

Павел Воронов

pavel.voronov@arcadia.spb.ru

DevOps повсюду — От MSI к Docker

*Как поставить приложение на любое
окружение, или добавляем Docker жизни в
скучный enterprise*

План доклада

1. Как это было — «зонтики», бутстраперы и Windows Installer
2. Что такое Docker for Windows — Почему? Какие варианты?
3. Выбранный путь
 - Что потеряли и нашли
 - Работа и отладка, сборка и развертывание
4. Выводы и планы
5. Демонстрация наших инструментов



О себе

В Аркадии с 2006 года,
руководитель проекта,
Technical Product Owner

Более 12 лет в области
управления конфигурацией и
разработки ПО под Windows

Закончено несколько
успешных проектов
SWE 5d->1d, FIN 2w->2h



<https://www.linkedin.com/in/pavelvoronov/>

Для начала

1. Мир бесконечно сложен
2. Делаем сложные вещи — простыми
3. Всегда можно создать решение следующего уровня. Пункт 1.

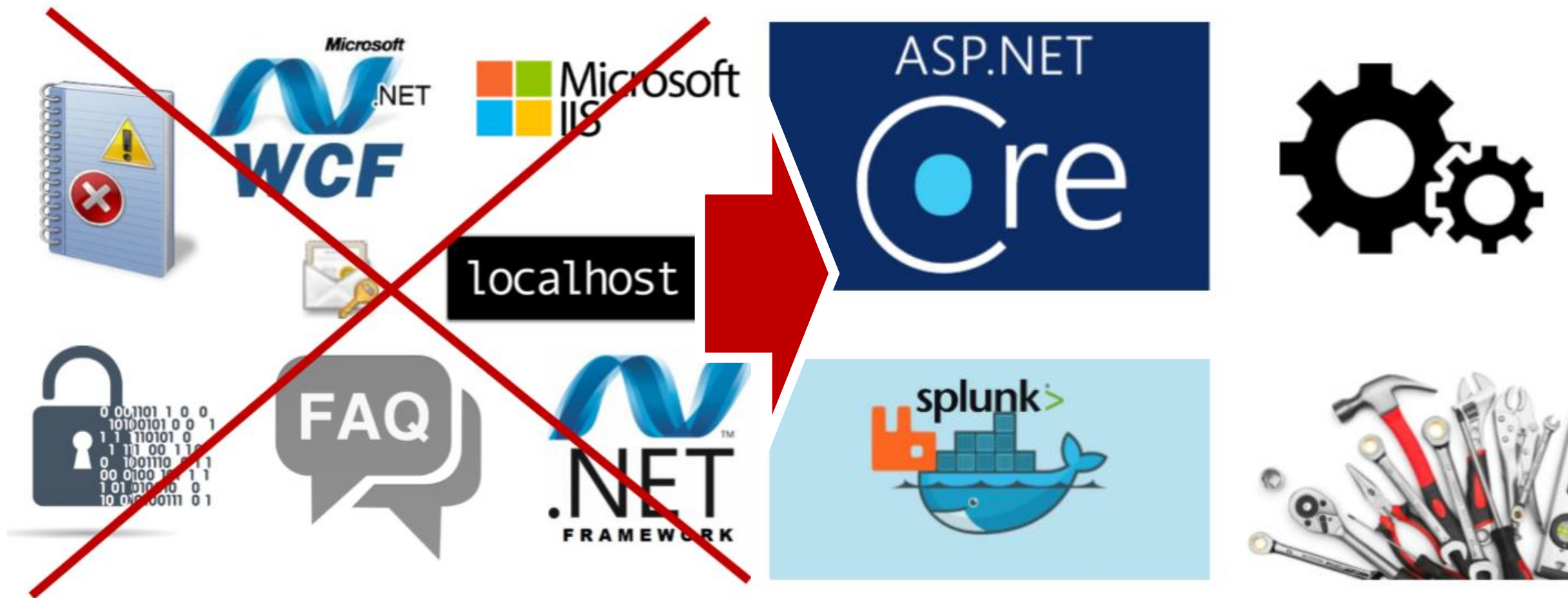
Client brief



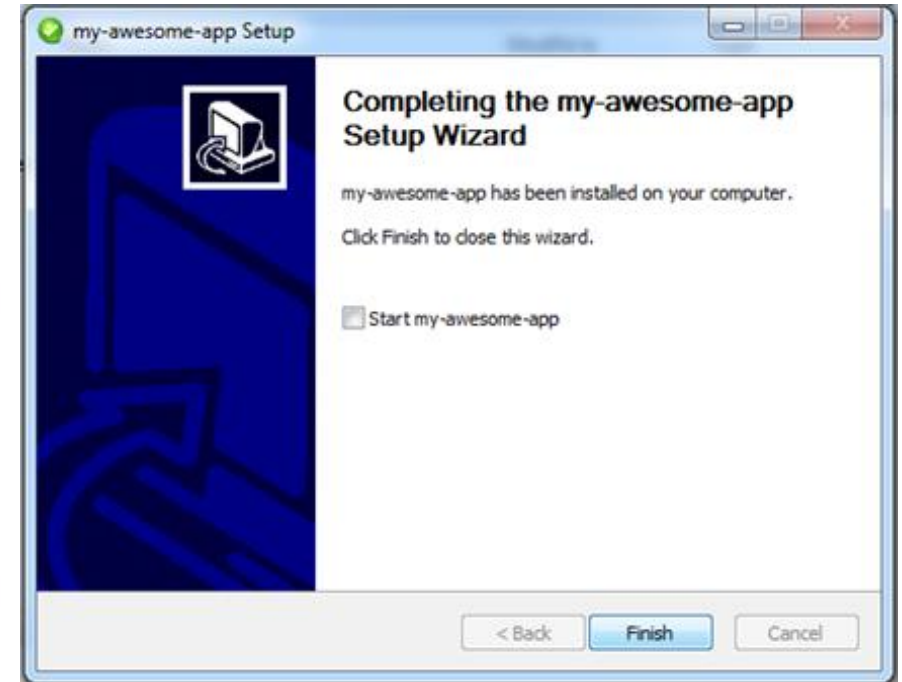
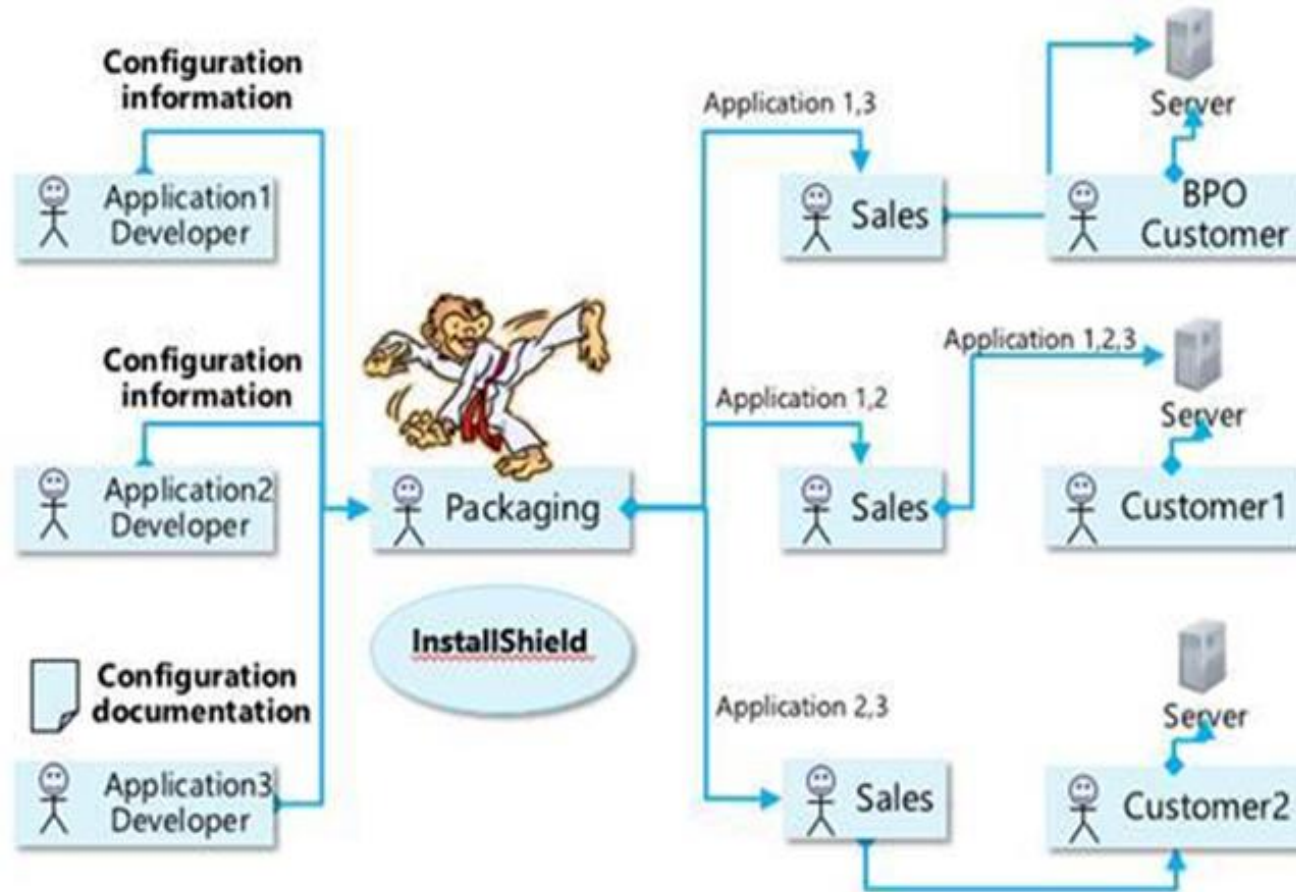
Client budget



