Microsoft

Модернизация ИТ-инфраструктуры с помощью Windows Server 2016 (совместно с Veeam Software)

Александр Шаповал
Microsoft

Александр Шаповал

Эксперт по стратегическим технологиям

Email: ashapo@microsoft.com

Blog: http://blogs.technet.com/b/ashapo

https://habrahabr.ru/company/microsoft/

Twitter: @ashapoval

IT Camps

- IT Camp – это
  - Технологические семинары для ИТ-специалистов
  - Проводятся экспертами Microsoft
  - Предполагают выполнение лабораторных работ

- Материалы: http://1drv.ms/1kLGFB9
  - Что нового в Windows 10 Enterprise
  - Расширение возможностей ЦОД с помощью Microsoft Azure
  - Модернизация ИТ-инфраструктуры

Программа мероприятия

09:30 - 10:00	Регистрация
10:00 - 11:00	**Виртуализация**
11:00 - 12:00	**Инфраструктура хранилищ**
12:00 - 12:15	Перерыв
12:15 - 13:15	**Сетевая инфраструктура**
13:15 - 14:00	Обед
14:00 - 14:45	**Nano Server**
14:45 - 15:00	Перерыв
15:00 - 17:00	**Повышаем доступность ИТ-инфраструктуры на основе Windows Server (Veeam Software)**

Microsoft

Виртуализация

Александр Шаповал
Microsoft

Предыстория

МАСШТАБИРУЕМОСТЬ

64 виртуальных ЦП на ВМ

1 ТБ ОП на ВМ

4 ТБ ОП на узел

320 логических процессоров на узел

64 ТБ виртуальный жесткий диск (VHDX)

1024 ВМ на узел

Вирт. топология NUMA

СЕТЬ

Встроенная виртуальная сеть

Шлюз виртуальной сети

Расширенные ACL для портов

vRSS

Динамические рабочие группы

ГИБКОСТЬ

Динамическая память

Динамическая миграция (ДМ)

ДМ со сжатием

ДМ напрямую через SMB

ДМ хранилища

ДМ в режиме «ничего общего» (Shared Nothing)

ДМ между версиями

Быстрое добавление и изменение размера VHDX

Функция управления качеством обслуживания в системе хранения данных

Динамический экспорт ВМ

ГЕТЕРОГЕННОСТЬ

Linux

FreeBSD

ДОСТУПНОСТЬ

Кластеризация узлов

Кластеры из 64 узлов

Гостевая кластеризация

Общий диск VHDX

Реплика Hyper-V

И МНОГОЕ ДРУГОЕ…

ВМ 2-го поколения

Улучшенные сеансы

Автоматическая активация ВМ

Встроено.

Безопасность и изоляция

Привилегированная структура

Популяризация технологий виртуализации привела к неожиданным последствиям для безопасности

1 **Администраторы структуры или виртуальной среды**

Обладают высочайшими привилегиями (в отличие от традиционной модели, где наиболее доверенными ИТ-специалистами являются администраторы домена).

2 **Виртуализованные контроллеры домена**

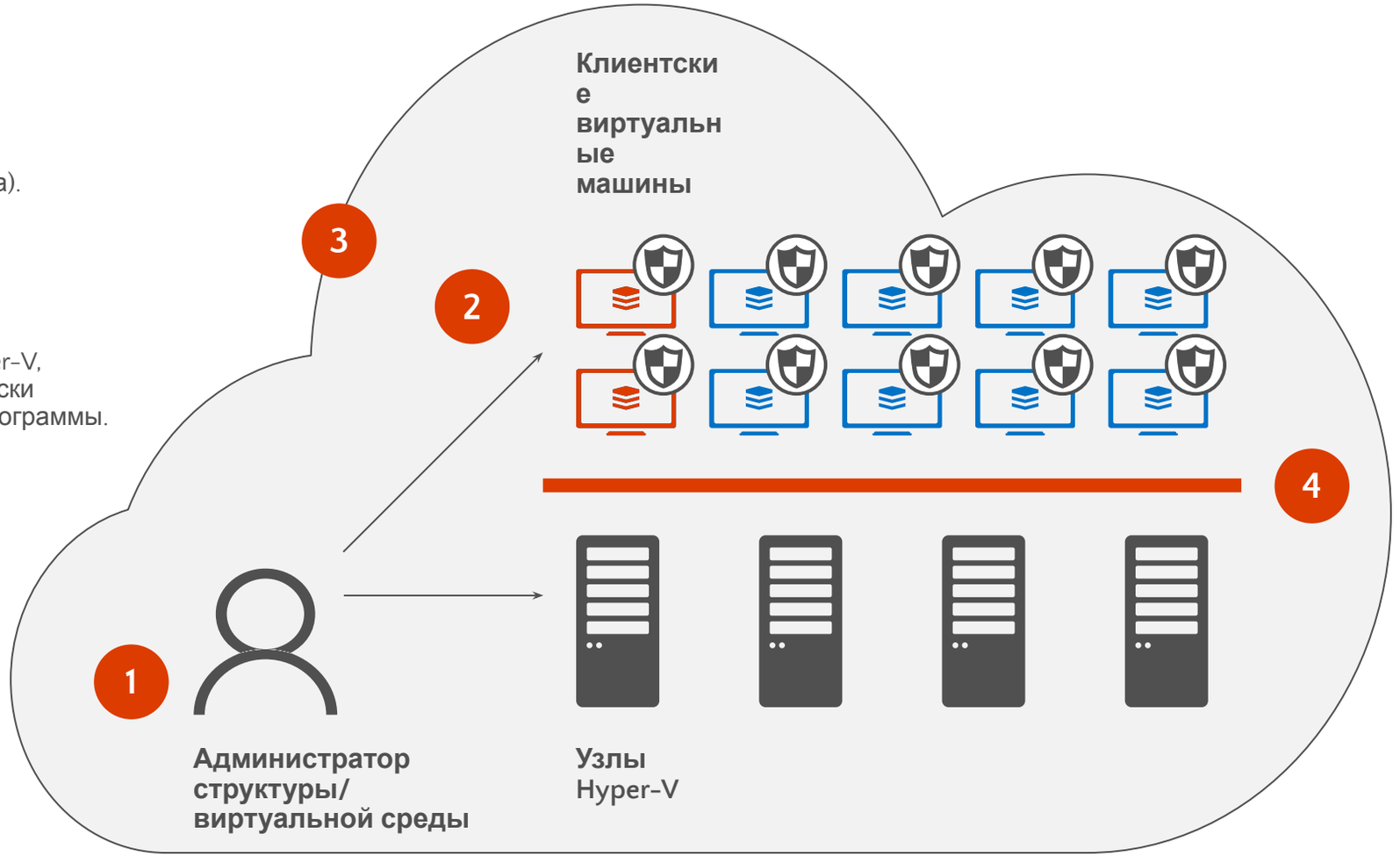
Если ЦОД виртуализованы и я — администратор Hyper-V, то я могу отключить ВМ, скопировать виртуальные диски для автономных атак или установить вредоносные программы.

3 **Публичное облако**

Администраторы структуры потенциально обладают полным доступом к клиентским ВМ.

4 **Экранированные виртуальные машины (Shielded VMs)**

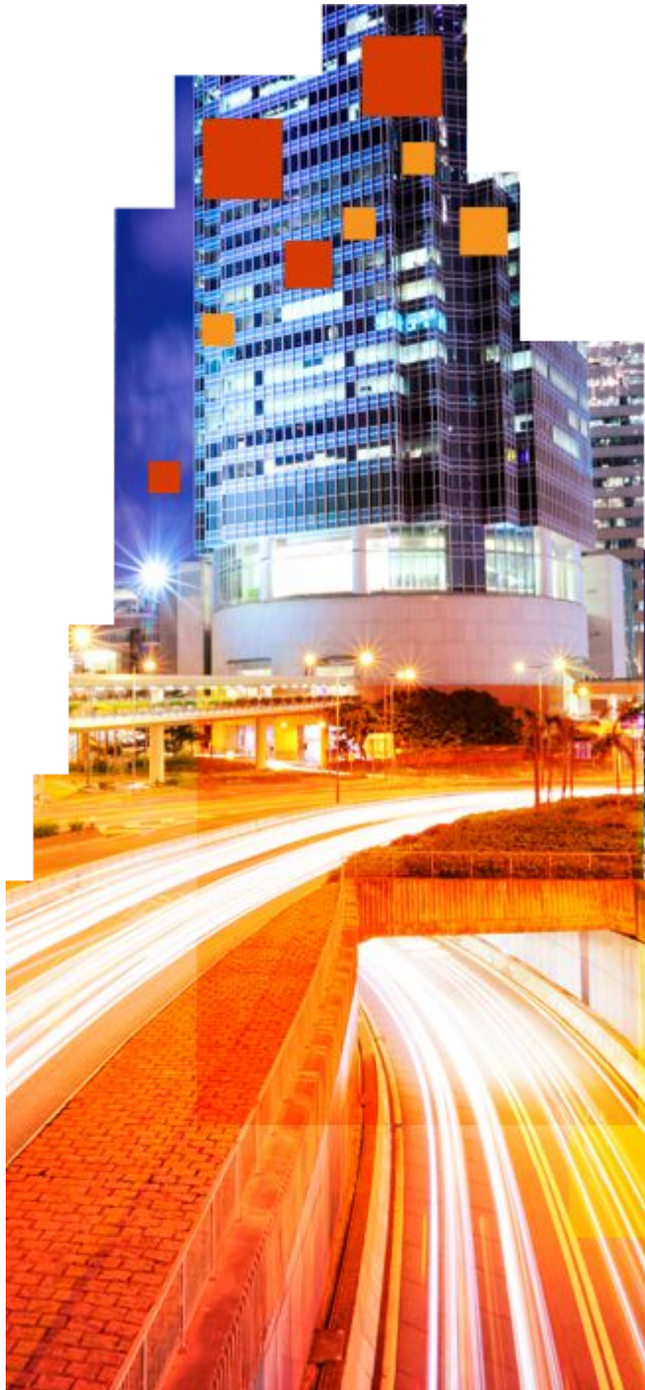
Строгое разделение администраторов структуры и администраторов рабочих нагрузок с помощью механизмов шифрования и защищенных секретов.



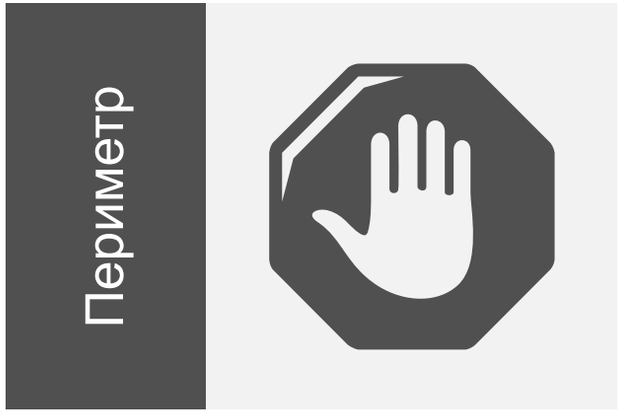
Что же такое «экранированная виртуальная машина»?

Данные и состояние экранированной ВМ защищены от просмотра, хищения и модификации со стороны как вредоносных программ, так и администраторов ЦОД[1]

[1] Администраторов инфраструктуры, хранилищ, серверов и сети.



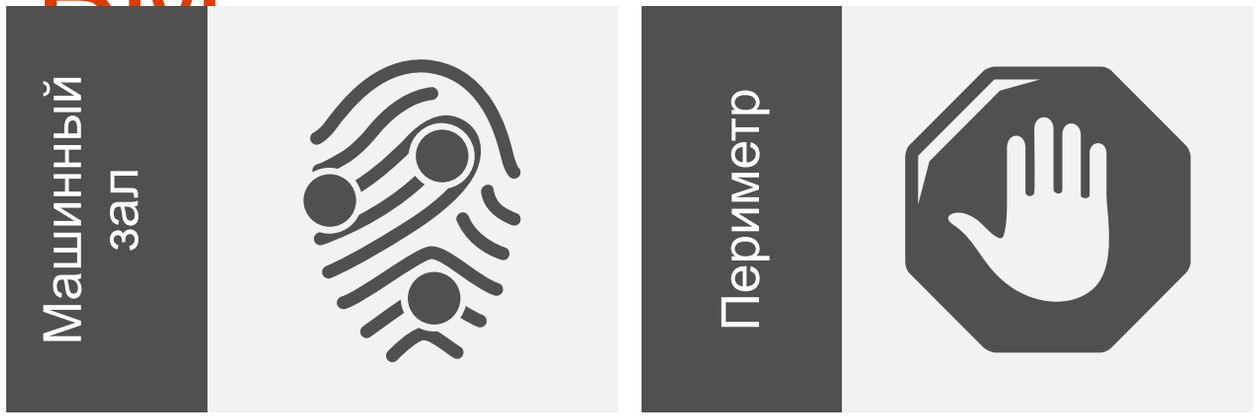
Этап 1. Текущая ситуация

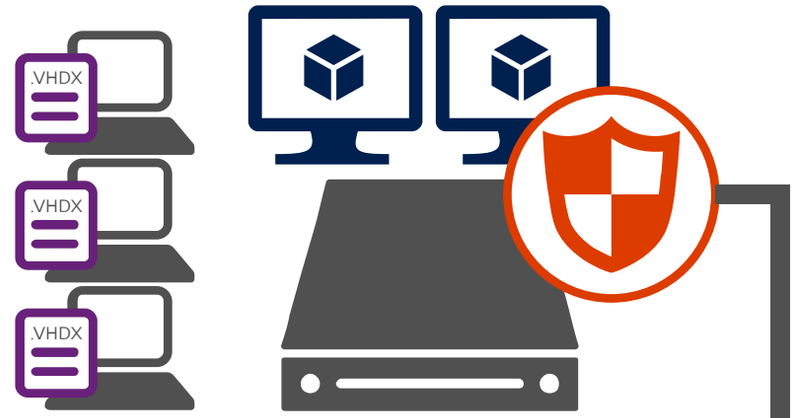


Hyper-V

	Физические компьютеры	Виртуальные машины
Администратор сервера	Да	Да
Администратор хранилища	Нет	Да
Администратор сети	Нет	Да
Оператор резервного копирования	Нет	Да
Администратор узла виртуализации	Нет	Да

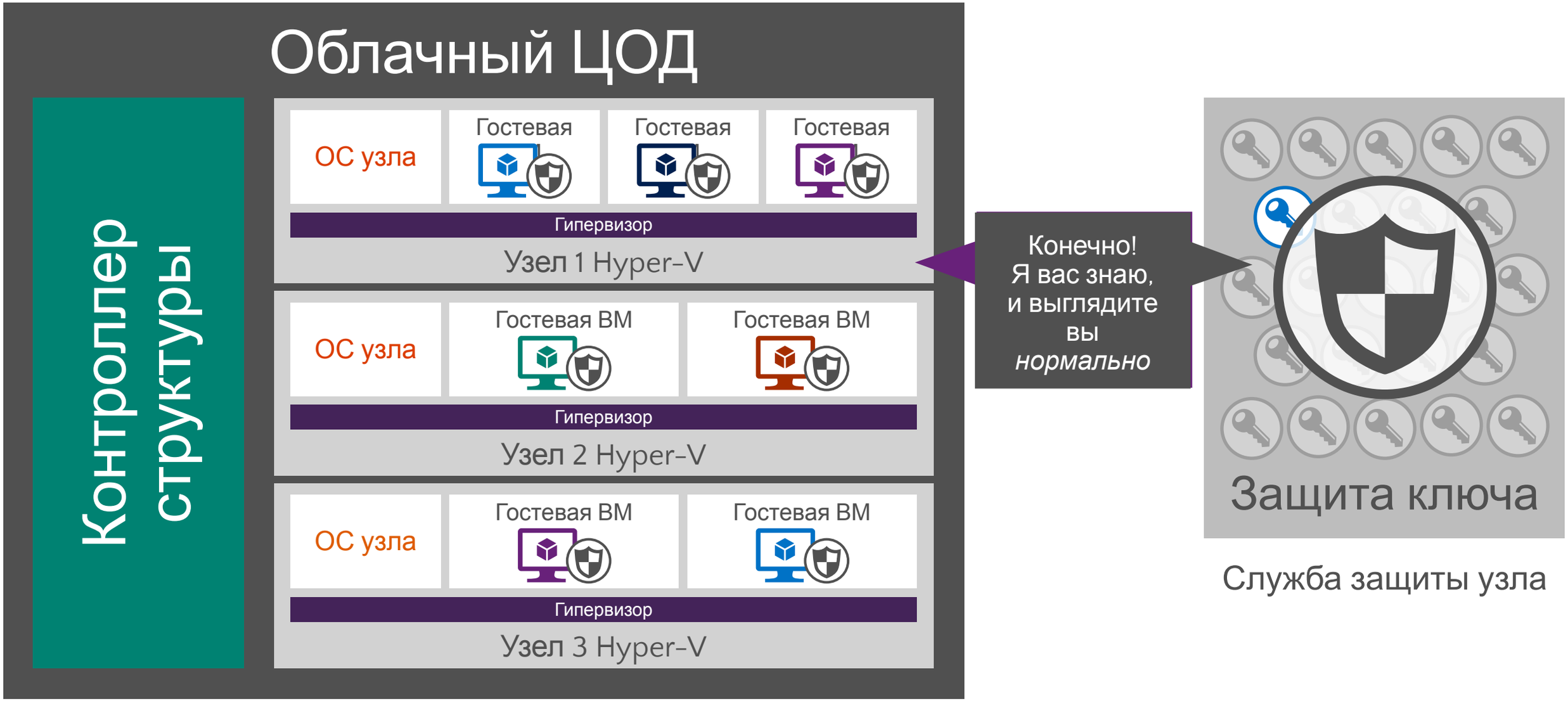
Этап 1. Шифрование данных и состояния ВМ





	Физические компьютеры	Виртуальные машины
Администратор сервера	Да	Зависит от конфигурации
Администратор хранилища	Нет	Нет
Администратор сети	Нет	Нет
Оператор резервного копирования	Нет	Нет
Администратор узла виртуализации	Нет	Нет

Этап 2. Дешифровальные ключи под управлением внешней системы



Компонент 1. ВМ 2-го поколения

Загрузка с виртуального встроенного UEFI

Обеспечивает безопасную загрузку, гарантируя невозможность модификации как встроенного ПО UEFI, так и загрузочных файлов ВМ.

