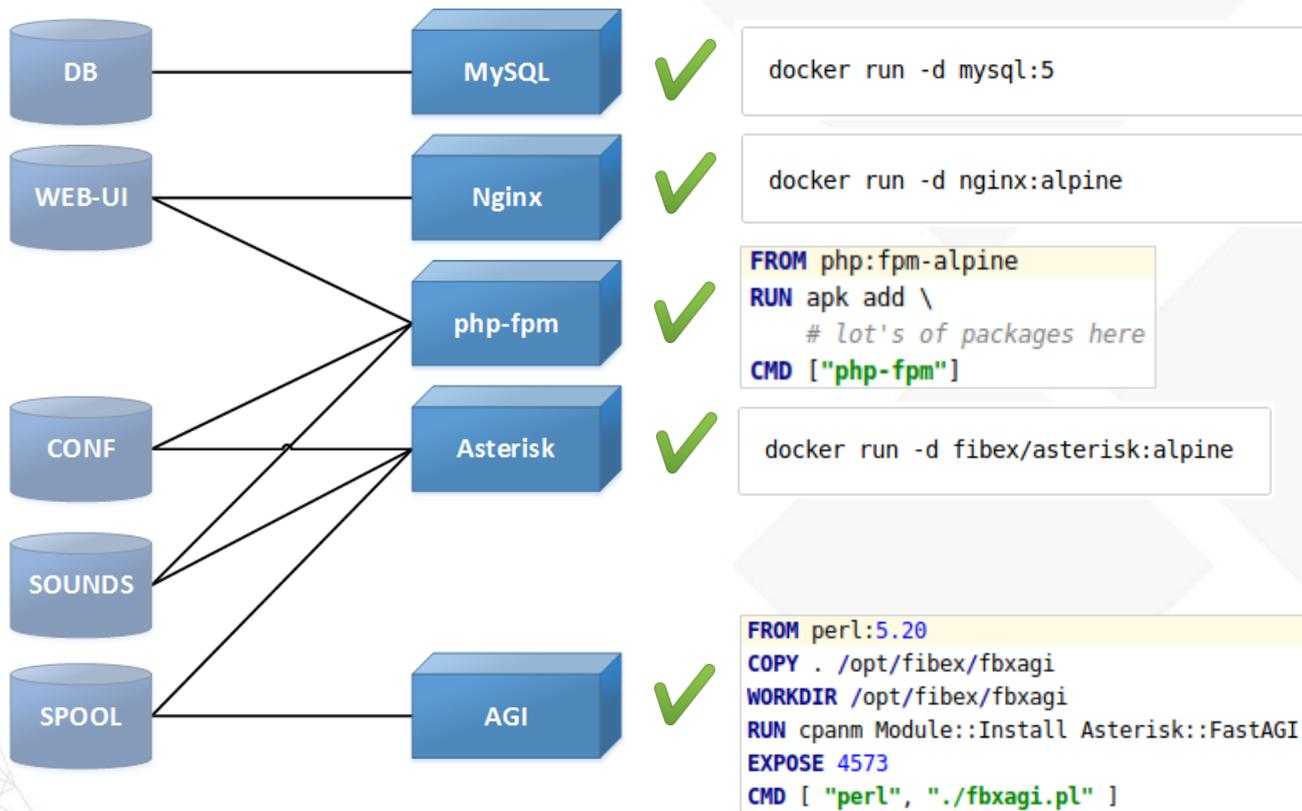
ЧИТ КОД (thx to Evan McGree)

<https://hub.docker.com/r/bettervoice/freeswitch-container>

```
CIP=$(docker inspect --format='{{.NetworkSettings.Networks.$NID.IPAddress}}' $CID)
sudo iptables -A DOCKER -t nat -p udp -m udp ! -i docker0 --dport 10000:20000 -j DNAT --to-destination $CIP:10000-20000
sudo iptables -A DOCKER -p udp -m udp -d $CIP/32 ! -i docker0 -o docker0 --dport 10000:20000 -j ACCEPT
sudo iptables -A POSTROUTING -t nat -p udp -m udp -s $CIP/32 -d $CIP/32 --dport 10000:20000 -j MASQUERADE
```

- \$CID – имя контейнера или его идентификатор
- \$NID – идентификатор используемой overlay сети
- Запускается на хосте после запуска контейнера
- Делает проброс большого диапазона портов одним правилом

PROFIT!



PROFIT?



Плюсы

- «Гибкий» стек
- Масштабируемость
- Fault isolation
- Дешевле



Минусы

- PJSIP
- NAT в overlay network
- Высокий порог входа?



ЧТО ДАЛЬШЕ?

- Выкат в prod
- Кластеры на Nomad + Consul
- Установка в инфраструктуры k8s (ЦОД)
- High-load с autoscale



ASTERCONF
- 2019

СПАСИБО ЗА ВНИМАНИЕ!

Антон Захаров

+7 (495) 748 55 88

anton@fibex.su

 t.me/c0rnoTa