У другой команды

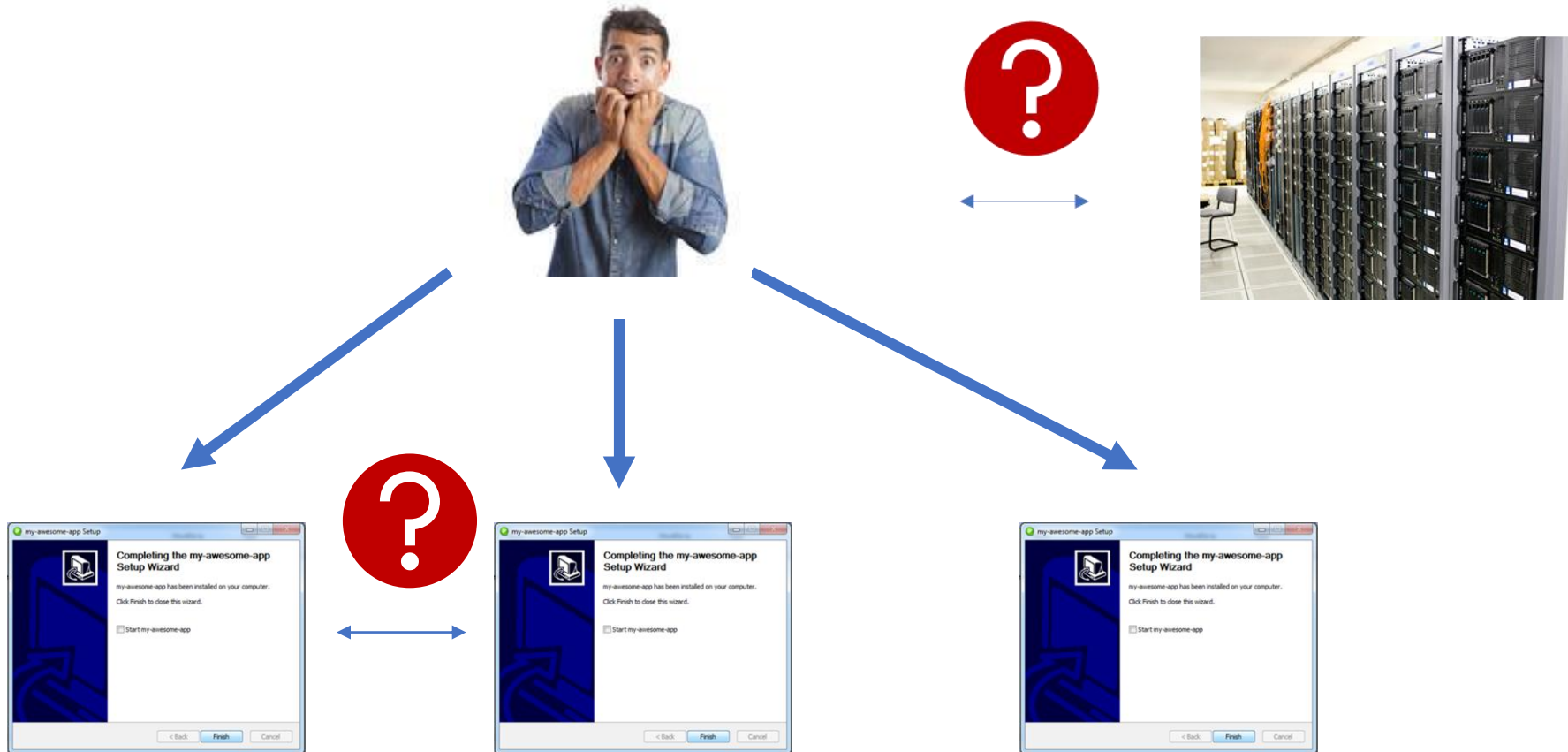


В начале был «хаос»...