Также позволяет применять шифрование дисков BitLocker для виртуальных дисков ВМ.

Поддержка современных ОС

Поколение 2 поддерживает Windows Server 2012/Windows 8 и более поздние версии.

Поддержка Windows Server 2008/2008 R2 пока в разработке.

Компонент 2. Защищенная структура

Служба защиты узла (HGS): роль Windows Server, используемая для реализации защищенной структуры

HGS — основа служб аттестации и распределения ключей, позволяющих запускать экранированные ВМ на защищенных узлах.

Защищенный узел: узел структуры, на котором могут запускаться экранированные ВМ. Защищенные узлы считаются доверенными только после прохождения идентификации. Для успешной аттестации узел должен быть корректно настроен.

Аттестация: процесс, в ходе которого служба защиты узла (HGS) проверяет, является ли узел частью структуры, защищен ли он, и каково состояние его конфигурации.

Распределение ключей: операция передачи ключа на защищенный узел, после которой он может разблокировать и запускать экранированные ВМ.

Служба защиты узла должна выполняться в собственном домене Active Directory и быть изолированной от AD текущей структуры.

Компоненты: аттестация

Аттестация Hardware-trusted
(на базе TPM)

Более сложная настройка и конфигурация
- Регистрация доверенного платформенного модуля каждого узла Hyper-V (EKpub) в HGS.
- Создание базовой политики CI для каждого SKU устройства.
- Развертывание HSM и применение сертификатов с защитой HSM.

Для узлов Hyper-V необходимы новые устройства
- Необходима поддержка TPM 2.0 и UEFI 2.3.1.

Самые надежные уровни контроля
- Основа доверия — аппаратная платформа.
- Соответствие политике CI — необходимое условие выпуска ключа (аттестации).
- Недоверие администратору структуры.

Аттестация Admin-trusted
(на основе Active Directory)

Упрощенные развертывание и настройка
- Настройка доверия Active Directory + регистрация группы.
- Авторизация узла Hyper-V для запуска экранированных ВМ путем добавления его в группу Active Directory.

Существующие устройства, скорее всего, соответствуют требованиям

Поддерживаемые сценарии
- Защита данных при хранении и передаче.
- Безопасное аварийное восстановление на ресурсы хостера (ВМ уже экранирована).

Менее надежные уровни контроля
- Доверие администратору структуры.
- Отсутствие измеряемой загрузки и аппаратной защиты.
- Отсутствие контроля целостности кода.

Характерно для поставщиков услуг

Характерно для предприятий

Настройка аттестации

Режим аттестации

Режим TPM применяется в случае, когда вы доверяете лишь устройствам, на которых выполняется Hyper-V.

Режим AD применяется в случае, когда вы доверяете администраторам Active Directory и структуры.

Список авторизованных узлов

В режиме TPM необходимо настроить список известных EKpub для авторизованных узлов.

В режиме AD необходимо настроить лишь группу (или группы) Active Directory.

Условия выпуска ключа

В режиме TPM служба аттестации проверяет состояние узла (измерения загрузки и CI).

В режиме AD измерения загрузки и политики целостности кода в учет не принимаются.

Результат – экранированная ВМ

Экранированные ВМ

Узел
Hyper-V

Что происходит при запуске экранированной ВМ?

- vTPM позволяет использовать шифрование дисков ВМ (например, BitLocker).
- Файлы конфигурации и состояние ВМ шифруются.
- Весь трафик динамической миграции также шифруется; использовать IPsec для этого не требуется.
- Аварийные дампы узла шифруются.
- По умолчанию аварийные дампы ВМ отключены. Если вы их включите, они также будут шифроваться.

У администраторов структуры нет доступа к ВМ

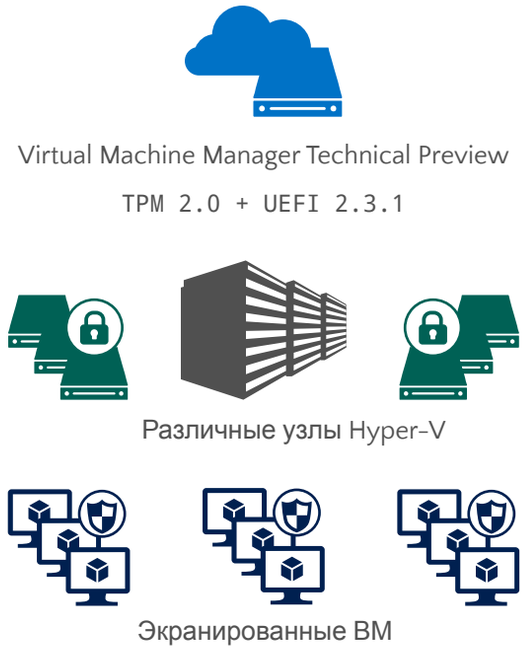
- Подключать отладчики во время выполнения невозможно (это запрещают VMWP защищенных ВМ, обеспечивающие работу каждой ВМ).
- Содержимое файлов VHDX, защищенное механизмом BitLocker, недоступно.
- Подключение к ВМ через консоль невозможно.
- ВМ могут выполняться только на известных и «исправных» (безопасных) узлах при помощи службы защиты узла.

Архитектуры

Инфраструктура ЦОД

Служба защиты узла
Relecloud.com

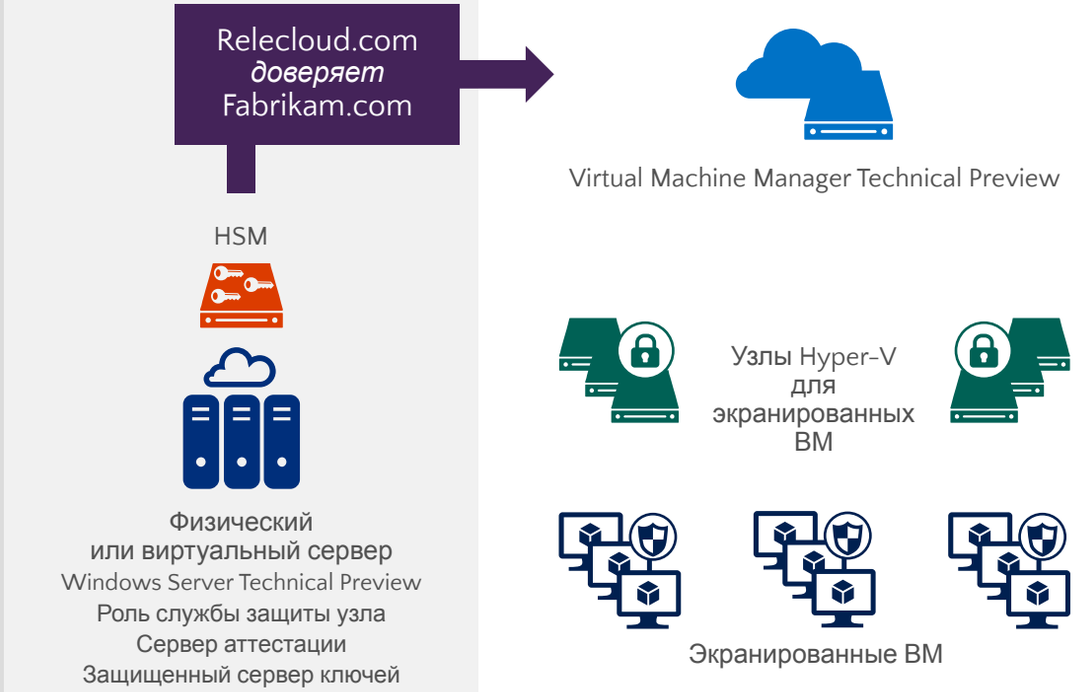
Active Directory хостера
Fabrikam.com



Инфраструктура ЦОД

Служба защиты узла
Relecloud.com

Active Directory хостера
Fabrikam.com



Демонстрация
Экранированные виртуальные машины

Доступность

Служба Failover Clustering

Встроенное решение, усовершенствованное в версии Windows Server Technical Preview

Устойчивость вычислений в ВМ

Обеспечивает устойчивость к временным сбоям, например, к разрывам сетевого соединения или отсутствию отклика от узла.

В случае изоляции узла ВМ продолжат работу, даже если узел выйдет из состава кластера.

Это поведение можно настраивать в соответствии с вашими требованиями. Значение по умолчанию — 4 минуты.

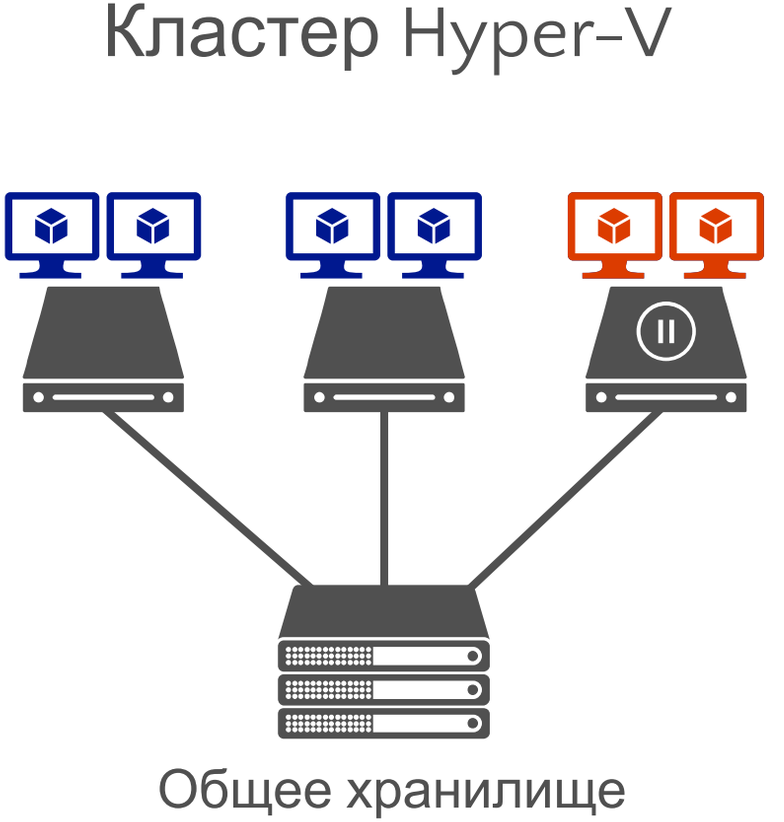
Устойчивость хранилища ВМ

Сохраняет состояние сеанса клиентской ВМ даже при временных сбоях хранилища.

Стек ВМ быстро и интеллектуально уведомляется о сбое базовой инфраструктуры хранения (с блочной записью или на основе файлов).

ВМ быстро переходит в состояние PausedCritical.

ВМ ожидает восстановления хранилища; состояние сеанса сохраняется до восстановления.



Служба Failover Clustering

Встроенное решение, усовершенствованное в версии Windows Server Technical Preview

Карантин для узлов

Неисправные узлы помещаются в карантин и больше не могут присоединяться к кластеру.

При таком подходе они не могут отрицательно повлиять на другие узлы и на кластер в целом.

Узел помещается в карантин после трех неожиданных выходов из кластера в течение часа.

После того как узел помещен в карантин, для ВМ выполняется динамическая миграция из узла кластера, без перебоев в работе ВМ.

Гостевая кластеризация с общим диском VHDX

Не зависит от топологии базового хранилища

Гибкая и безопасная

Общий диск VHDX позволяет обойтись без представления базового физического хранилища для гостевой ОС.

НОВИНКА Размер общих дисков VHDX можно изменять без перехода в автономный режим.

Упрощенное общее хранилище для ВМ

Несколько виртуальных машин одновременно используют общие файлы VHDX в качестве общего хранилища данных.

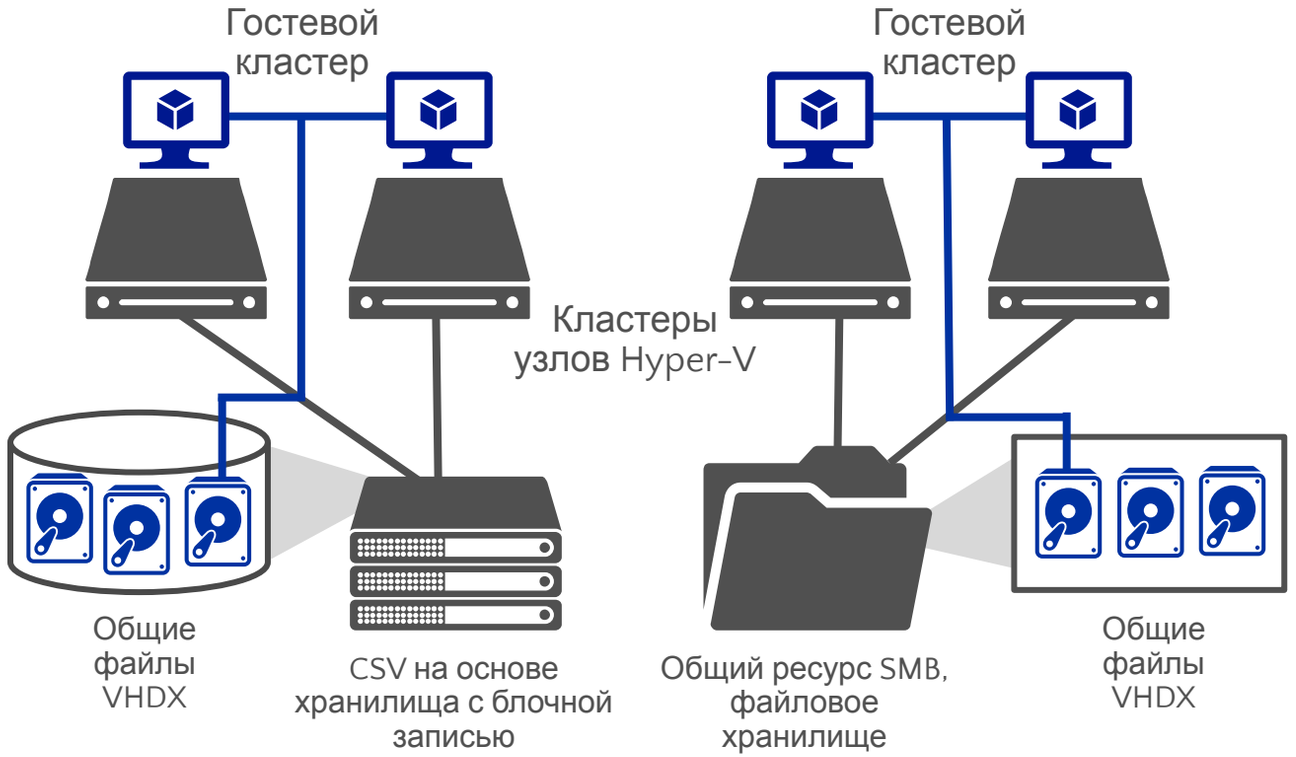
Для ВМ оно представляет собой общий виртуальный диск SAS, который можно использовать для кластеризации на уровне гостевой ОС и приложений.

Используется постоянное резервирование SCSI.

Общие файлы VHDX размещаются на общем томе кластера (CSV) в хранилище с блочной записью или в файловом хранилище SMB.

НОВИНКА Средства защиты

Общие файлы VHDX поддерживают реплику Hyper-V и резервное копирование на уровне узла.



Управление памятью

Высокая гибкость для оптимальной загрузки узлов

Статическая память

Параметр Startup RAM (ОЗУ при запуске) определяет объем памяти, который будет выделен вне зависимости от потребности ВМ в памяти.

НОВИНКА Изменение размера во время выполнения

Теперь администраторы могут **увеличивать** и **уменьшать** объем оперативной памяти ВМ без остановки машины.

Нижняя граница параметра — объем памяти, необходимый ВМ в настоящий момент, верхняя — объем физической системной памяти.