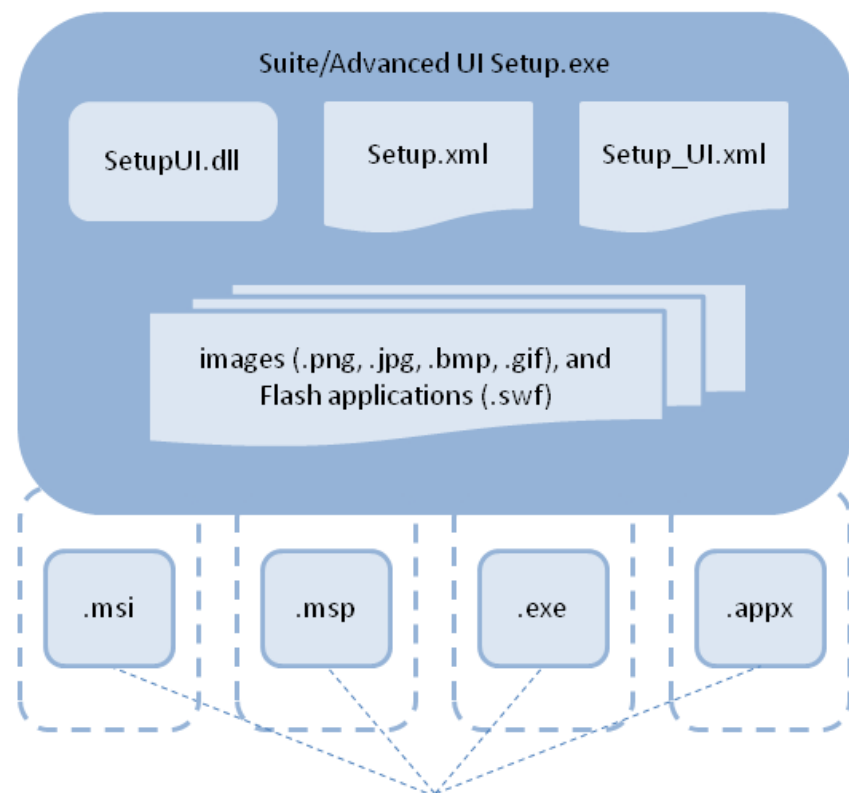


MSI, InstallScript, C++, VB Script

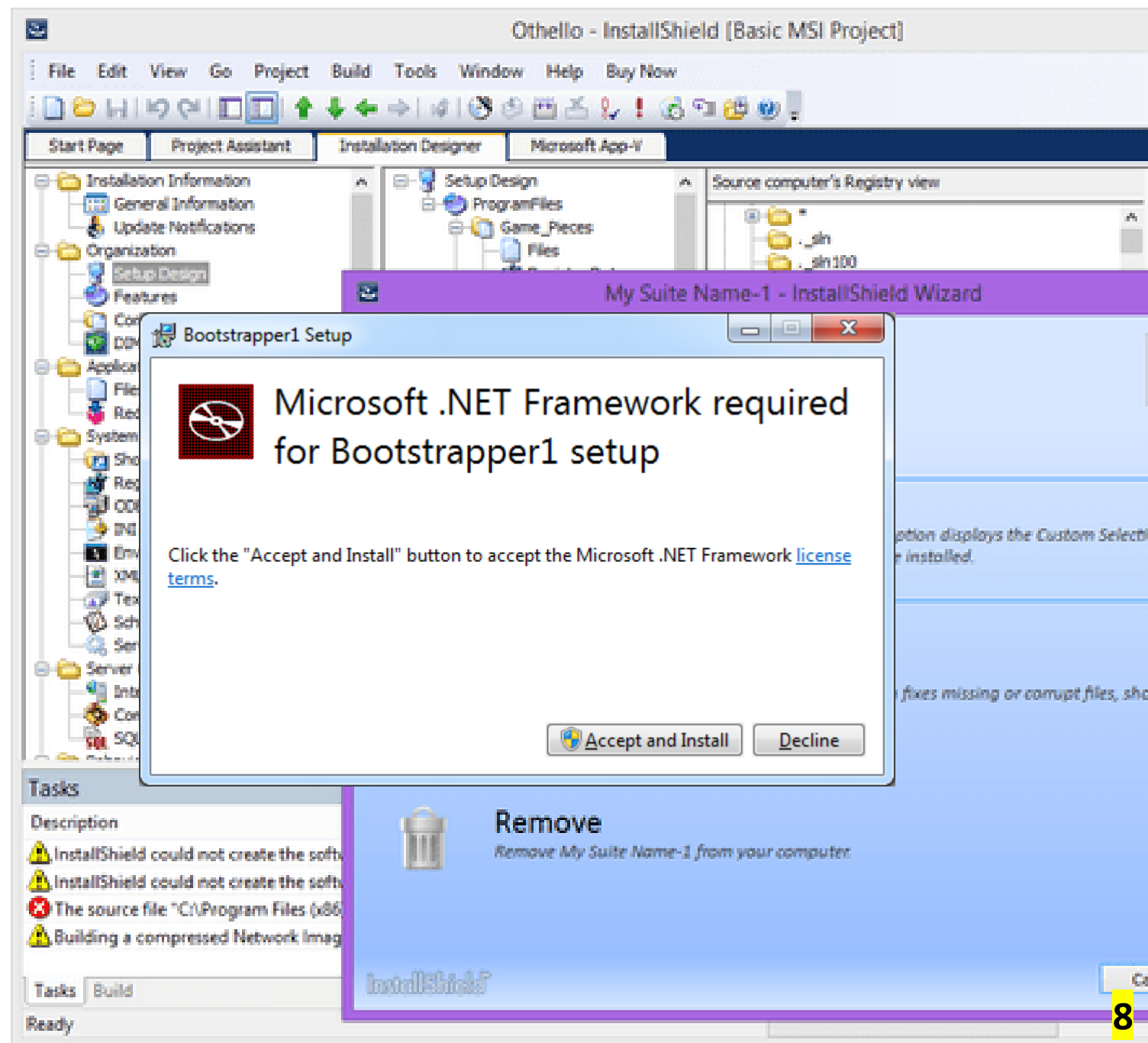
Если просто, то так



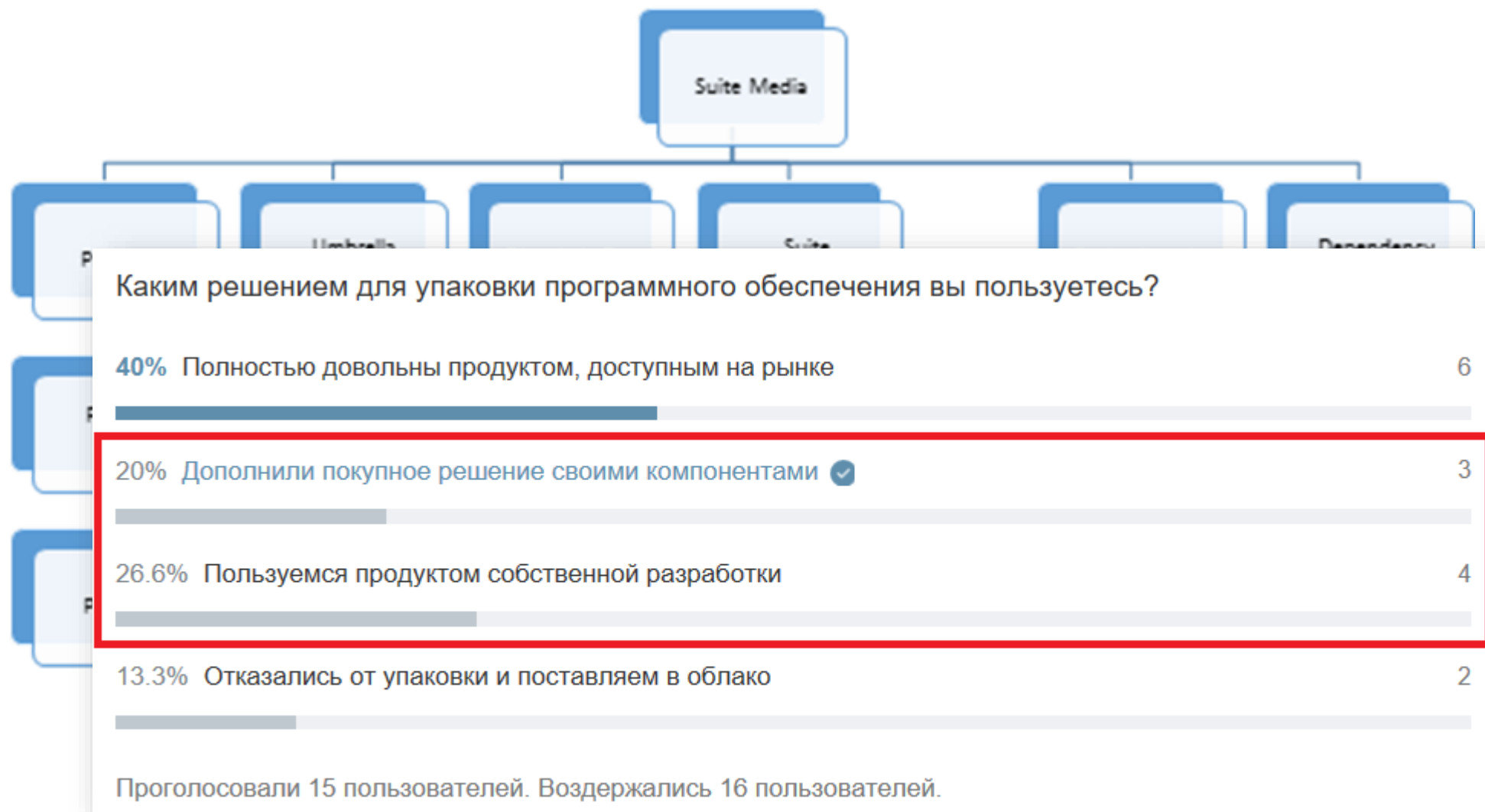
Бутстраперы...



Suite/Advanced UI packages and InstallShield prerequisite packages
(copied from source media, extracted from
Setup.exe, or downloaded from Web)



Что работает и зарабатывает сейчас



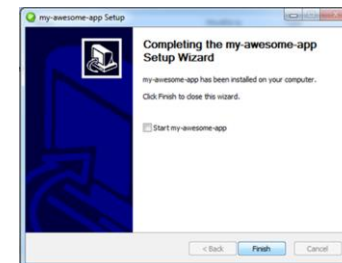
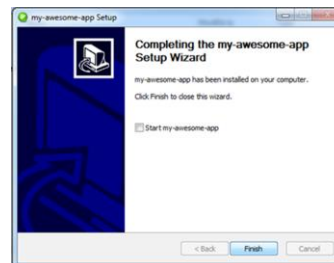
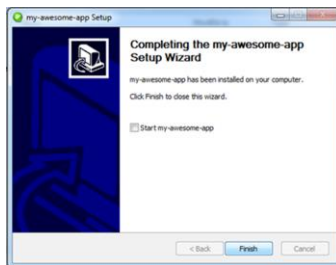
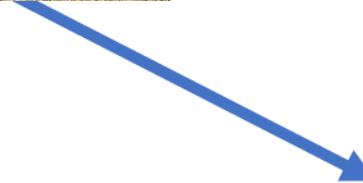
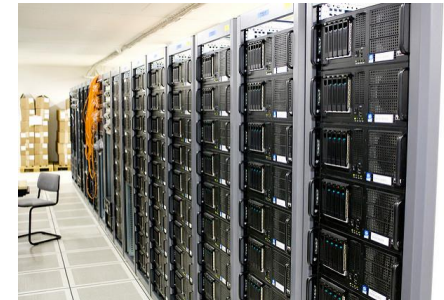
Стало так




[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)



A white car is parked in the foreground on the right side of the frame. The background is a long, narrow industrial tunnel with a high ceiling supported by metal beams. The floor is concrete with yellow lines. A bright light source is visible at the far end of the tunnel, creating a strong perspective. The text "Мир меняется: Я понял, что такое неэффективность..." is overlaid on a dark semi-transparent rectangle in the lower-left area.

Мир меняется: Я понял, что такое неэффективность...