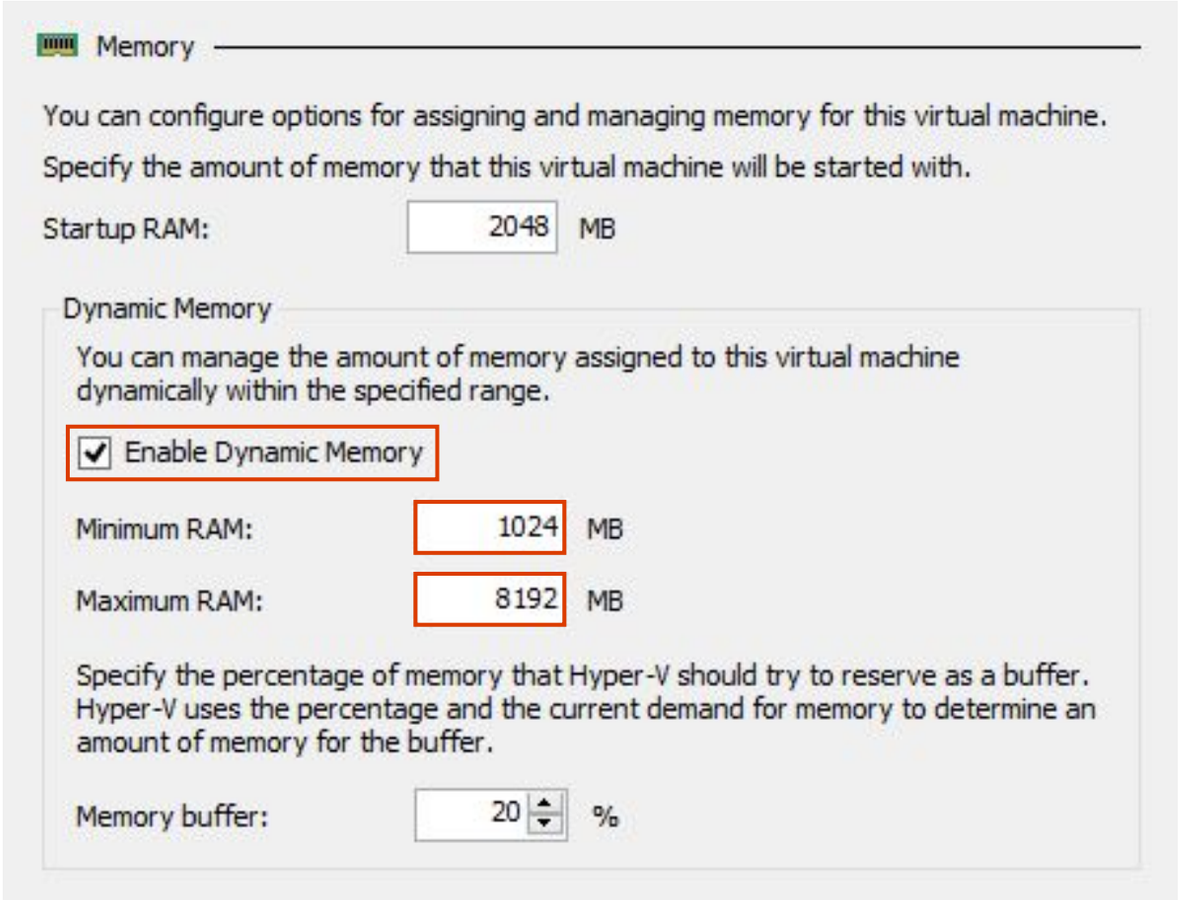
Динамическая память

Позволяет динамически перераспределять память между запущенными ВМ.

Помогает эффективнее использовать ресурсы, повысить уровень консолидации и надежность операций перезагрузки.

Изменение размера во время выполнения

Если параметр Dynamic Memory (Динамическая память) включен, администраторы могут повысить максимальный или уменьшить минимальный объем оперативной памяти без остановки ВМ.



Виртуализация и сети

Усовершенствования виртуального сетевого адаптера

Гибкость

Теперь администраторы могут добавлять и удалять виртуальные NIC (vNIC) ВМ, не останавливая ее.

По умолчанию включено; доступно только для ВМ 2-го поколения.

vNIC можно добавлять с помощью графического интерфейса Hyper-V Manager или PowerShell.

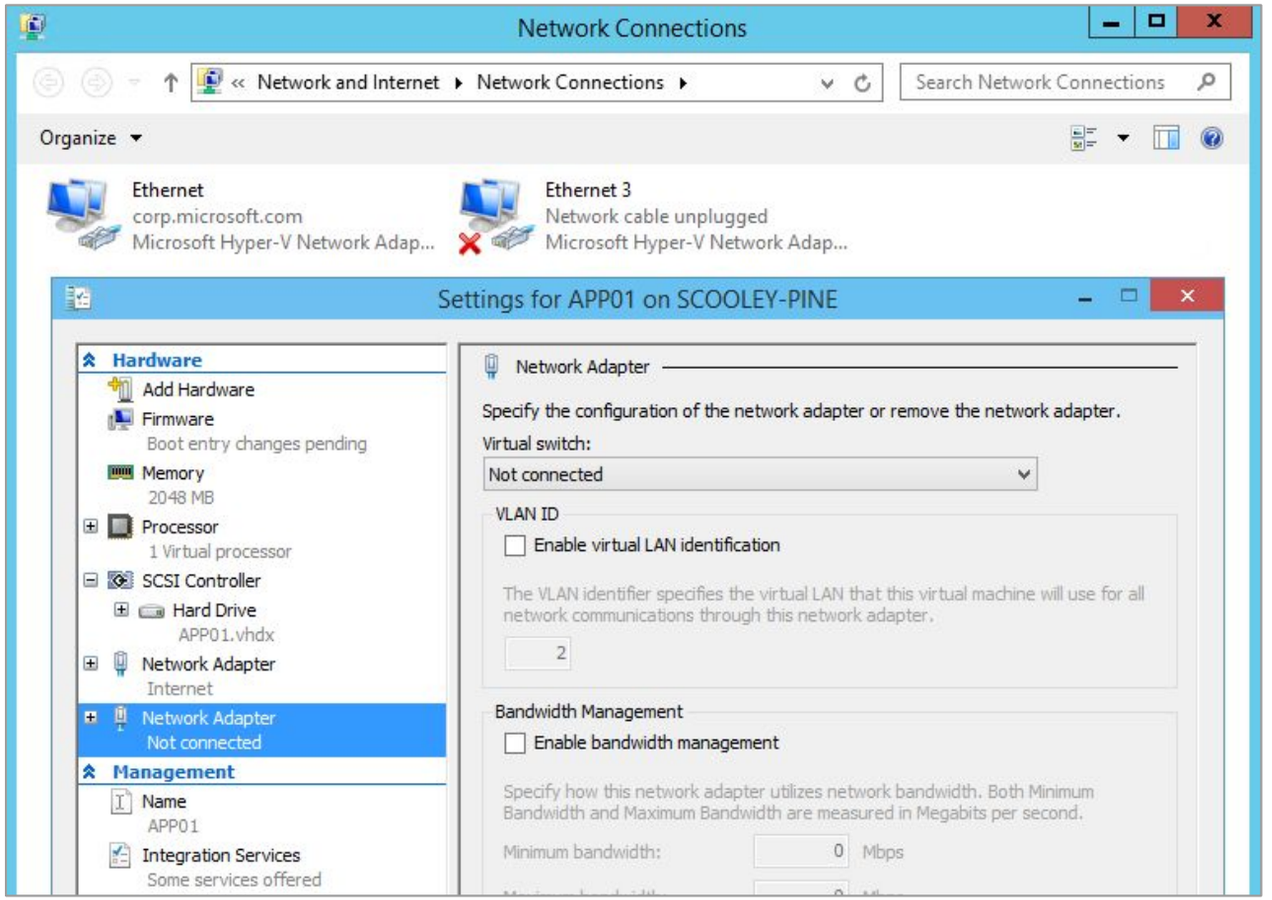
Полная поддержка

Возможность «горячего» добавления и удаления vNIC доступна для всех поддерживаемых гостевых ОС Windows и Linux.

Идентификация vNIC

Новая возможность: присвоение vNIC в настройках ВМ имени, которое будет отображаться в гостевой операционной системе.

```
Add-VMNetworkAdapter -VMName “TestVM” – SwitchName
“Virtual Switch” -Name “TestNIC” -Passthru |
Set-VMNetworkAdapter -DeviceNaming on
```



Применение обновлений

Последовательные обновления ОС кластера

Добавлена возможность обновления узлов кластера без остановки ключевых рабочих нагрузок

Упрощенный процесс обновления

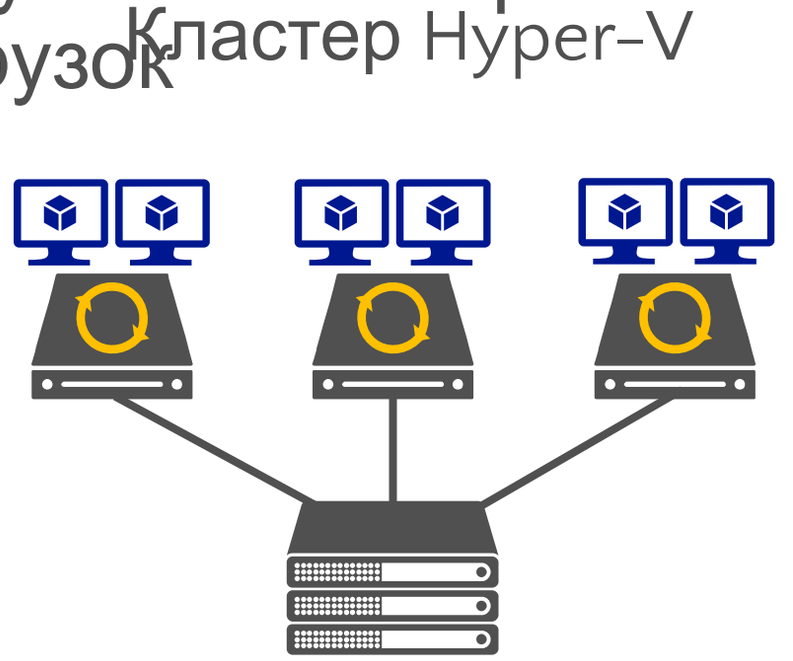
ОС узлов кластера можно обновить с Windows Server 2012 R2 до Windows Server Technical Preview без остановки рабочих нагрузок Hyper-V и SOFS.

По мере развития технологий инфраструктуру можно обновлять, не прерывая выполнение рабочих нагрузок.

Поэтапные обновления

1. Узел кластеров приостанавливается, рабочие нагрузки переносятся из него на доступные для миграции ресурсы.
2. Узел исключается, операционная система заменяется чистой установкой Windows Server Technical Preview.
3. Новый узел добавляется обратно в активный кластер. Теперь кластер работает в смешанном режиме. Процесс повторяется для других узлов.

Функциональные возможности кластера сохраняются на уровне Windows Server 2012 R2 до обновления всех узлов. После завершения администратор запускает команду `Update-ClusterFunctionalLevel`.



Узлы кластера Windows Server 2012 R2	Обновленные узлы кластера Windows Server

Обновления виртуальных машин

Новые процессы обновления и обслуживания ВМ

Режим совместимости

При миграции виртуальной машины на узел Windows Server Technical Preview она остается в режиме совместимости с Windows Server 2012 R2.

ВМ обновляется отдельно от узла.

Виртуальные машины можно переместить в более ранние версии, пока они не будут обновлены вручную.

```
Update-VMVersion vmname
```

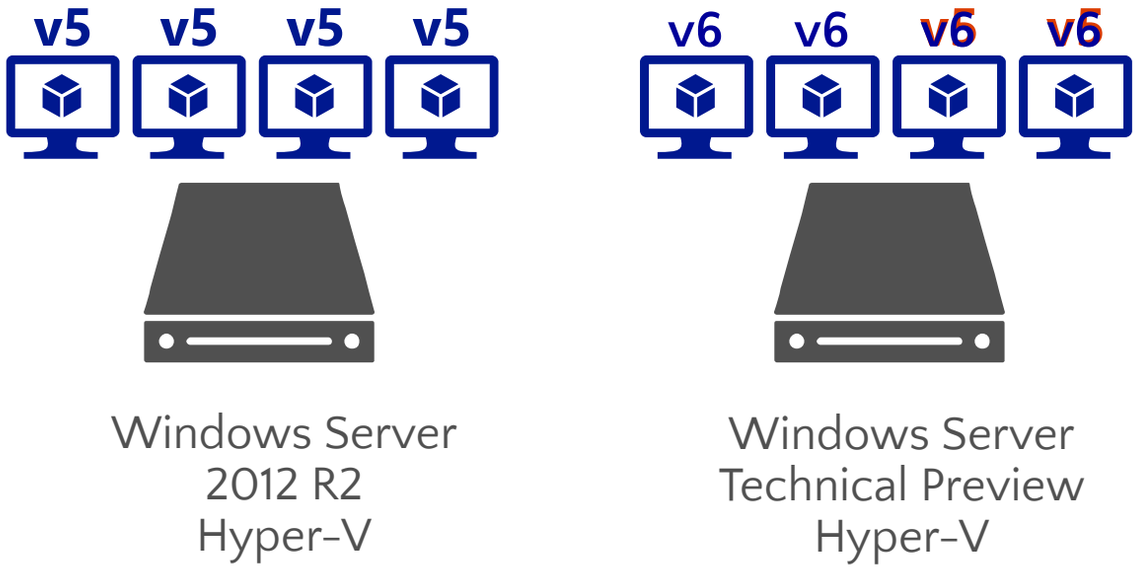
После обновления ВМ смогут использовать новые функции своего узла Hyper-V.

Модель обслуживания

Драйверы ВМ (службы интеграции) обновляются по мере необходимости.

Обновленные драйверы ВМ отправляются напрямую гостевой операционной системе посредством Центра обновления Windows.

Команда `Update-VMVersion`
обновляет ВМ до новейшей версии аппаратной платформы
и позволяет им использовать новые функции Hyper-V



Повышение операционной эффективности

Рабочие контрольные точки

Полная поддержка рабочих сред

Полная поддержка ключевых рабочих нагрузок

Удобная функция создания образа виртуальной машины в определенный момент времени и ее быстрого восстановления из этого образа. Способ восстановления полностью поддерживается для всех рабочих нагрузок производственной среды.

VSS

Служба моментального снимка тома (VSS) применяется в виртуальных машинах Windows для создания рабочих контрольных точек; она служит заменой технологии сохранения состояний.

Знакомая функция

Для пользователя она не отличается от функций сохранения и восстановления контрольных точек.

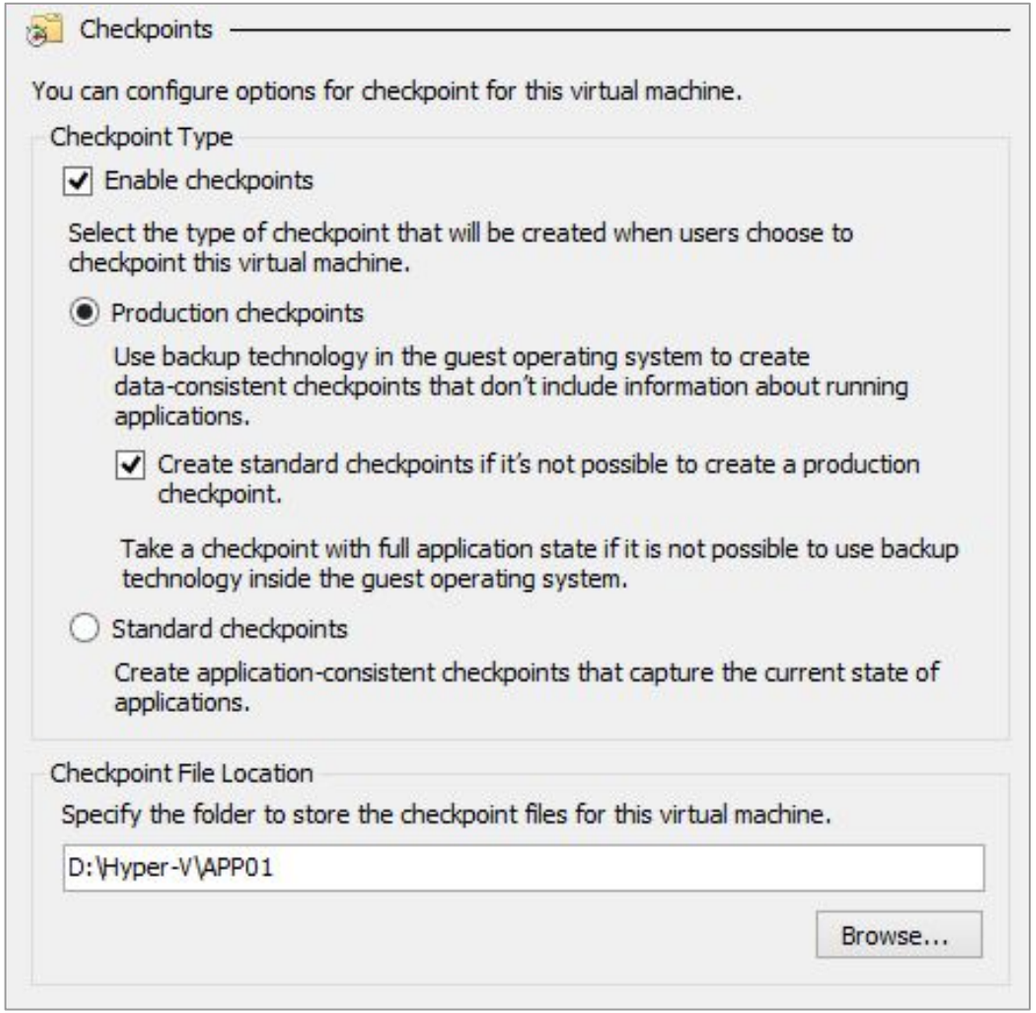
Восстановление контрольной точки аналогично восстановлению чистой резервной копии сервера.

Linux

Виртуальные машины Linux записывают на диск буферы файловой системы, чтобы обеспечить ее целостность в контрольной точке.

Рабочие контрольные точки используются по умолчанию

Новые виртуальные машины будут использовать рабочие контрольные точки, а в случае их недоступности — стандартные контрольные точки.



PowerShell Direct

Безопасное соединение между узлом Hyper-V и гостевой ВМ, позволяющее отправлять командлеты PS и с легкостью выполнять сценарии

В настоящее время поддерживаются гостевые ОС Windows 10/Windows Server 2016 на узлах Windows 10/Windows Server 2016.

Настраивать удаленное или сетевое подключение PS не требуется.

Необходимы только гостевые учетные данные.

От этого узла можно подключиться только к конкретной гостевой системе.

```
Enter-PSSession -VMName VMName
Invoke-Command -VMName VMName -ScriptBlock { Fancy Script }
```

Улучшения Hyper-V Manager

Многочисленные улучшения Hyper-V Server упрощают удаленное управление и устранение неисправностей

Поддержка альтернативных учетных данных

Подключение по IP-адресу

Подключение через Windows Remote Management

Ускорение операций с VHDX благодаря ReFS

Файловая система Resilient File System:

Максимально повышает доступность данных и операций в сети, невзирая на ошибки, обычно приводящие к потере данных или простоям

Быстрое восстановление после повреждения файловой системы без ущерба для доступности.