Взгляд с другой стороны

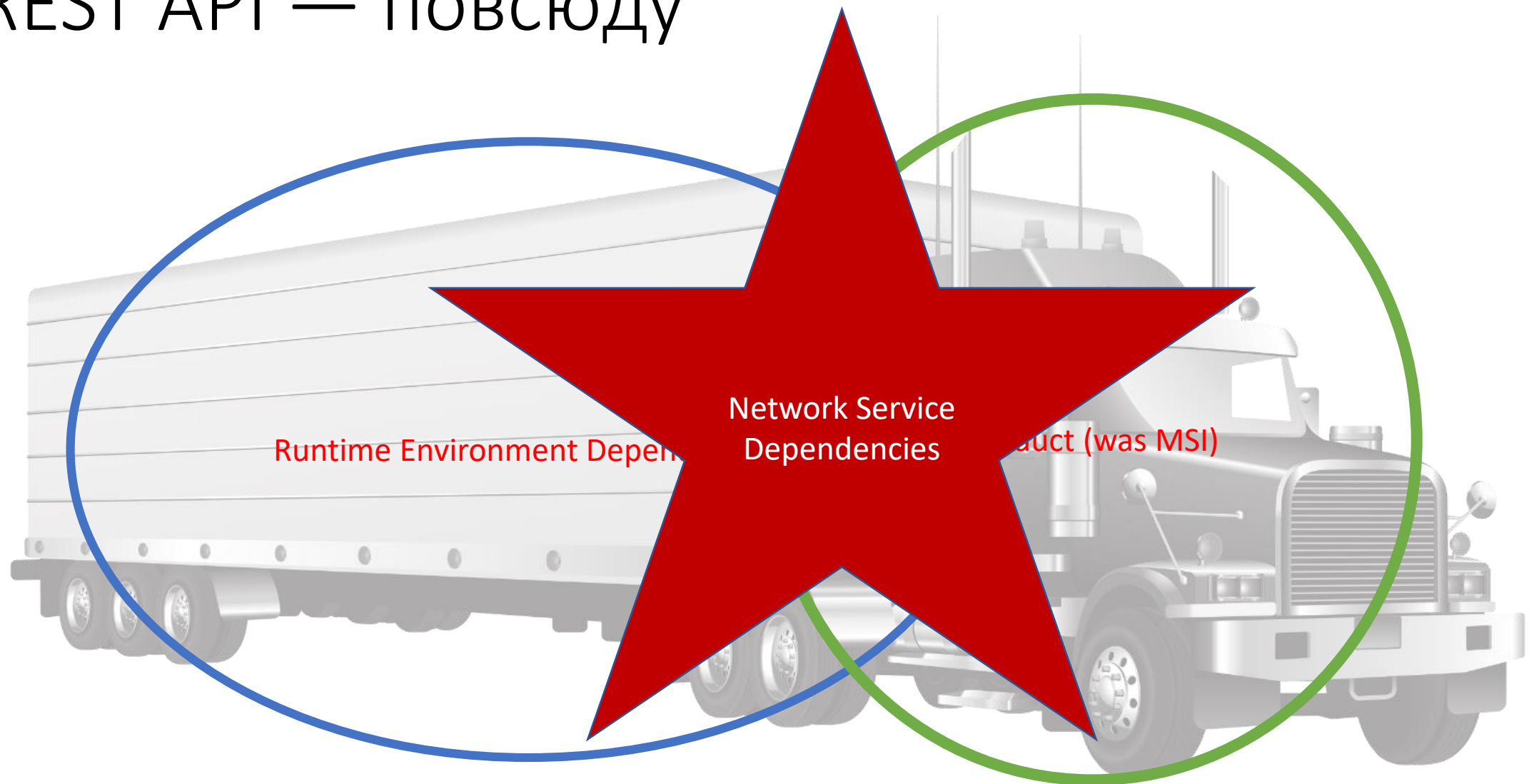
- MSI — база данных, содержащая изменения, вносимые в ОС



- Docker — система контроля версий, запись внесенных изменений



REST API — повсюду



Как-то так... The Beatles!



Docker

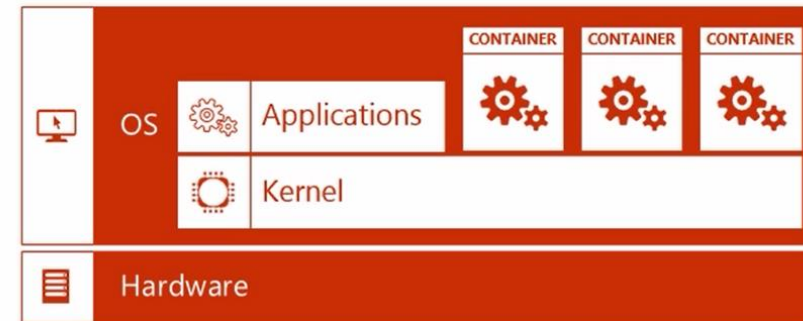
Container

Напоминалка...

- Управление ресурсами — подобно VM
 - Сеть — подобно VM, сложнее
 - Процесс сборки — ближе к MSI
 - Software (Docker) vs Hardware (VM)
-
- **Off topic:** holy war — Linux Server vs Windows Server 😊

Containers vs. Virtual Machines

Containers = Operating system virtualization



Traditional virtual machines = hardware virtualization



Общий Kernel? Hyper-V vs Process Isolation

Container OS version	Host OS version				
					Windows Server version 1803 Builds 17134.
					Supports Only <input type="button" value="hyperv"/> isolation
					Supports Only <input type="button" value="hyperv"/> isolation
Windows Server version 1803 Builds 17134.	Not supported	Not supported	Not supported	Not supported	Supports <input type="button" value="process"/> or <input type="button" value="hyperv"/> isolation

<https://docs.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/version-compatibility>

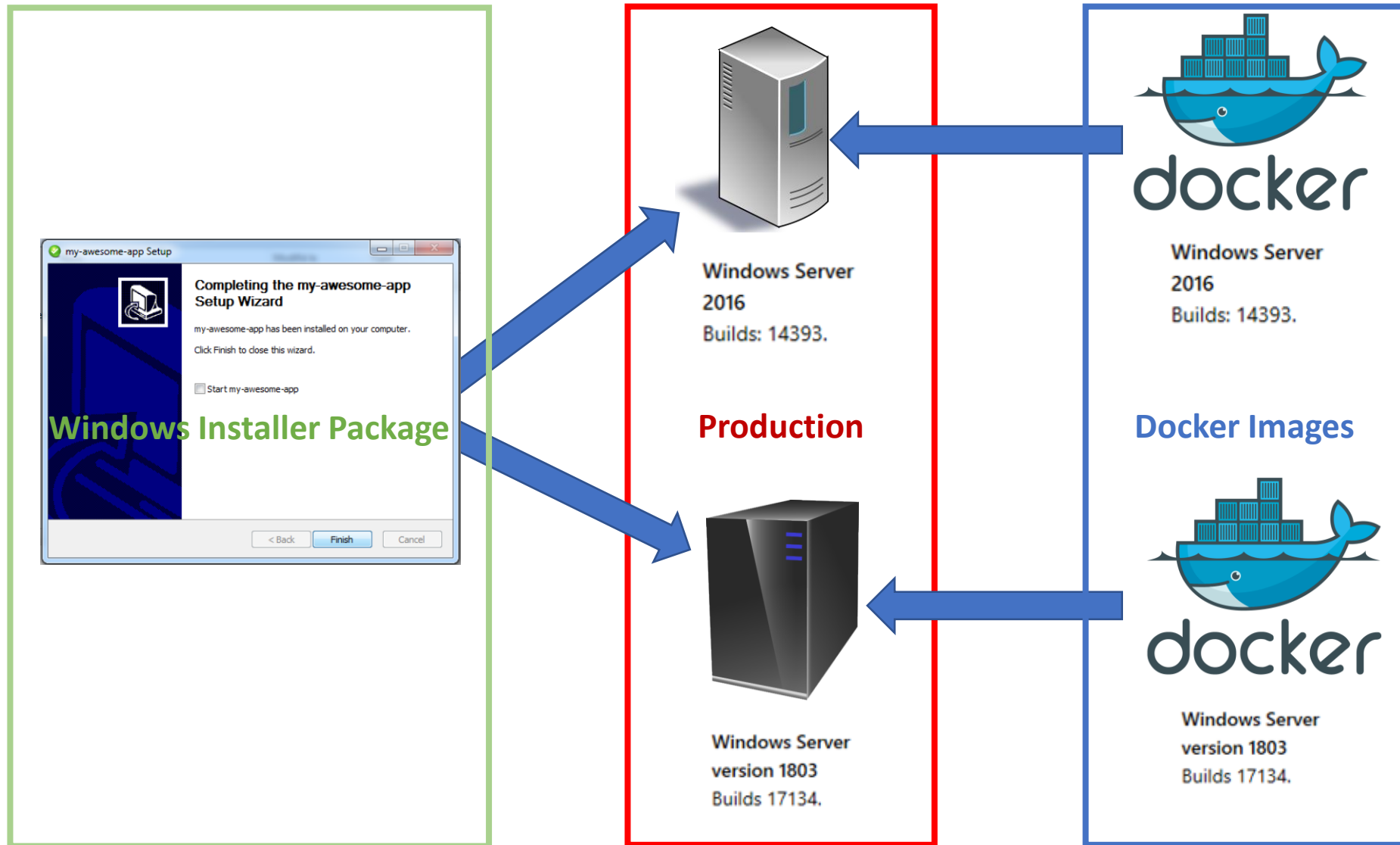
Изоляция на уровне Hyper-V

- Низкая производительность
- Требуется в 5 раз больше оперативной памяти
- Есть недоработки

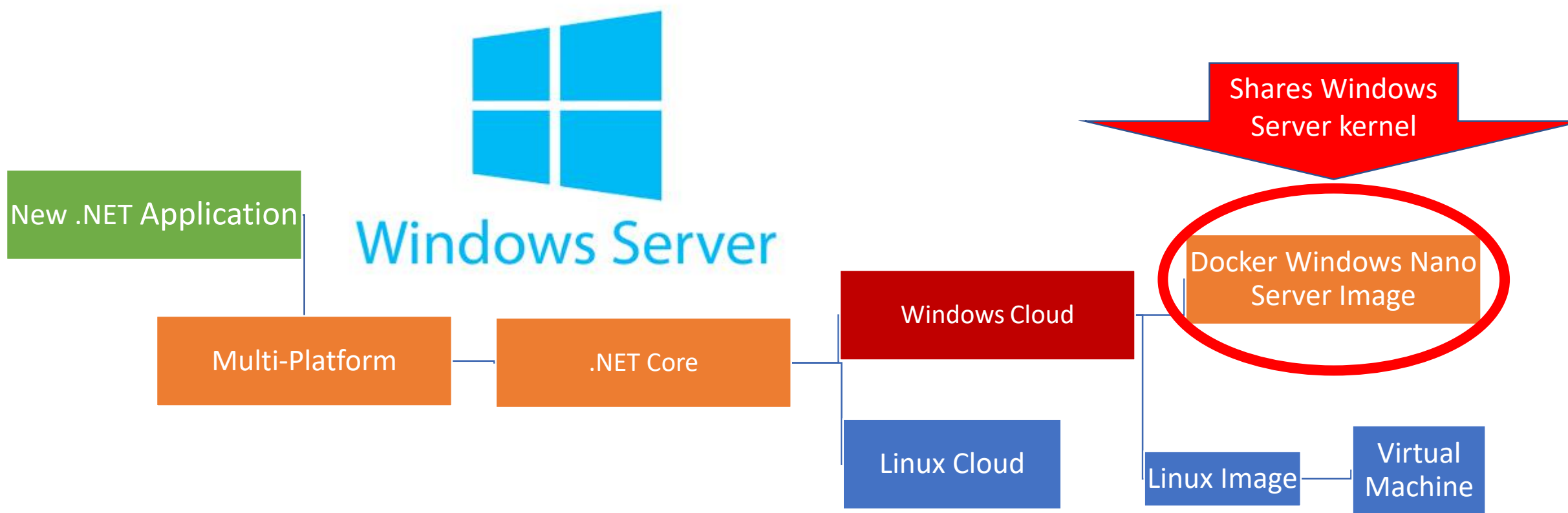


[Product Information](#) [Try It](#) [Partners](#)

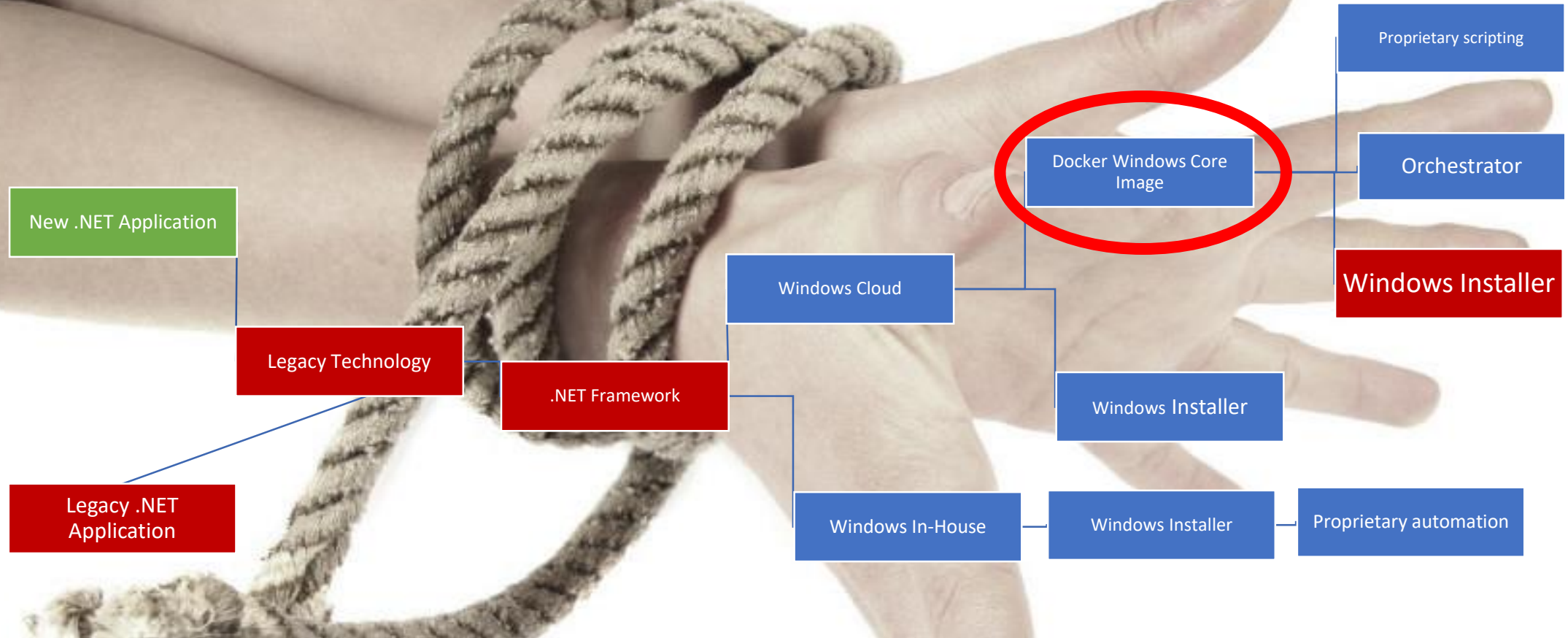
Различия в production с Windows Installer



Когда Docker for Windows? Если нет «якорей»



Когда Docker for Windows? Если что-то есть...



Сомнительные идеи для продакшена

- Docker в in-house — великоват и сложноват
- MSI в облако — гибкость под вопросом
- Конфигурировать работающий контейнер
- Смешивать Windows и Linux контейнеры на одном хосте
- Docker внутри виртуальной машины: Hyper-V isolation
- MSMQ, MSDTC, F#, ASP.NET Web Forms, Web Pages

Правила, нарушаем и дополняем



Tag			:1		:2	:latest
	:1.0	:1.1	:1.2	:2.0	:2.1	:3.0
Digest	91efj6	u82lq	2re7f	3rpn1	1n4ef	5wd1k

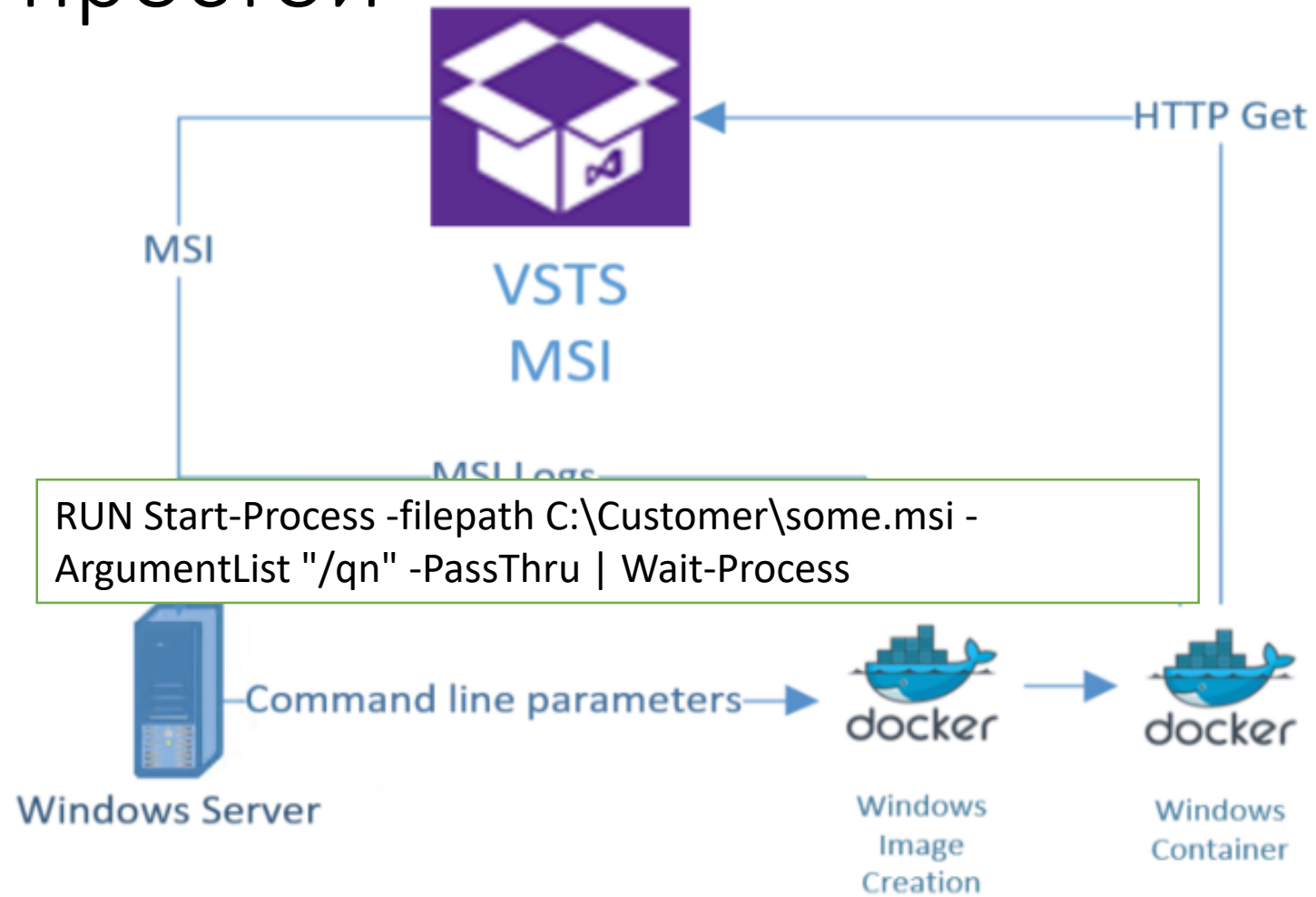
- 1) Don't store data in containers
- 2) Don't ship your application in two pieces
- 3) Don't create large images
- 4) Don't use a single layer image
- 5) Don't create images from running containers
- 6) Don't use only the "latest" tag
- 7) Don't run more than one process in a single container
- 8) Don't store credentials in the image.
- + 9) Don't mix Windows and Linux containers on the same host in production