Устойчивость к повреждениям, вызванным отключением электроэнергии.

Периодическая проверка контрольных сумм для метаданных файловой системы.

Улучшенная защита целостности данных.

ReFS продолжает работать при восстановлении подкаталогов, знает о размещении «потерянных» подкаталогов и автоматически восстанавливает их.

Преимущества интеллектуальной файловой системы: позволяет…

Мгновенно создавать фиксированные диски.

Мгновенно осуществлять объединение дисков.

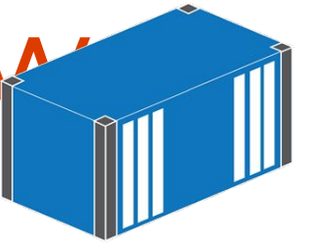
Microsoft

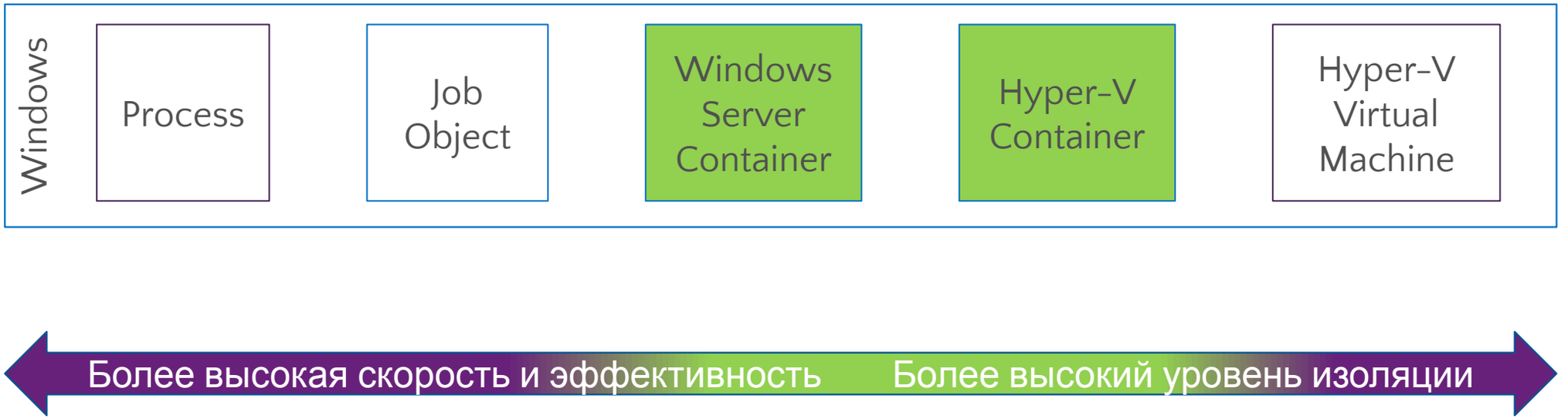
Контейнеры

Александр Шаповал
Microsoft

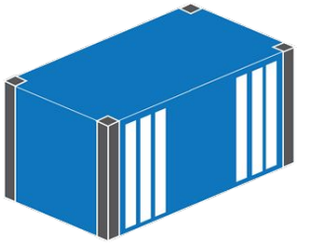
Что такое контейнеры?

Технологии изоляции в Windows

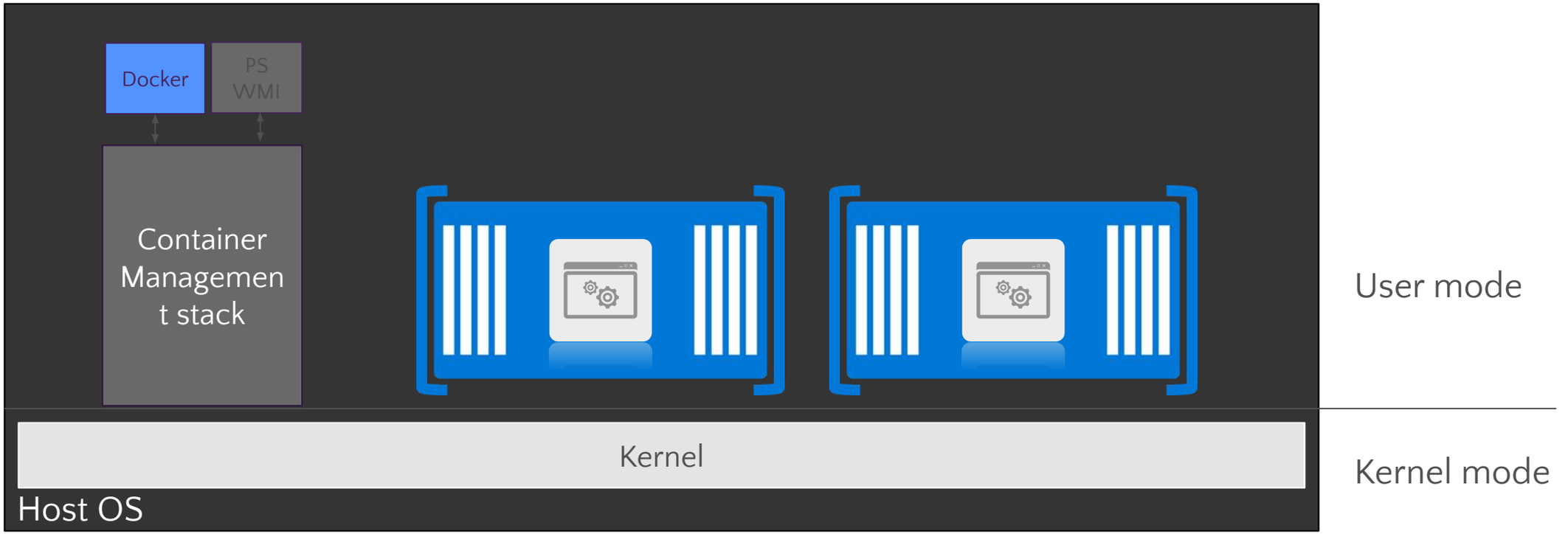




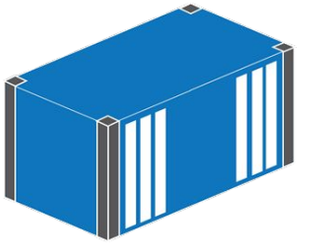
Контейнеры Windows Server



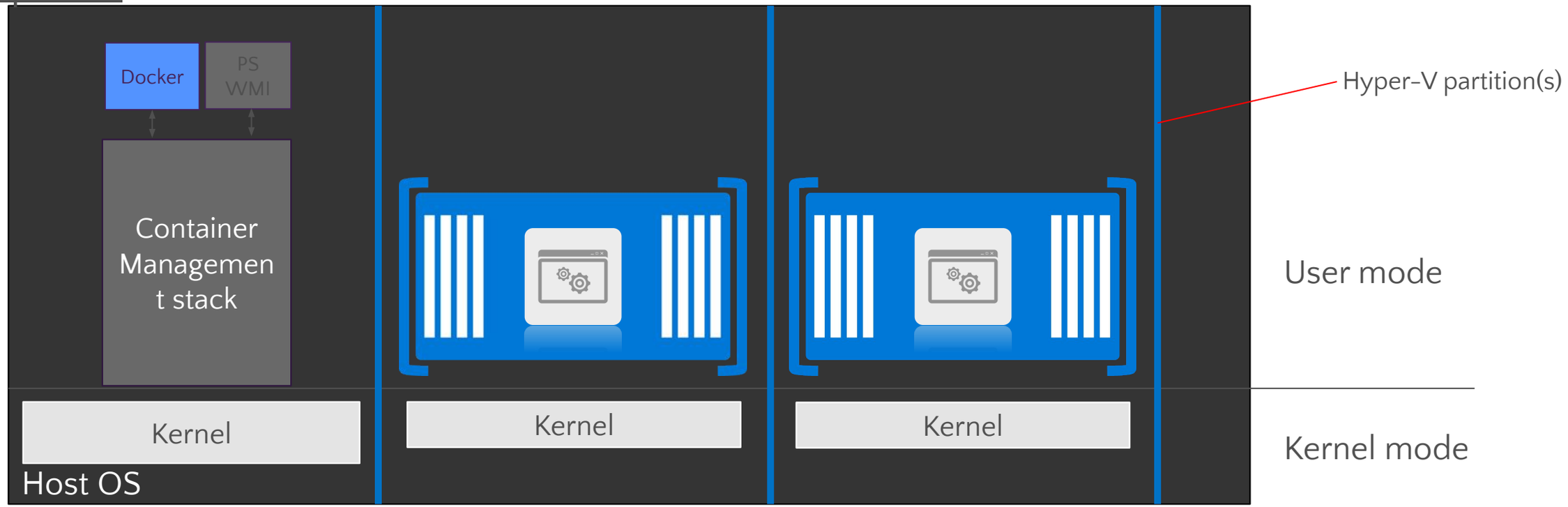
- Изолированная среда выполнения приложений



Контейнеры Hyper-V

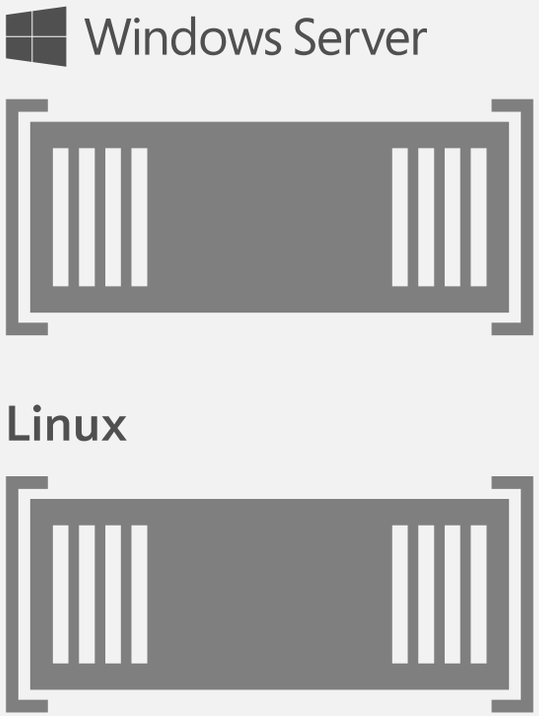


- Изолированная среда выполнения приложений с дополнительным уровнем изоляции, обеспечиваемым Hyper-V

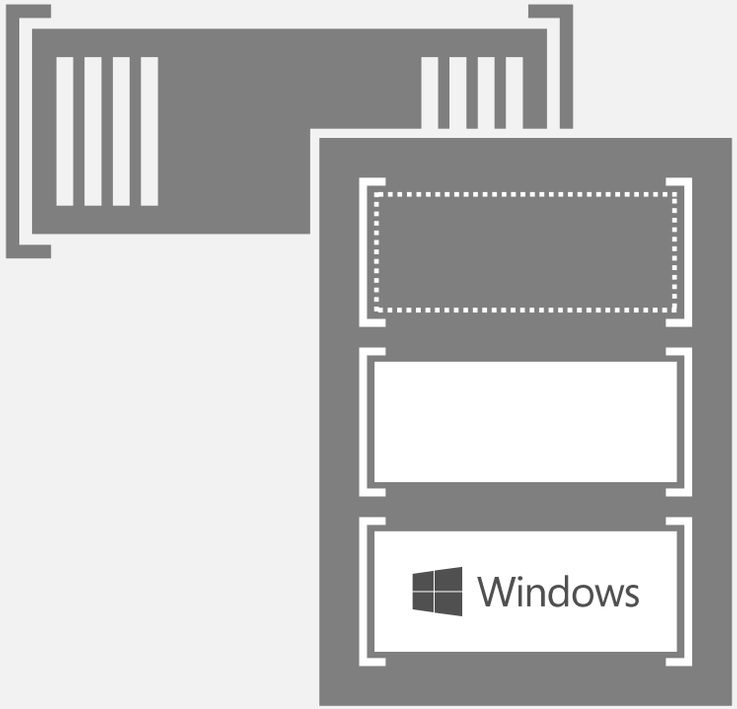


Экосистема контейнеров

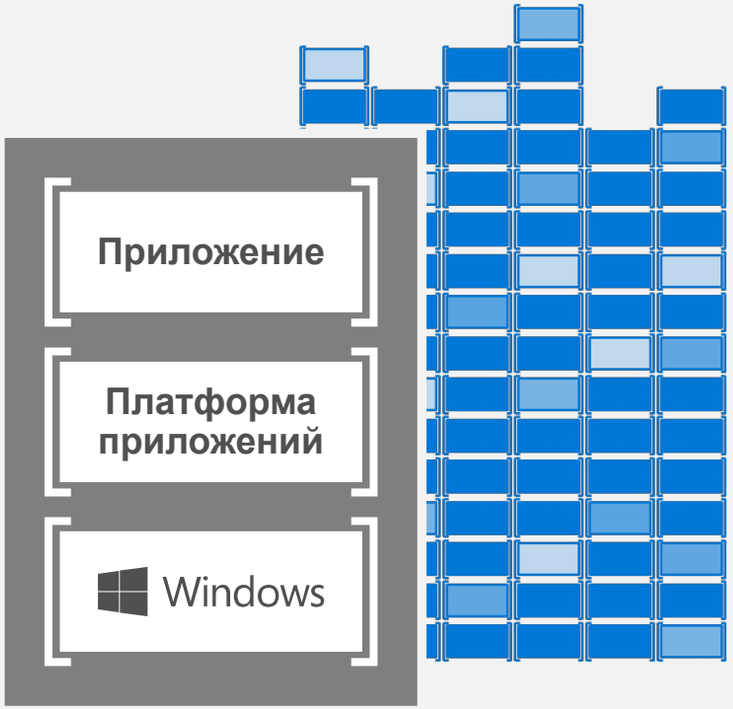
Среда выполнения контейнера



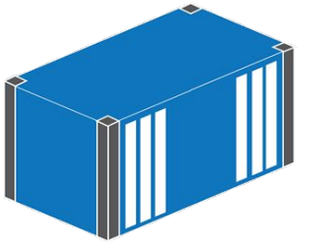
Образы контейнера



Репозиторий образов



Образы контейнеров



```
PS>Get-ContainerImage

Name      Publisher       Version        IsOSImage
------    ----------      --------       ------------
Windows   CN=Microsoft    10.0.10250.0   True
```

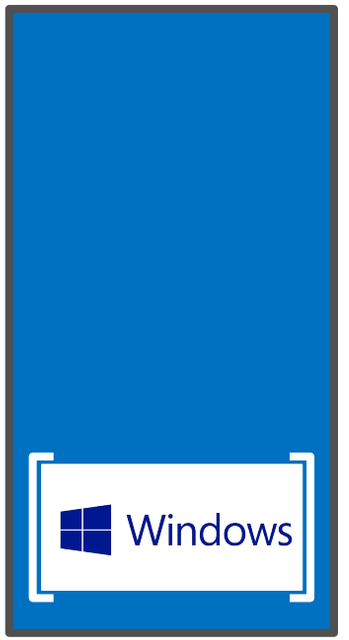
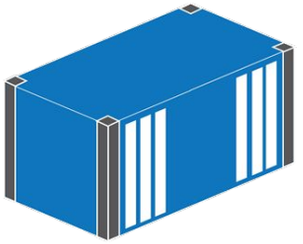
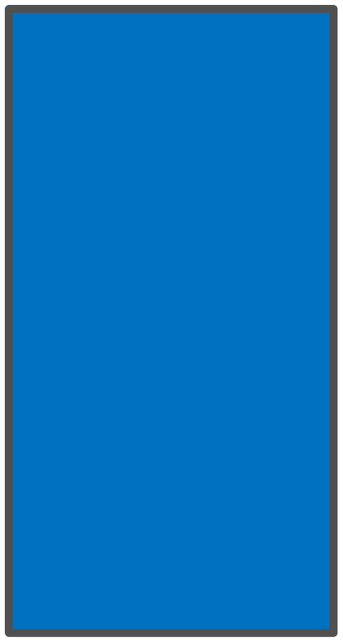


Image Repository

Образы контейнеров



```
PS> New-Container -Name 'Node' -ContainerImageName 'Windows'
```



Container image: Node

Container: Node -OFF

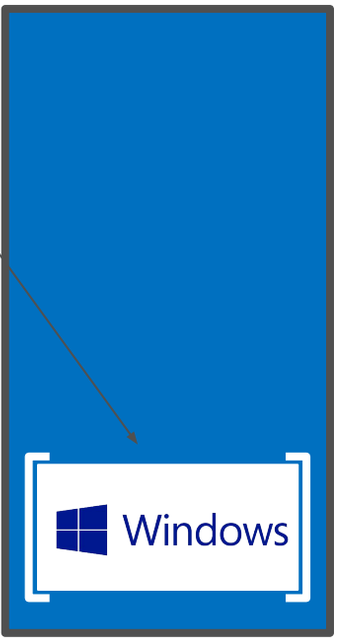
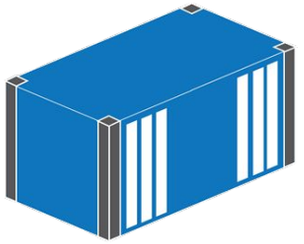
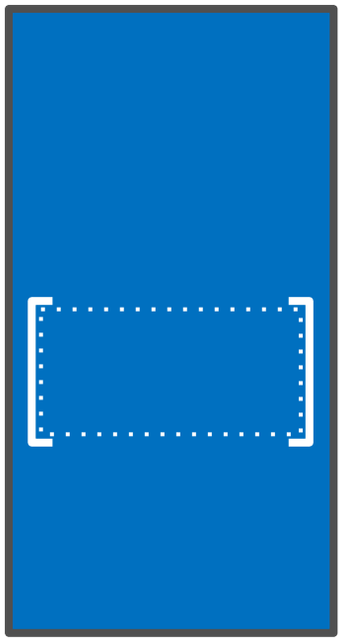


Image Repository

Образы контейнеров



```
PS> New-Container -Name 'Node' -ContainerImageName 'Windows'
PS> Start-Container 'Node'
```



Container image: Node

Container: Node

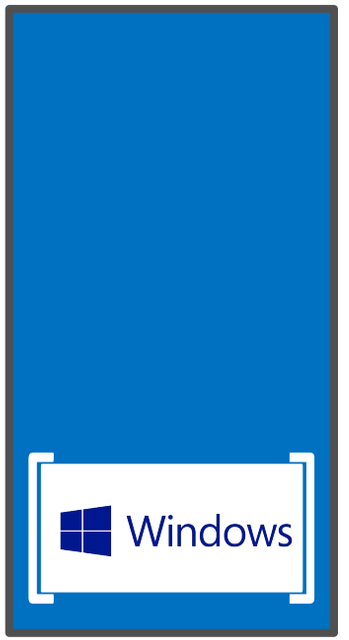
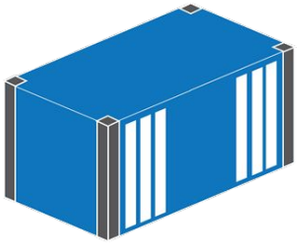
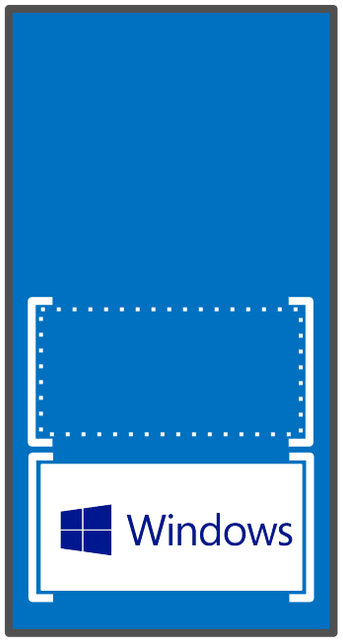


Image Repository

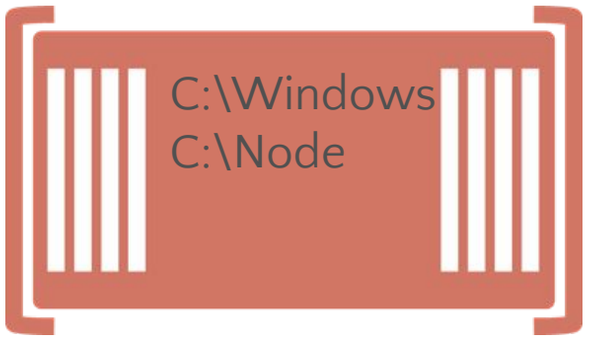
Образы контейнеров



```
PS> New-Container -Name 'Node' -ContainerImageName 'Windows'
PS> Start-Container 'Node'
Inside the container...
[abc-123] PS> cmd /c node.msi
```



Container image: Node



Container: Node

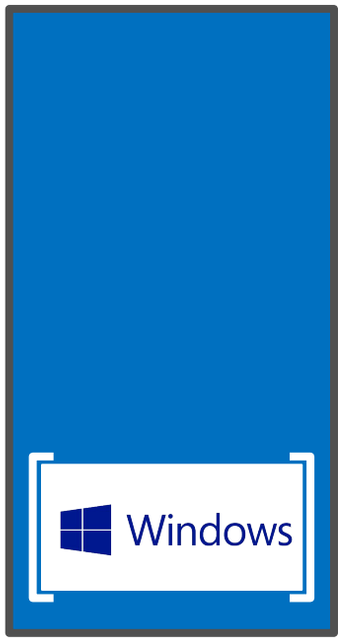
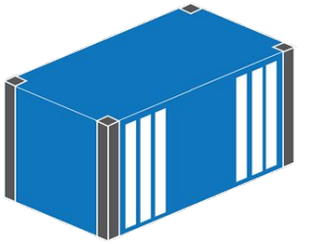
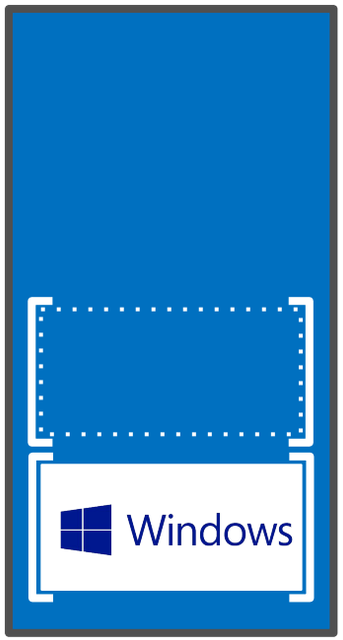


Image Repository

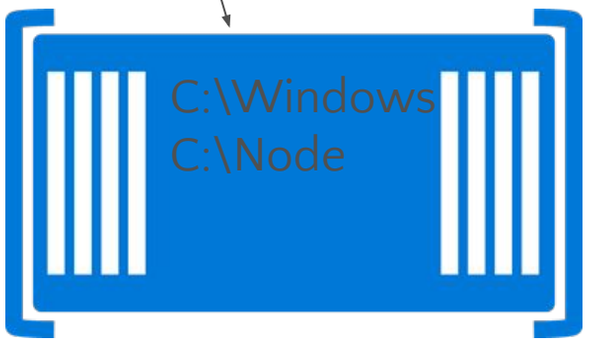
Образы контейнеров



```
PS> New-Container -Name 'Node' -ContainerImageName 'Windows'
PS> Start-Container 'Node'
Inside the container...
[abc-123] PS> cmd /c node.msi
Outside the container...
PS> Stop-Container 'Node'
```



Container image: Node



Container: Node -OFF

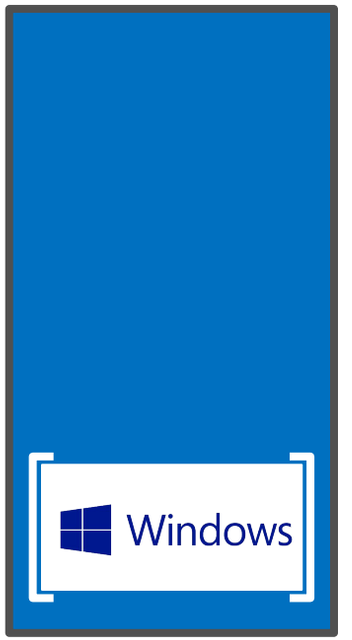
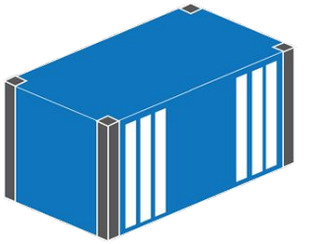
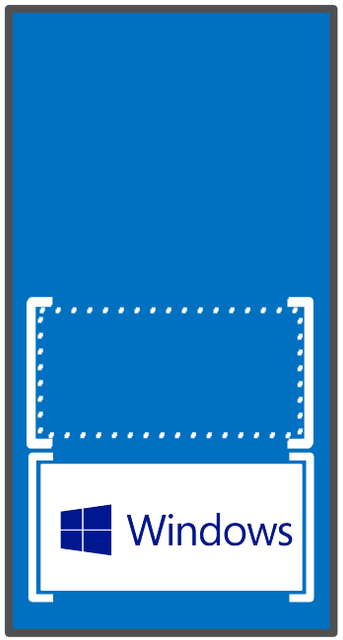


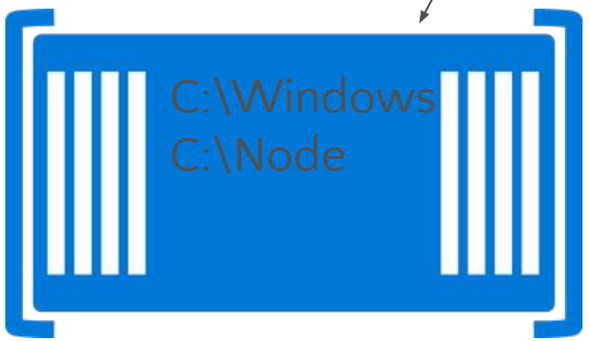
Image Repository

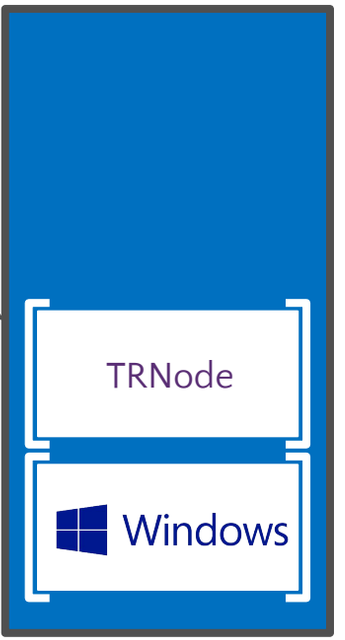
Образы контейнеров



```
PS> New-Container -Name 'Node' -ContainerImageName 'Windows'
PS> Start-Container 'Node'
Inside the container...
[abc-123] PS> cmd /c node.msi
Outside the container...
PS> Stop-Container 'Node'
PS> New-ContainerImage –ContainerName 'Node' –Name 'TRNode'
```





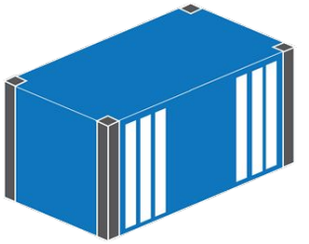


Container image: Node

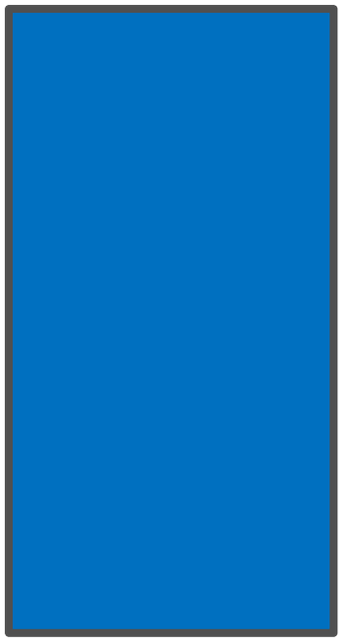
Container: Node -OFF

Image Repository

Образы контейнеров



```
PS> New-Container -Name 'Node' -ContainerImageName 'Windows'
PS> Start-Container 'Node'
Inside the container...
[abc-123] PS> cmd /c node.msi
Outside the container...
PS> Stop-Container 'Node'
PS> New-ContainerImage –ContainerName 'Node' –Name 'TRNode'
PS> New-Container -Name 'Web' –ContainerImageName 'TRNode'
```



Container image: Web

Container: Web -OFF

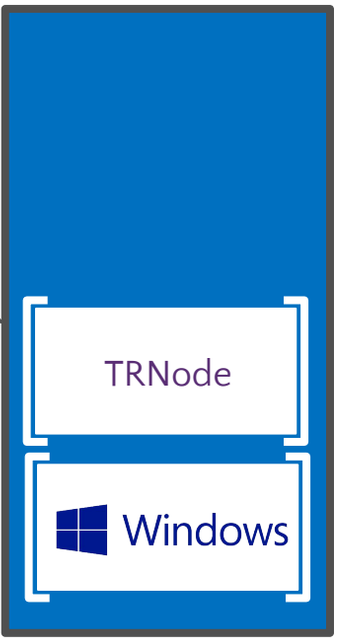
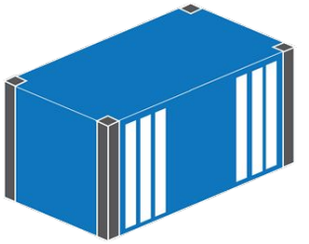
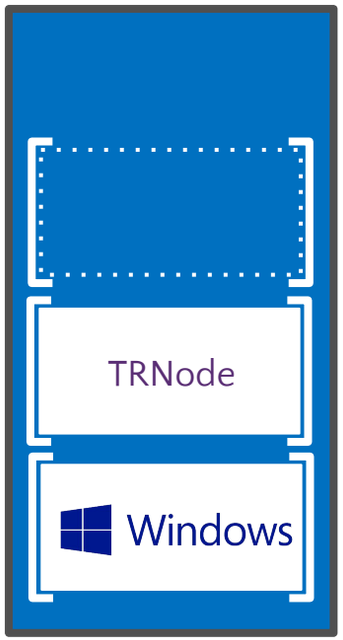


Image Repository

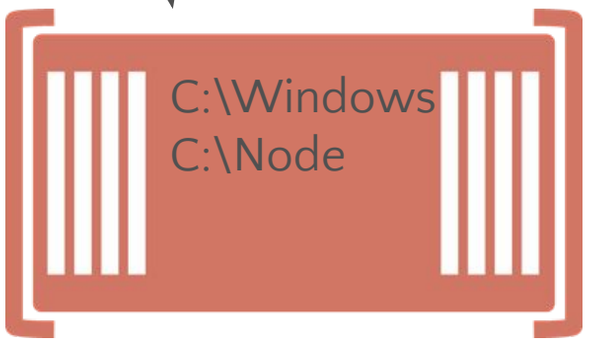
Образы контейнеров



```
PS> New-Container -Name 'Node' -ContainerImageName 'Windows'
PS> Start-Container 'Node'
Inside the container...
[abc-123] PS> cmd /c node.msi
Outside the container...
PS> Stop-Container 'Node'
PS> New-ContainerImage –ContainerName 'Node' –Name 'TRNode'
PS> New-Container -Name 'Web' –ContainerImageName 'TRNode'
PS> Start-Container 'Web'
```



Container image: Web



Container: Web

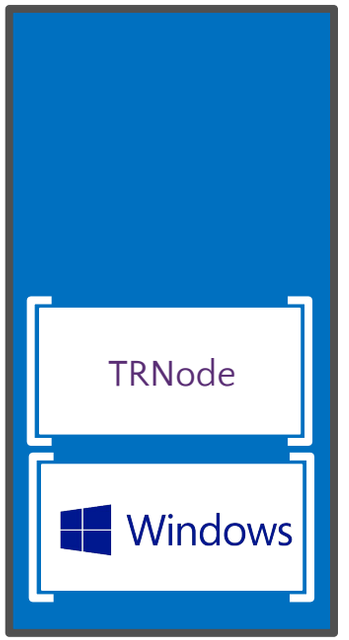


Image Repository

Применение контейнеров в разработке

Процесс разработки с использованием контейнеров

Локальный репозиторий

Платформа приложений

Windows Server

Центральный репозиторий

Процесс разработки с использованием контейнеров

Платформа приложений

Локальный репозиторий

Разработчики могут выбирать необходимые платформы приложений и переносить их из центральных репозиториев в локальную среду

Платформа приложений

Windows Server

Центральный репозиторий

Процесс разработки с использованием контейнеров

Платформа приложений

Windows Server

Локальный репозиторий

Разработчики могут выбирать необходимые платформы приложений и переносить их из центральных репозиториев в локальную среду

Необходимые зависимости идентифицируются автоматически и запрашиваются локально

Платформа приложений

Windows Server

Центральный репозиторий

Процесс разработки с использованием контейнеров

Разработчики используют привычные языки программирования и среды

Платформа приложений

Windows Server

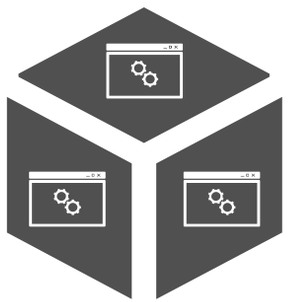
Локальный репозиторий

Платформа приложений

Windows Server

Центральный репозиторий

Процесс разработки с использованием контейнеров



Приложения скомпилированы и собраны в стандартном формате, привычном для разработчиков