Based on:

<https://developers.redhat.com/blog/2016/02/24/10-things-to-avoid-in-docker-containers/>

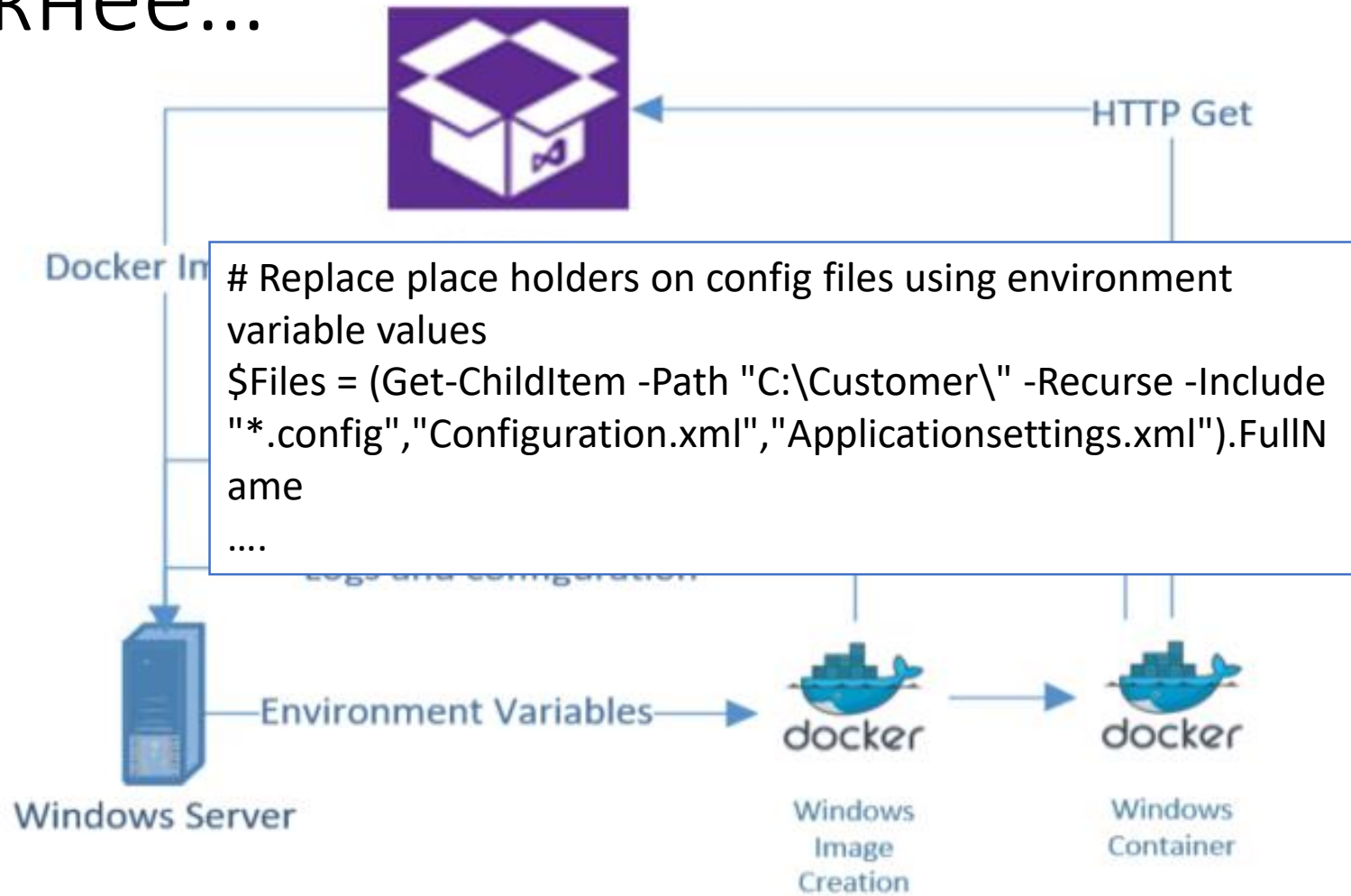
<https://blogs.msdn.microsoft.com/stevelasker/2018/03/01/docker-tagging-best-practices-for-tagging-and-versioning-docker-images/>

Самый простой



Windows Installer -> Windows Core Image
Wider technology support

Сложнее...



PowerShell (or WSA?) -> Windows Nano/Core Image
~500 MB instead of 12 GB

Безопасность — минимальная поверхность атаки

Достоинства контейнеров

1. Они минимальны
2. Специализированы
3. Изолированы
4. Воспроизводимы

Потенциальные уязвимости

1. Ядро
2. Denial of Service
3. Привилегии
4. Содержимое образа
5. Open source

Мониторинг во время выполнения



Дополнительная гибкость

- Сами образы Docker сжать нельзя 😊
- Вытащить Dockerfile из образов
- Каждое изменение RUN, COPY, ADD— новый слой
- Слить в текстовом редакторе или при помощи инструмента
- Разделить вручную

Typical networking

Virtual Machine (Host)

Frontend: “unique ip, port 80”

Backend: “localhost, port xxxx”

Other options: Bridge, No

Docker (Bridge)

Frontend: “unique ip, port xxxx:80”

Backend: “unique ip, port xxxx:xxxx”

Other options: Host, Container, No.

Кастинг дирижёра

Выбор – зависит от стратегии использования



kubernetes



How to use volumes in Swarm

```
version: '3'
volumes:
  poc:
services:
  redis:
    volumes:
      - poc:/redis
```

How to use volumes in Kubernetes :(

1. Create the pv [sample](#)
2. Create the pvc [sample](#)
3. Create the deployment specifying your pvc [sadness sample](#)

Кастинг дирижера



kubernetes

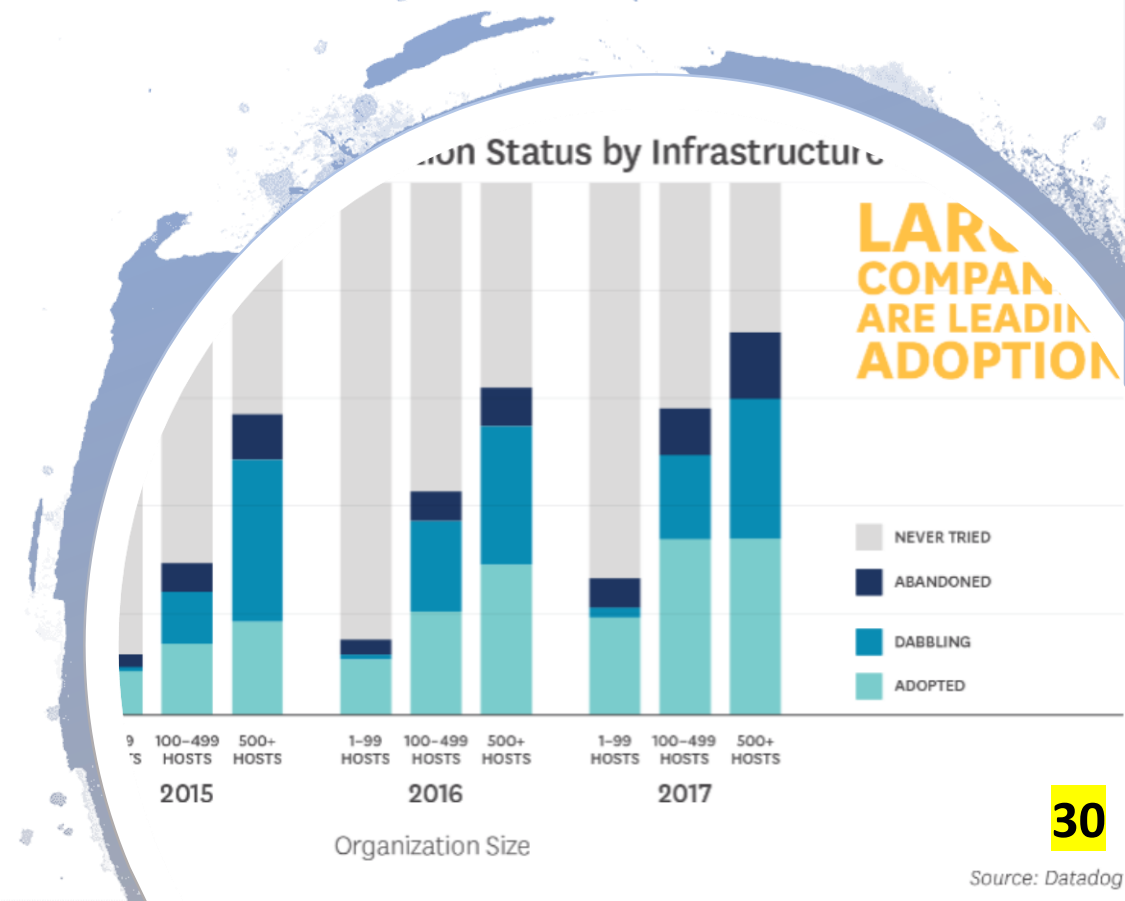
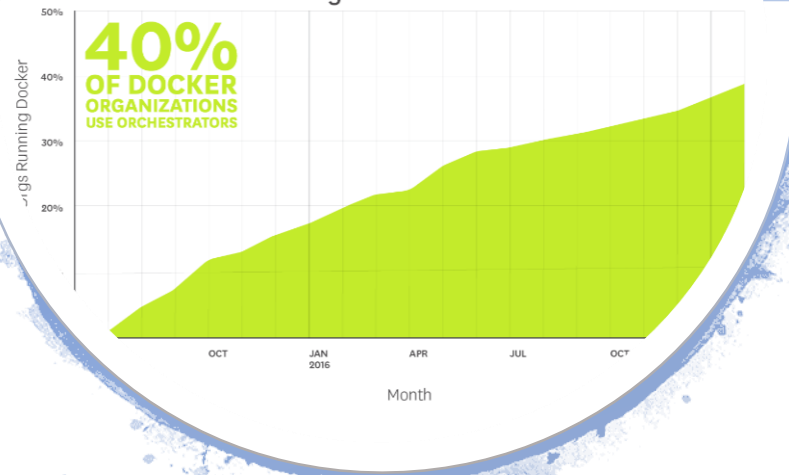
Kubernetes

- + Rancher 2.x (-kubernetes, -unfinished, +clusters)
- OpenShift (-\$\$\$\$, -clusters, +support, +scaling, ?win)



Docker Swarm

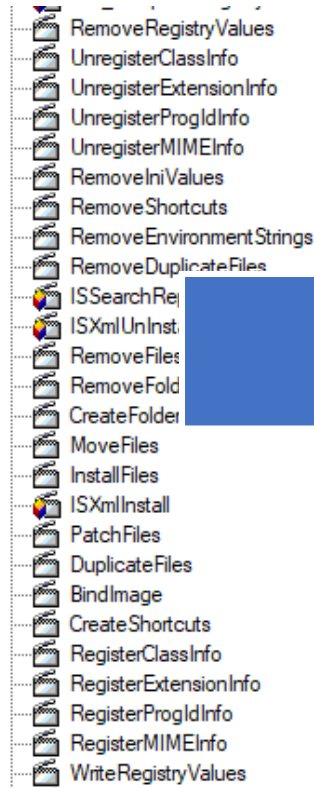
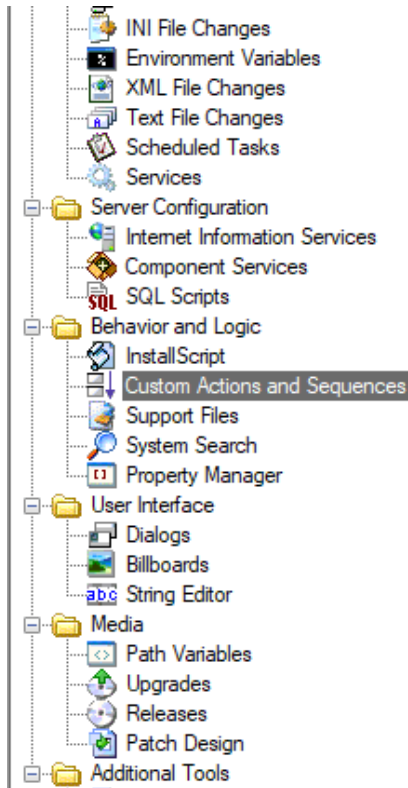
- + Universal Control Plane (-\$\$\$\$, -ent.ed)
- + Portainer.io (-support, -features, +\$\$\$)
- + Compose & proprietary scripting (-complex, +exp)



Как пример, наш скучный enterprise

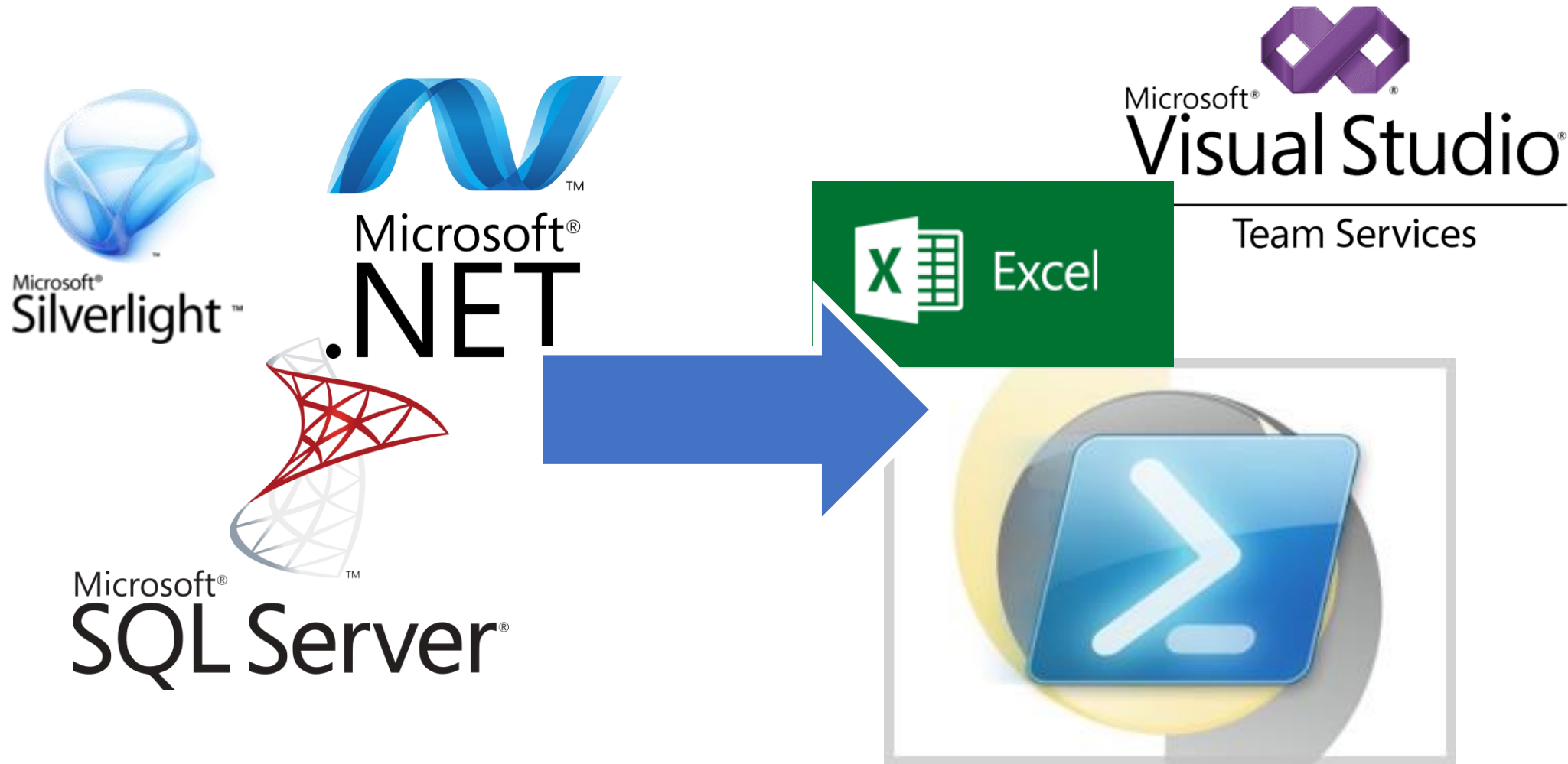
- Очень важные данные
 - Повреждение недопустимо, а тестирование ресурсоемко
- Множество унаследованных приложений, которые не будут переписаны на новые технологии в ближайшем будущем ☹
 - Мы всё же хотим двигаться вперёд, писать что-то новое 😊
- Не можем поддерживать многообразие технологий
 - Иногда надо просто сделать — чтобы работало, то что есть