Платформа приложений

Windows Server

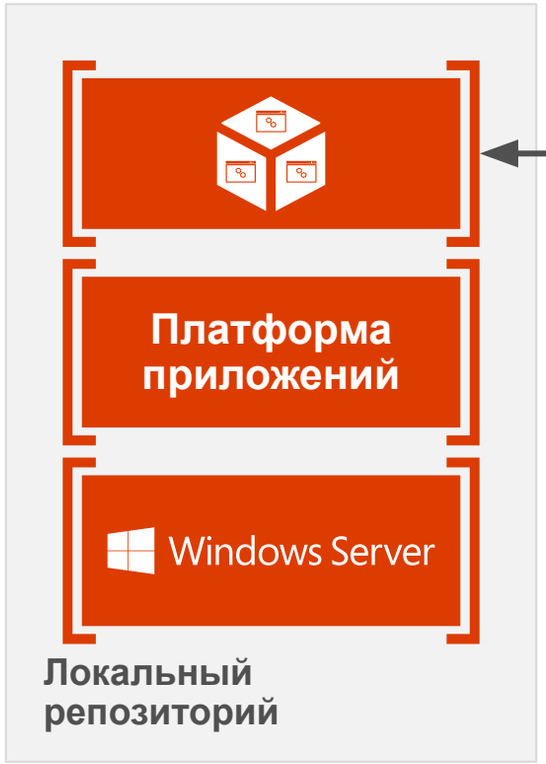
Локальный репозиторий

Платформа приложений

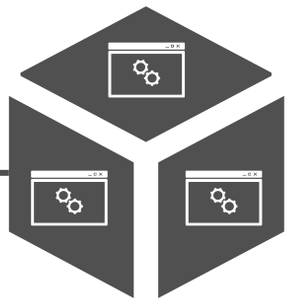
Windows Server

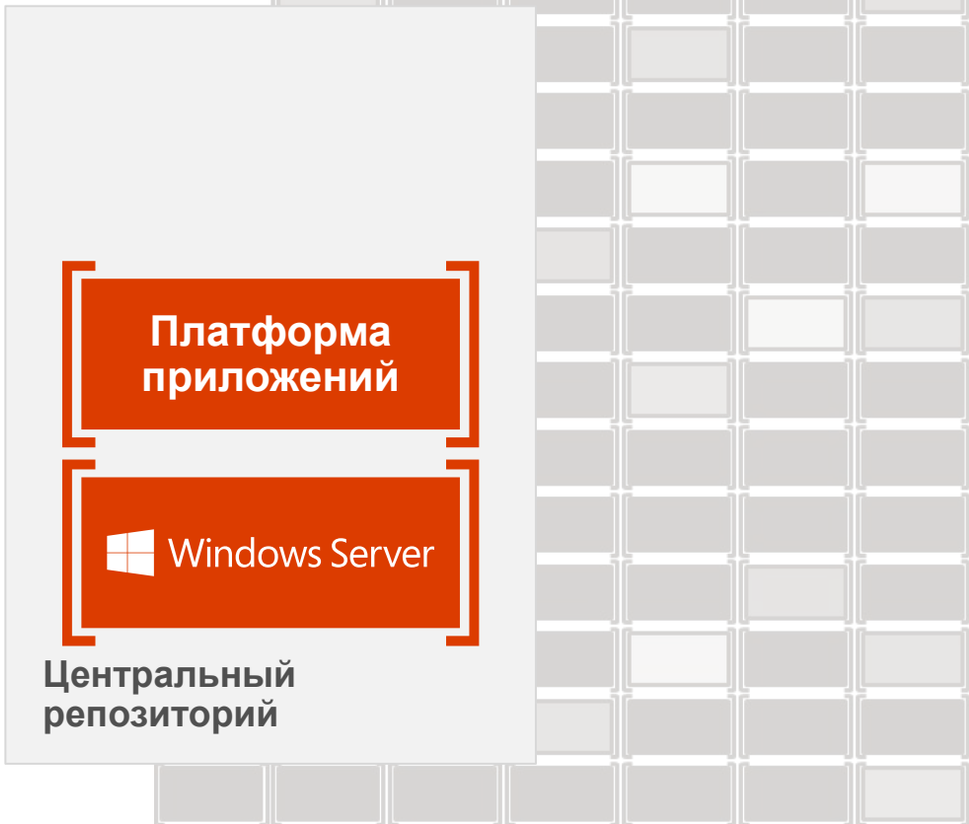
Центральный репозиторий

Процесс разработки с использованием контейнеров

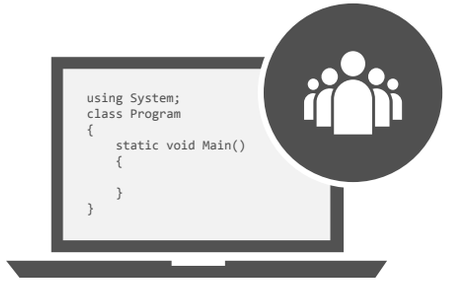


Формируется новый образ контейнера, содержащий созданное разработчиком приложение





Процесс разработки с использованием контейнеров

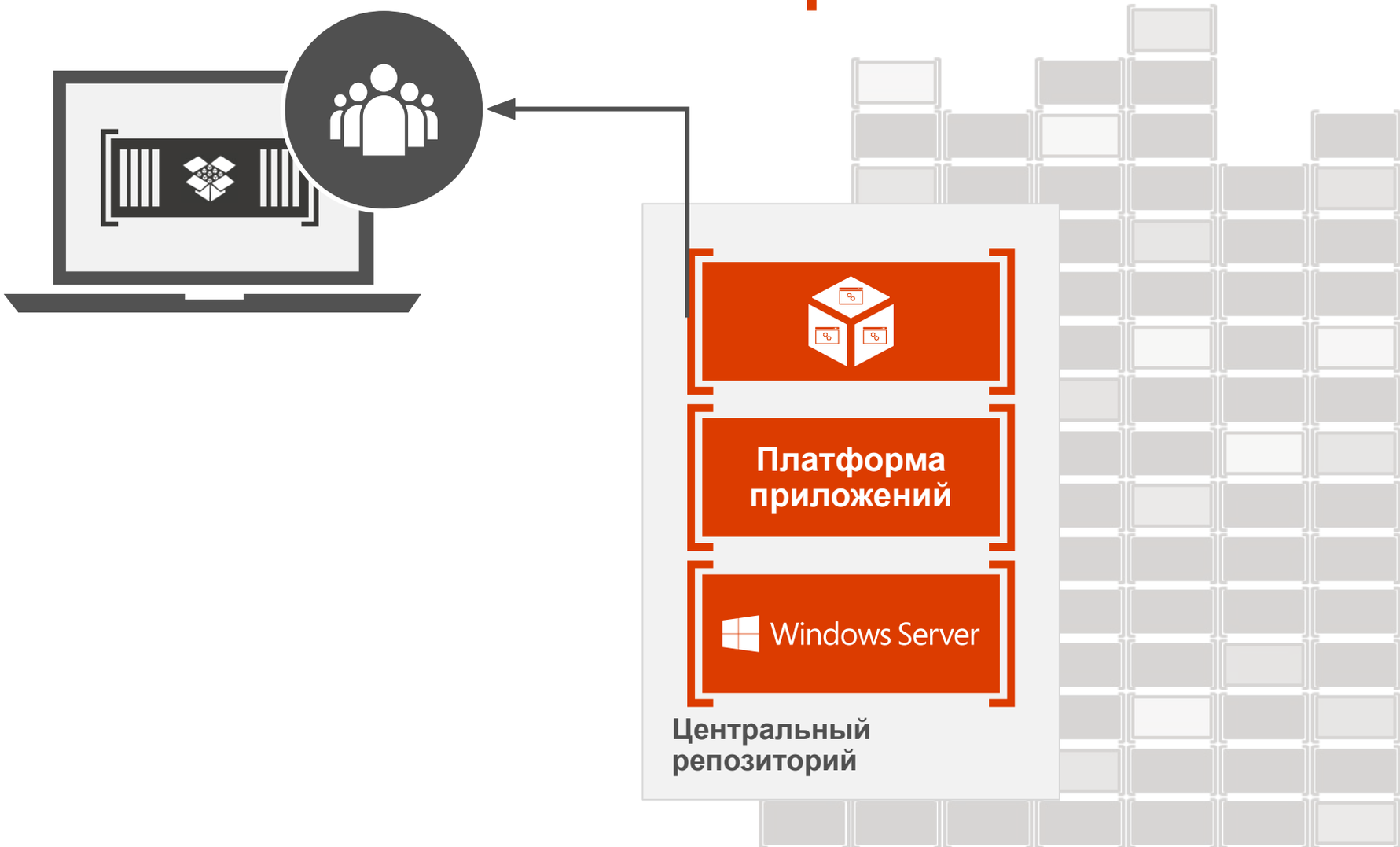


Процесс разработки с использованием контейнеров

Процесс разработки с использованием контейнеров

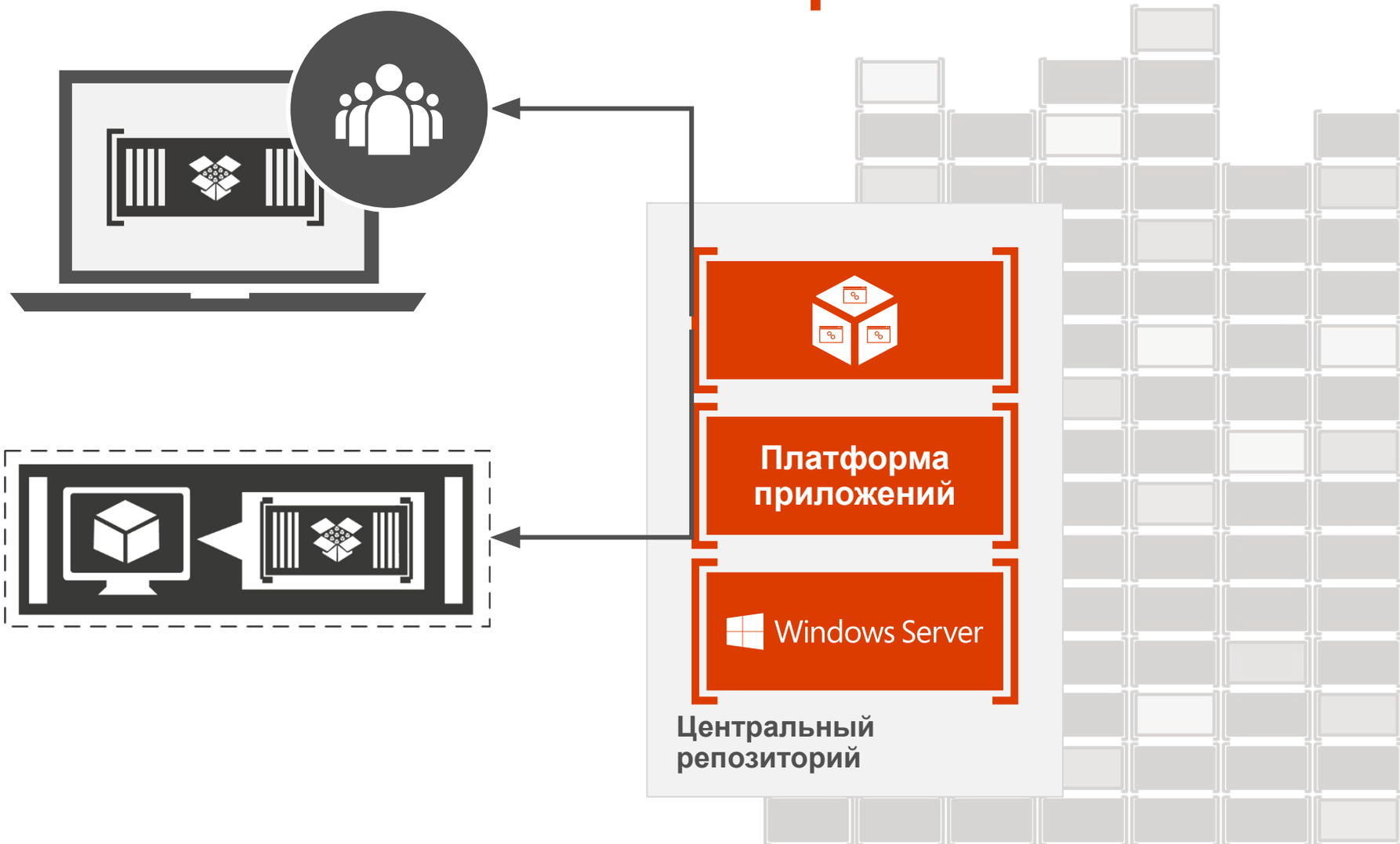
Модульное тестирование

Совместное использование с другими разработчиками

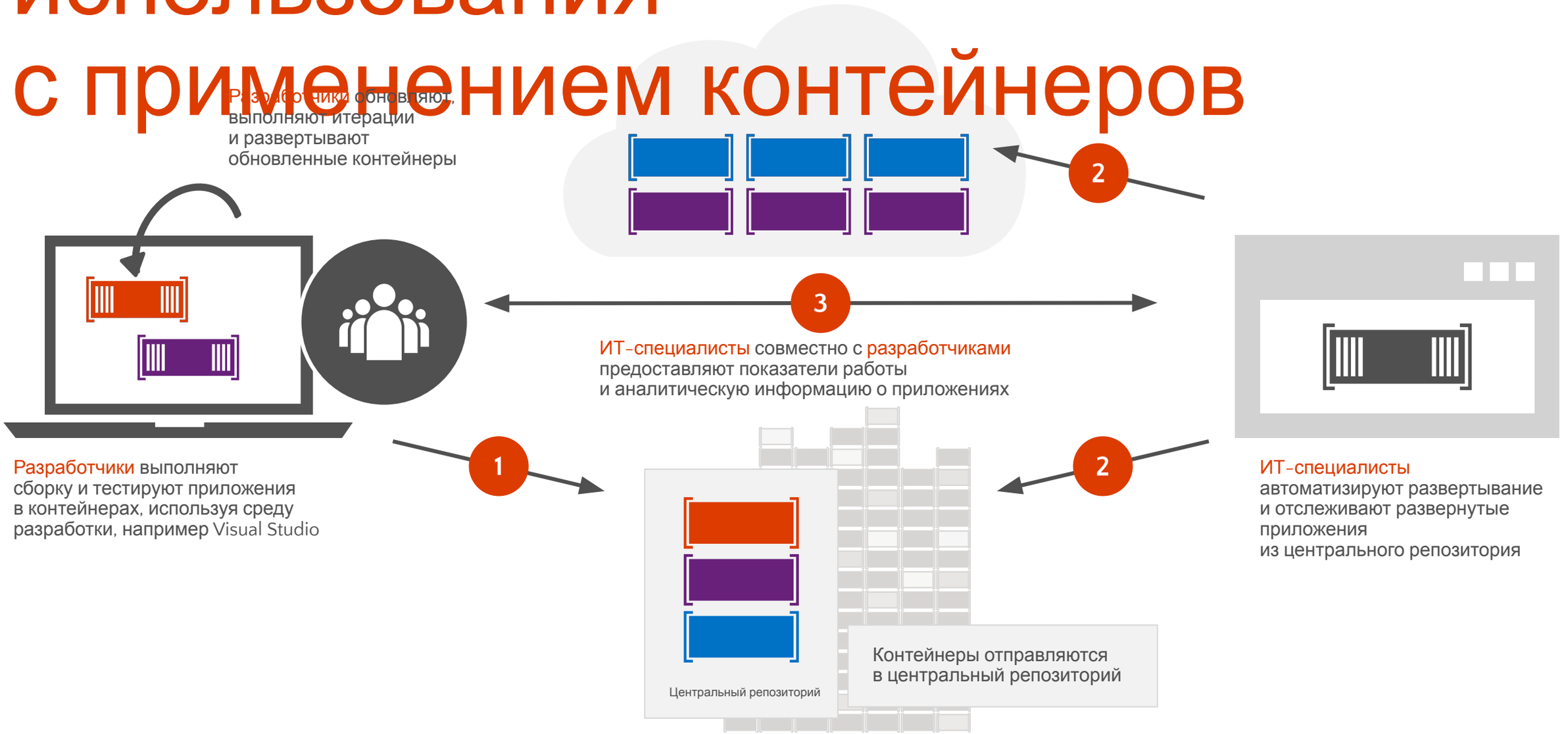


Процесс разработки с использованием контейнеров

- Модульное тестирование
- Совместное использование с другими разработчиками
- Поэтапная интеграция или контроль качества



Процесс разработки и использования с применением контейнеров



Разработчики выполняют сборку и тестируют приложения в контейнерах, используя среду разработки, например Visual Studio

ИТ-специалисты автоматизируют развертывание и отслеживают развернутые приложения из центрального репозитория

Демонстрация
Работа с контейнерами в PowerShell

Варианты использования контейнеров

Варианты использования контейнеров

Характеристики рабочей нагрузки

Горизонтально масштабируемая

Распределенная

С разделением состояний

Быстрая (пере)загрузка

Характеристики развертывания

Эффективное размещение

Мультитенантность

Быстрое развертывание

Широкие возможности автоматизации

Быстрое масштабирование

Распределенные вычисления	Базы данных	Интернет	Прочие задачи	Горизонтальное масштабирование
$f(x)$				