Что же у нас? Конфигурация



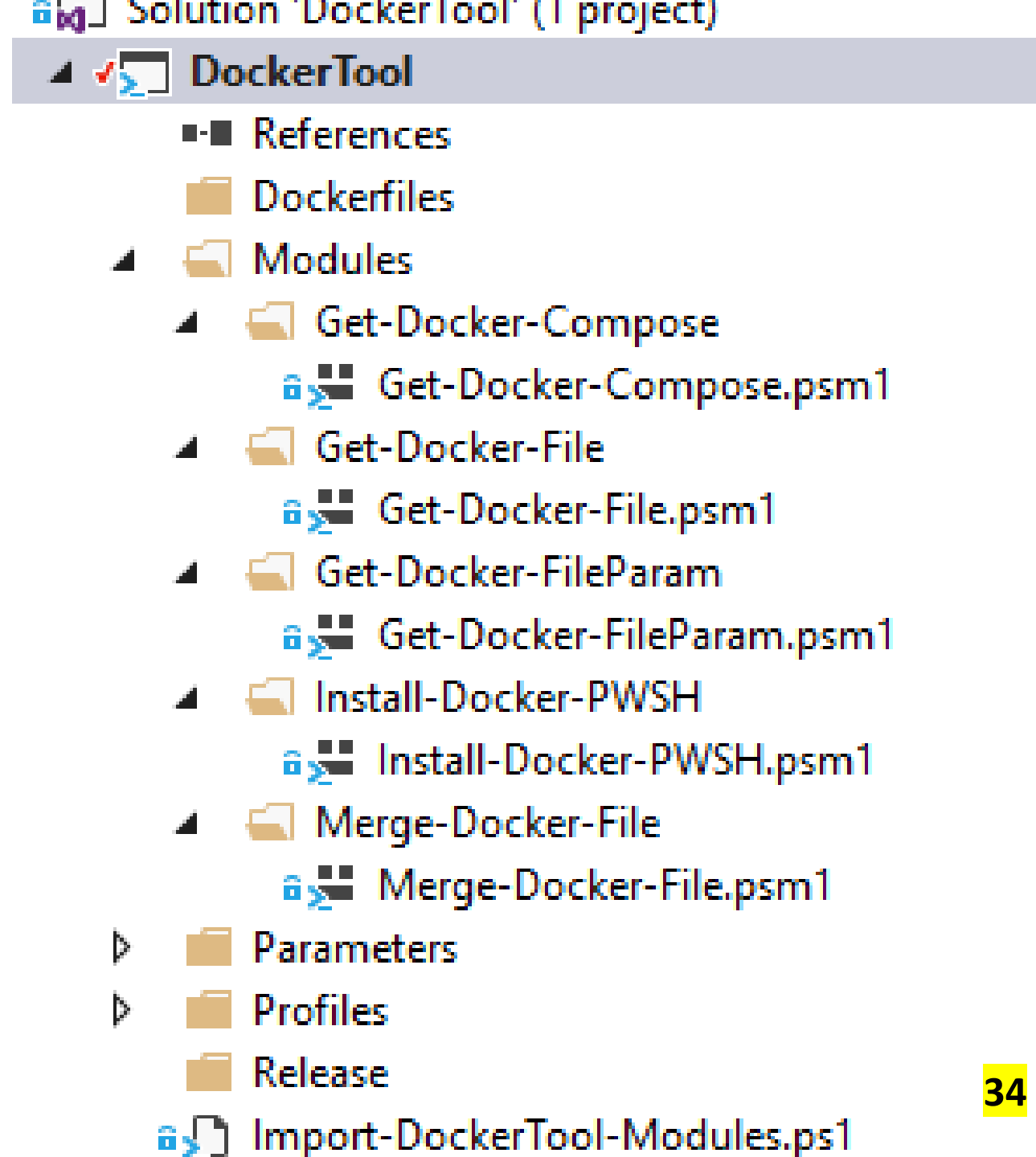
```
1 FROM /base-image:latest
2
3 # Import certificate and grant IIS access to it
4 COPY ["/cert", "/cert"]
5 RUN certutil -f -p password -importPFX
6   takenown /f 'C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys'
7   icacls 'C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys' /grant administrators:(F)
8
9 RUN New-WebAppPool -Name 'AppPool'; \
10 $AppPool = Get-Item 'IIS:\AppPools\ AppPool'; \
11 $AppPool.enable32BitAppOnWin64 = $True; \
12 $AppPool.startMode = 'AlwaysRunning'; \
13 $AppPool.processModel.loadUserProfile = $True; \
14 $AppPool.processModel.idleTimeout = [TimeSpan]::FromMilliseconds(10); \
15 $AppPool.recycling.periodicRestart.time = '00:00:00'; \
16 $AppPool | Set-Item; \
17 Set-ItemProperty 'IIS:\AppPools\ AppPool' -Name recycling.value -Type String -Value 'AppPool'; \
18 New-Item -Path 'C:\inetpub\wwwroot\AppPool' -ItemType Directory; \
19 New-WebVirtualDirectory -Site 'Default Web Site' -Name 'AppPool' -Path 'C:\inetpub\wwwroot\AppPool'; \
20 New-Item -Path 'C:\inetpub\wwwroot\AppPool\Admin' -ItemType Directory; \
21 New-WebApplication -Site 'Default Web Site' -Name 'AppPool' -Path 'C:\inetpub\wwwroot\AppPool'; \
22 Set-ItemProperty -Path 'IIS:\Sites\Default Web Site\AppPool' -Name 'AppPool' -Value 'AppPool'; \
23 New-Item -Path 'C:\inetpub\wwwroot\AppPool\Admin\Organization' -ItemType Directory; \
24 New-WebApplication -Site 'Default Web Site' -Name 'AppPool' -Path 'C:\inetpub\wwwroot\AppPool'; \
25 Set-ItemProperty -Path 'IIS:\Sites\Default Web Site\AppPool' -Name 'AppPool' -Value 'AppPool'; \
26 New-Item -Path 'C:\inetpub\wwwroot\AppPool\Admin\PersonMaster' -ItemType Directory; \
27 New-WebApplication -Site 'Default Web Site' -Name 'AppPool' -Path 'C:\inetpub\wwwroot\AppPool'; \
28 Set-ItemProperty -Path 'IIS:\Sites\Default Web Site\AppPool' -Name 'AppPool' -Value 'AppPool'; \
29 New-Item -Path 'C:\inetpub\wwwroot\AppPool\Admin\Security' -ItemType Directory; \
30 New-WebApplication -Site 'Default Web Site' -Name 'AppPool' -Path 'C:\inetpub\wwwroot\AppPool'; \
31 Set-ItemProperty -Path 'IIS:\Sites\Default Web Site\AppPool' -Name 'AppPool' -Value 'AppPool'; \
32 New-Item -Path 'C:\inetpub\wwwroot\AppPool\PersonMasterHtml' -ItemType Directory; \
33 New-WebApplication -Site 'Default Web Site' -Name 'AppPool' -Path 'C:\inetpub\wwwroot\AppPool'; \
34 Set-ItemProperty -Path 'IIS:\Sites\Default Web Site\AppPool' -Name 'AppPool' -Value 'AppPool'; \
35
```

Что же у нас? Зависимости



Инструменты — теперь Open Source

- Используешь Open Source? Участвуй в разработке!
- Docker Tool — генерируем Docker Compose, реверс-инжиниринг, мерж образов
 - <https://github.com/SoftwareCountry/docker-tool>
- Portainer — оркестратор, поддержка Windows
 - <https://github.com/portainer/portainer>
- Portainer.io deploy for VSTS
 - <https://marketplace.visualstudio.com/items?itemName=OlliJanatuinen.portainer-deploy>



Спасибо за внимание 😊
Вопросы и комментарии...