Среды ОС контейнеров

Nano Server

Максимальная оптимизация

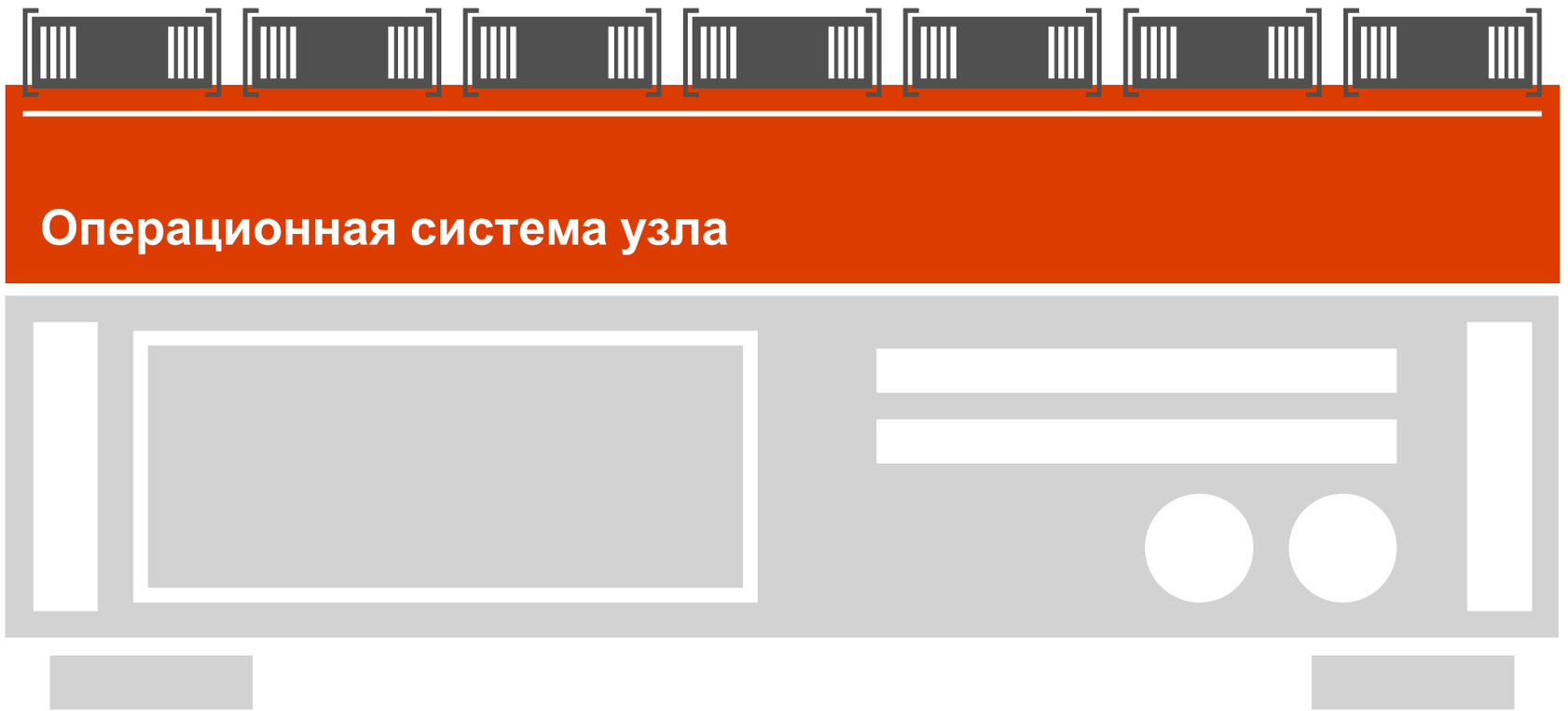
Облачные приложения

Server Core

Высокая совместимость

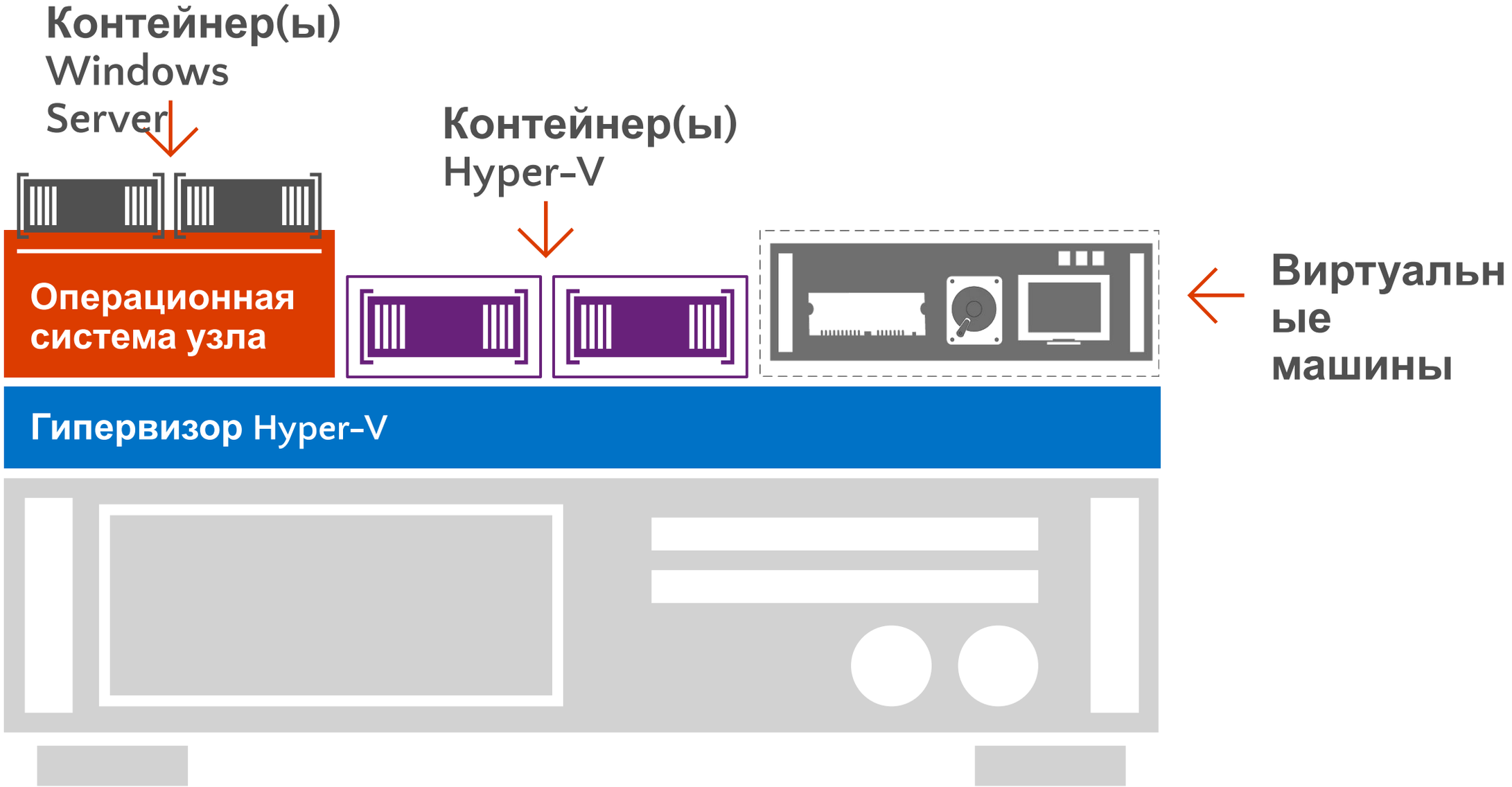
Традиционные приложения

Среда выполнения контейнера

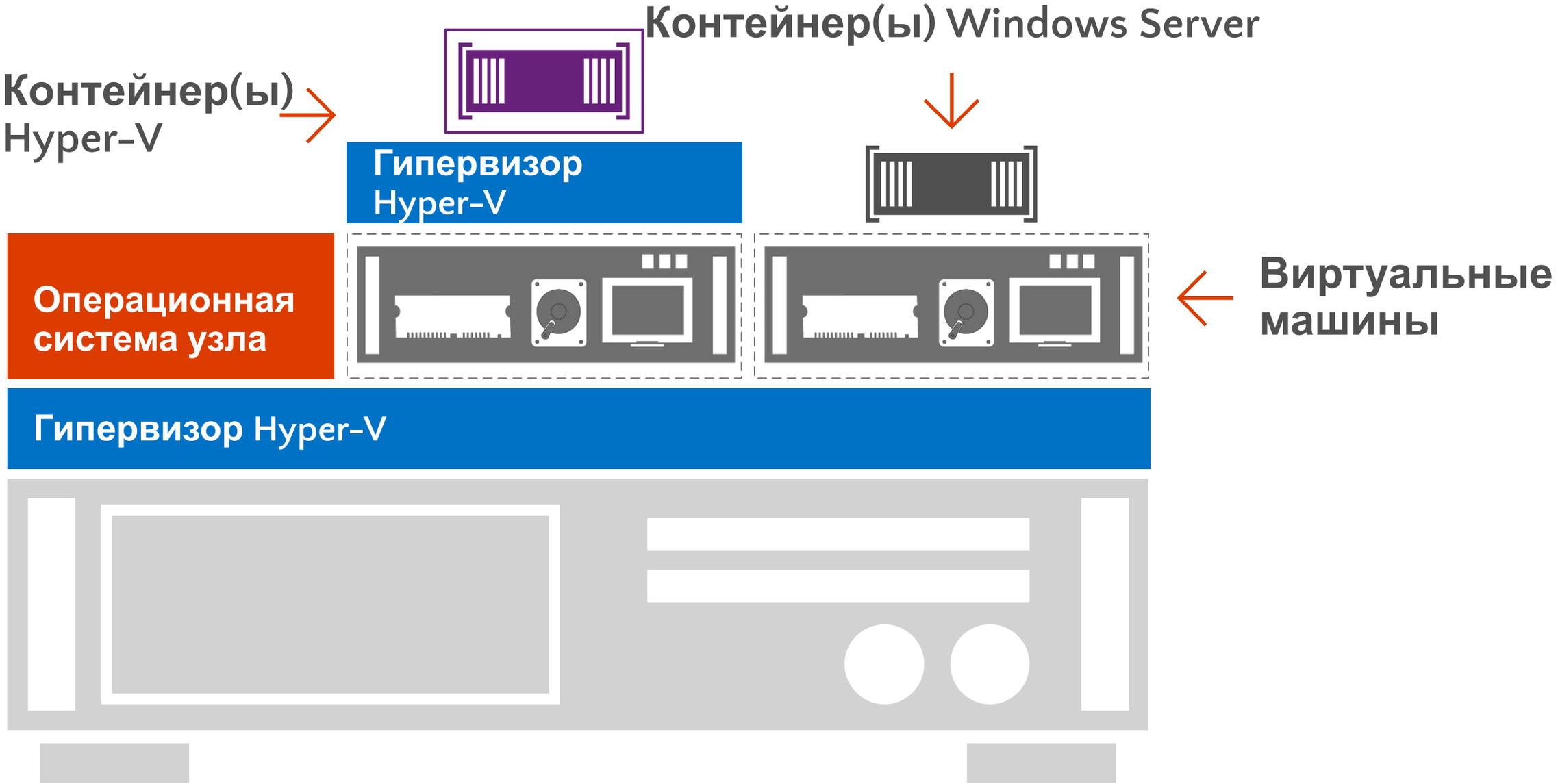


Контейнер(ы)
Windows Server

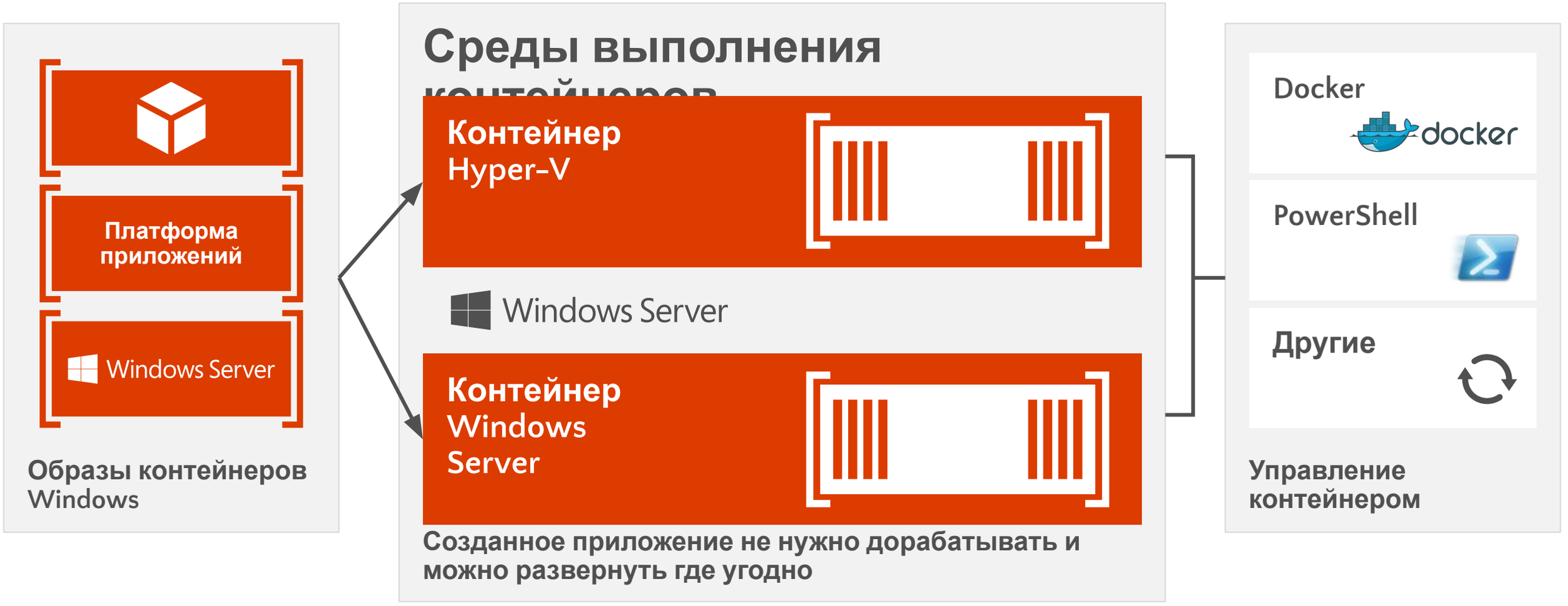
Среда выполнения контейнера



Среда выполнения контейнера



Разработка современных приложений, гибкая изоляция



Microsoft

Инфраструктура хранилищ

Александр Шаповал
Microsoft

Что такое программно-определяемое хранилище?

Что такое SAN на самом деле?

Адаптеры подключения

Устойчивое подключение к внешним источникам посредством iSCSI, FC, FCoE, NFS, SMB.

Контроллеры

«Мозг» SAN — обычно с процессором x86, оперативной памятью и поддержкой важных для предприятий функций (**тонкая подготовка, дедупликация, разделение хранилища на уровни** и т. п.).
Наличие нескольких контроллеров обеспечивает устойчивость.

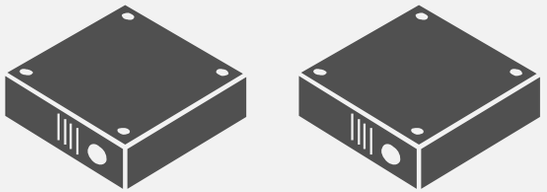
Физические диски

Накопители на основе SSD или HDD, предоставляющие необходимый объем для хранения данных. С помощью контроллеров объединяются в пулы и разделяются на LUN
(простое, с зеркалированием, с контролем четности и т. д.).

Особенности хранилища на базе Windows Server

Адаптеры подключения

Файловые серверы Windows Server поддерживают устойчивые подключения к внешним источникам посредством стандартных сетевых адаптеров 1GBE и 10GBE. Поддерживаются адаптеры до 56GB, 100GB RDMA. Поддерживаются подключения iSCSI, SMB 3.0 и NFS.



Роль контроллера теперь выполняет Windows Server

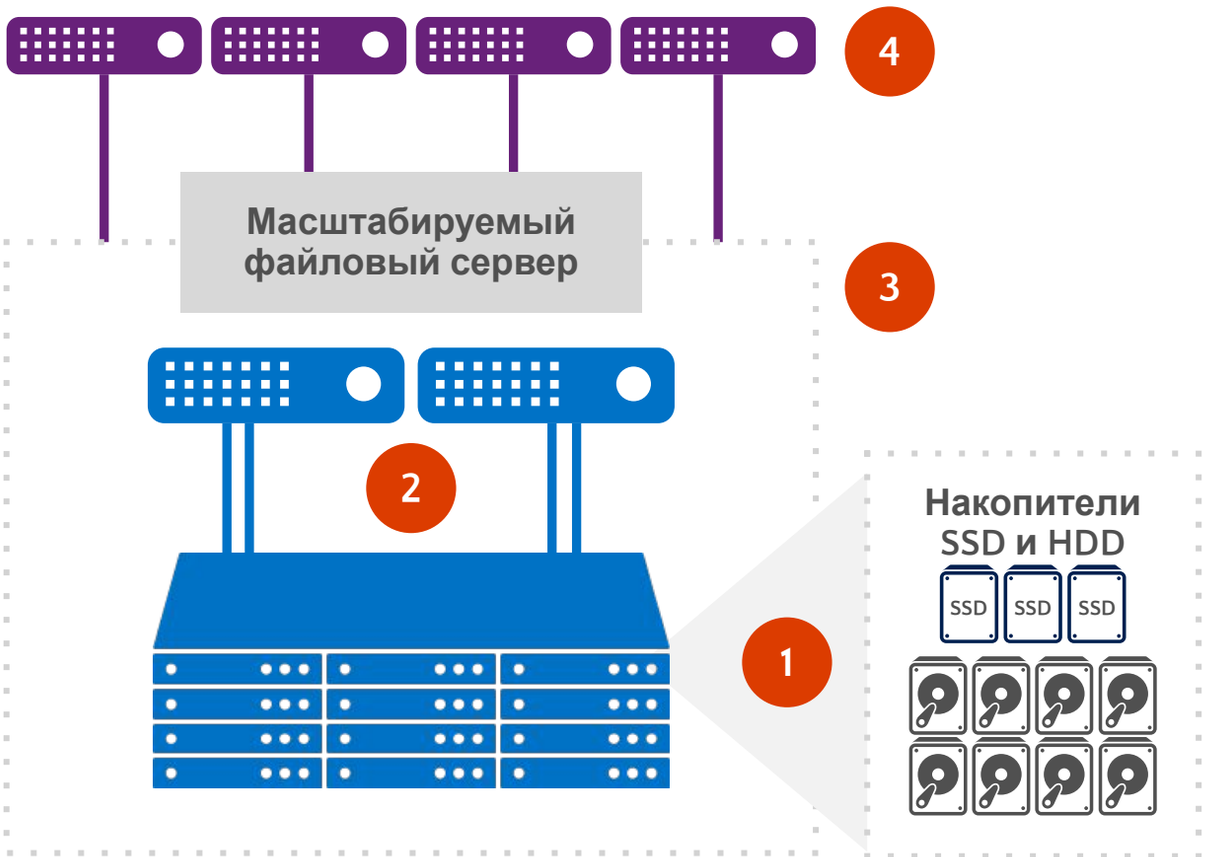
Объединенные в кластеры файловые серверы Windows Server (SOFS) формируют пулы дисков, затем разделяют их на дисковые пространства. Для пространств поддерживаются функции **тонкой подготовки, разделения на уровни** и **дедупликации.** Пространства могут быть простыми, **с зеркалированием** и **с контролем четности.**

Физические диски

Множество способов снижения затрат и упрощения инфраструктуры. HDD и SSD можно разместить на внешней полке JBOD с подключением через SAS, а также в корпусе файлового сервера (контроллера).

Архитектуры хранения

Архитектура Windows Server 2012 R2



1. Стандартная JBOD с накопителями SSD и HDD в отношении 1:4. С помощью дополнительных JBOD емкость можно увеличить.

2. До 8 стандартных серверов x86 под управлением Windows Server 2012 R2, подключенных к JBOD посредством SAS 6 Гб/12 Гб.

3.
- Сборка кластера Windows Server
- Включение Storage Spaces
- Создание пула носителей
- Создание дисковых пространств на основе пула
- Создание масштабируемого файлового сервера
- Создание непрерывно доступных файловых ресурсов на основе пространств

4. Файловые ресурсы служат хранилищами для узлов Hyper-V; доступ осуществляется посредством SMB 3.0. SMB Direct (RDMA) и SMB Multichannel обеспечивают высочайшую производительность. Поддержка скорости передачи данных более 56 Гбит/с.

Создание многоуровневых хранилищ на основе пространств

Оптимизация эффективности дисковых пространств

Пул дисков состоит из высокопроизводительных SSD и HDD большого объема

Механизмы передачи фрагментов файлов автоматически перемещают «горячие» данные на SSD, а «холодные» — на HDD

Кэширование с обратной записью отрабатывает на уровне SSD случайные операции записи, характерные для виртуальных развертываний

Администраторы могут вручную закреплять «горячие» файлы за SSD-накопителями, чтобы повысить производительность

Новые командлеты PowerShell для управления уровнями хранилища

Надежность дисковых пространств

Зеркалирование для обеспечения устойчивости

Зеркалирование с двумя копиями обеспечивает устойчивость в случае отказа одного диска

Зеркалирование с тремя копиями обеспечивает устойчивость в случае отказа двух дисков

Подходит для случайных операций ввода/вывода

Устойчивость с контролем четности

Кодирование LRC позволяет сократить расходы на хранение данных

Устойчивость к сбоям одного или двух дисков

Подходит для масштабных операций последовательного ввода/вывода

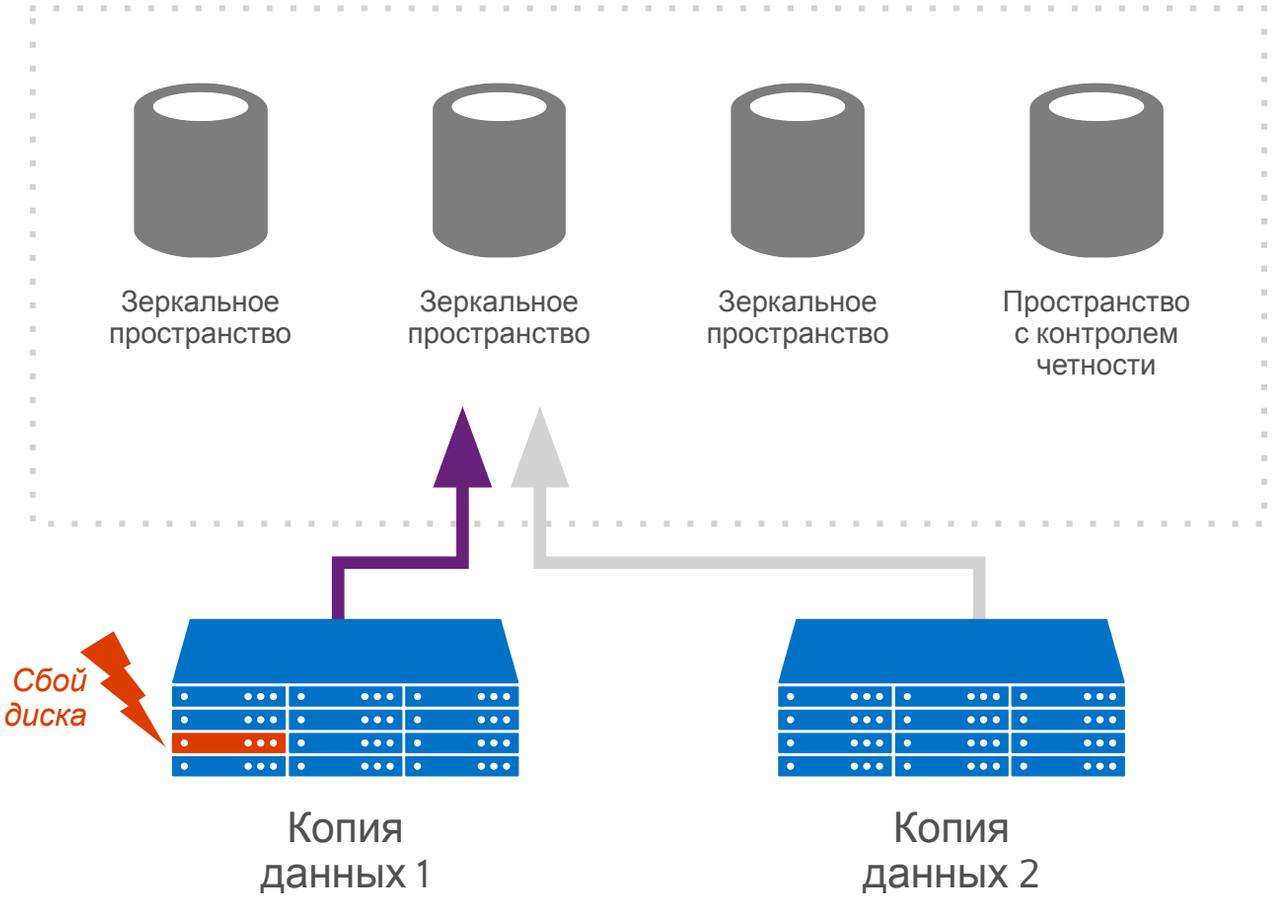
Отслеживание состояния блока накопителей

Устойчивость к сбоям всего блока накопителей

Параллельное перестроение

Псевдослучайное распределение с весами, подобранными для оптимальной загрузки менее используемых дисков

Воссозданное пространство распределяется и перестраивается параллельно



Windows Server 2016 — новая архитектура

Конвергентная (дезагрегированная) архитектура с технологией

Архитектура поддерживает независимое масштабирование кластеров Hyper-V (вычислительные ресурсы) и кластеров масштабируемых файловых серверов (SOFS; хранилища)

1. Стандартные серверы x86 с **локальными** накопителями SSD и HDD. Серверы соединены каналами 10GBE. Поддержка дисков SATA и NVMe.
   - Сборка кластера Windows Server
   - Включение Storage Spaces Direct
   - Создание пула носителей
   - Создание дисковых пространств на основе пула
   - Создание масштабируемого файлового сервера
   - Создание непрерывно доступных файловых ресурсов на основе дисковых пространств
   - Оптимизация для Storage Spaces Direct

2. Файловые ресурсы служат хранилищами для узлов Hyper-V; доступ осуществляется посредством SMB 3.0. SMB Direct (RDMA) и SMB Multichannel обеспечивают высочайшую производительность. Поддержка скорости передачи данных более 56 Гбит/с.

Windows Server 2016 — новая архитектура

Гиперконвергеная архитектура с технологией Storage Spaces Direct

Стек гиперконвергентных технологий

1. Стандартные серверы x86 с **локальными** накопителями SSD и HDD. Серверы соединены каналами 10GBE. Поддержка дисков SATA и NVMe.
   - Сборка кластера Hyper-V
   - Включение Storage Spaces Direct
   - Создание пула носителей
   - Создание дисковых пространств на основе пула
   - Создание общих томов кластера
   - Оптимизация для Storage Spaces Direct

2. Вычислительные узлы и хранилище масштабируются и управляются совместно. Как правило, масштабируемые развертывания малого и среднего размера.

Факторы эффективности хранилища

Качество обслуживания (QoS) для хранилища

Контроль и мониторинг производительности хранилища

Доступное из коробки решение

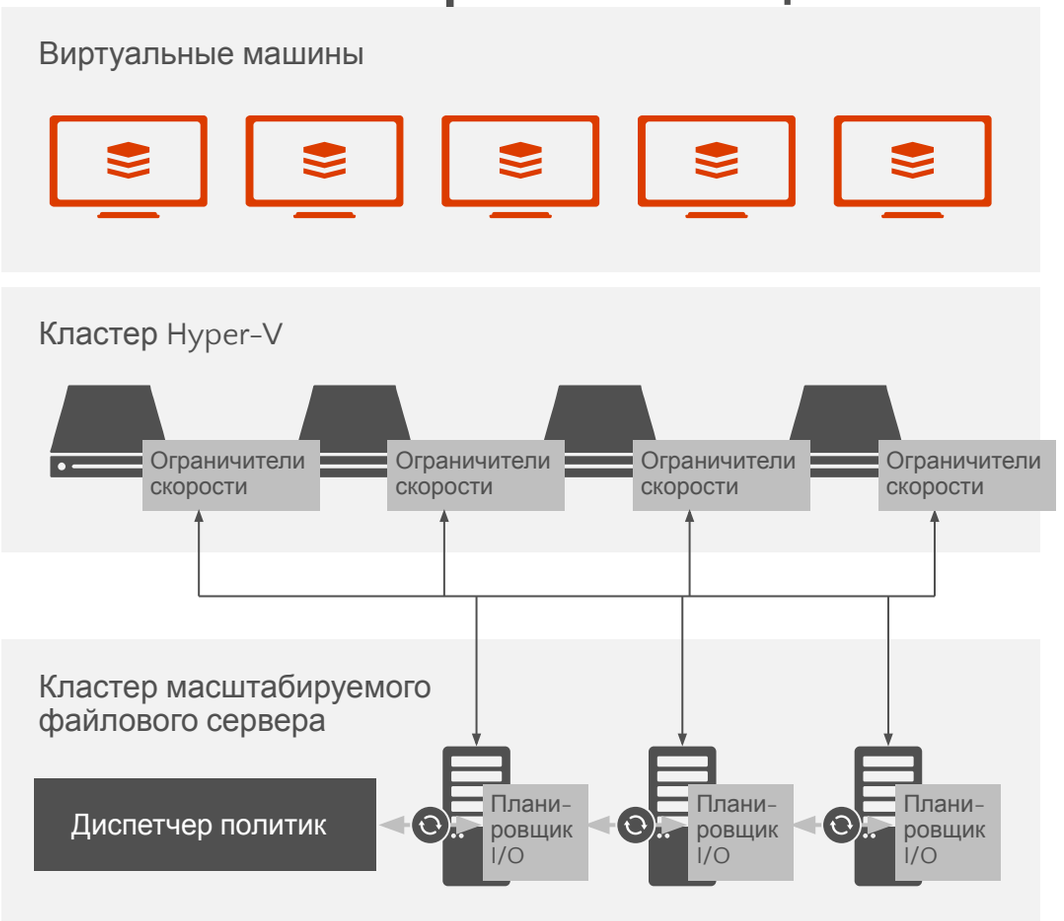
- Поддерживается по умолчанию для масштабируемого файлового сервера
- Автоматические метрики для вирт. жестких дисков, ВМ, узлов и томов
- Включает нормализованные операции ввода/вывода и задержку

Гибкие и настраиваемые политики

- Политики для отдельных вирт. жестких дисков, ВМ, служб и клиентов
- Ограничение количества операций ввода/вывода в секунду сверху и снизу
- Справедливое распределение в рамках политик

Управление

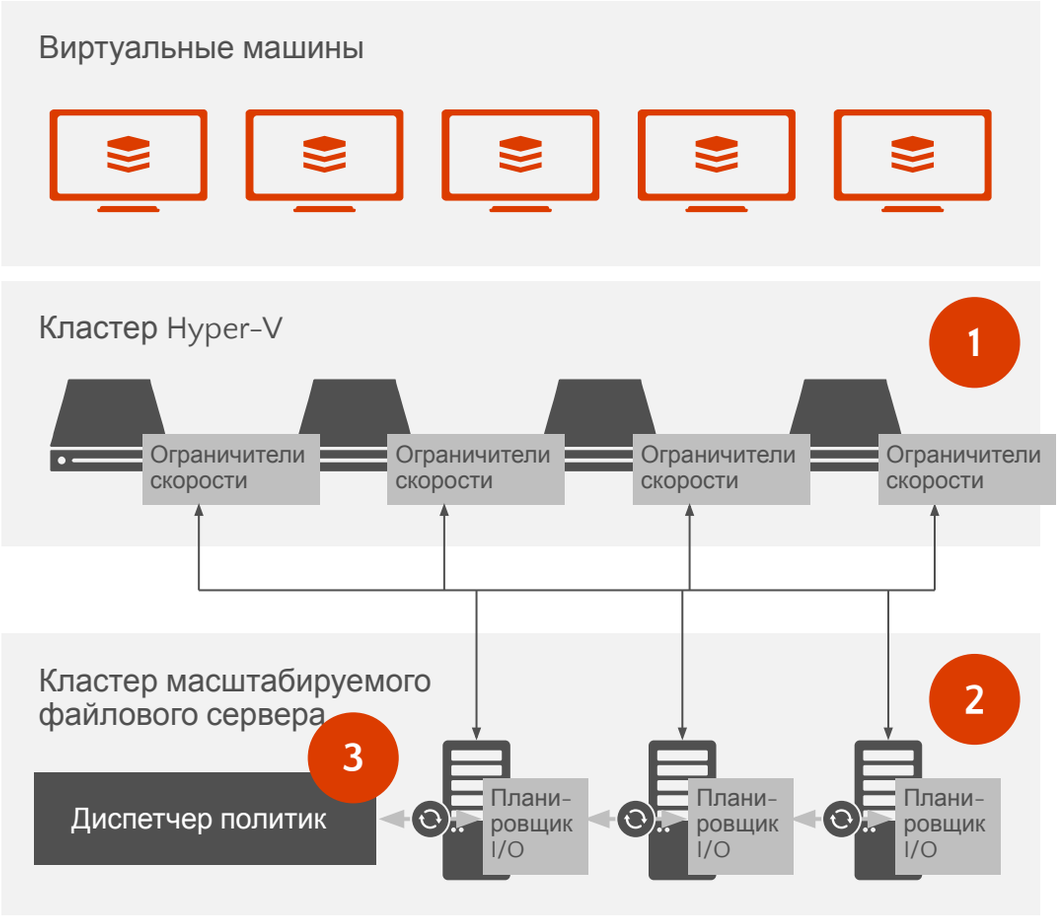
- System Center VMM и Ops Manager
- Встроенная PowerShell для Hyper-V и SoFS



Качество обслуживания для хранилища

Компоненты

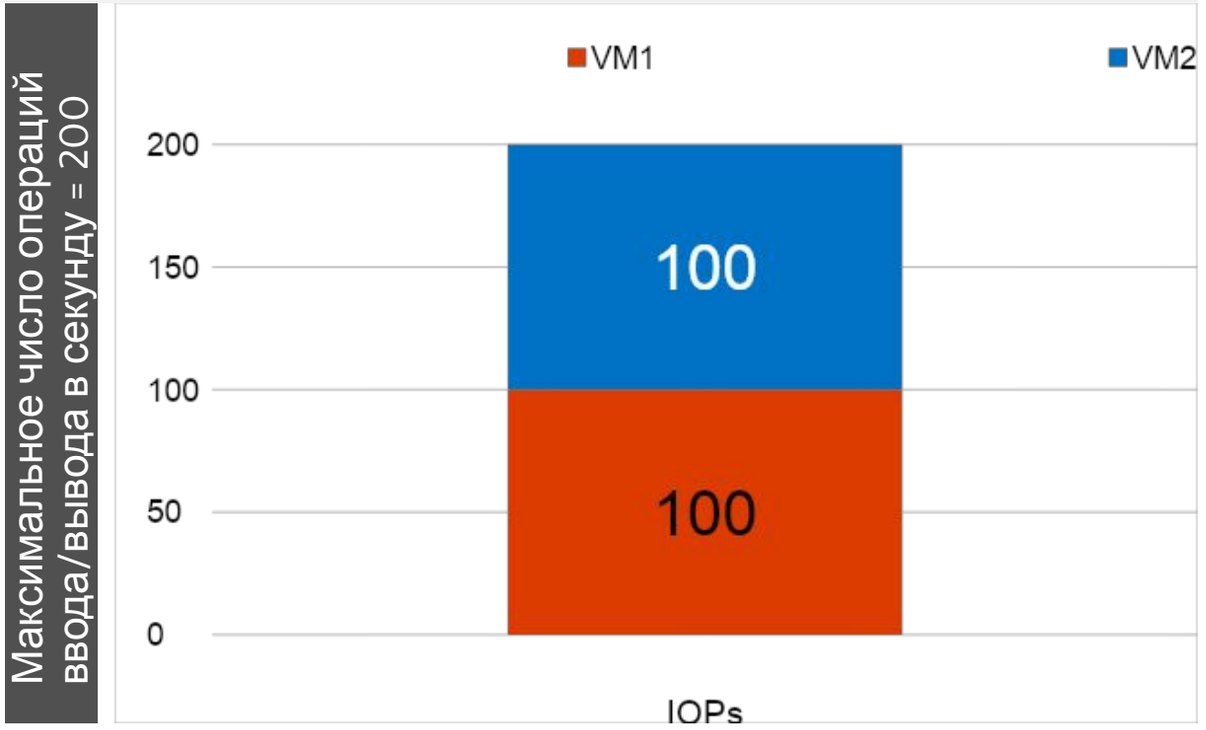
1. Профилировщик и **ограничитель скорости** на вычислительных узлах Hyper-V
2. **Планировщик операций ввода/вывода** распределен между узлами хранения
3. Централизованный **диспетчер политик** на кластере масштабируемого файлового сервера



Типы политик качества обслуживания для хранилищ

Один экземпляр

- Ресурсы распределены между ВМ
- Идеально подходит для представления кластеризованной рабочей нагрузки, приложения или клиента



Несколько экземпляров

- Все ВМ выполняют одну задачу
- Идеально подходит для создания уровней производительности для ВМ

Политики на основе PowerShell

```
# Deployment – Create policy (on File Server)
New-StorageQosPolicy –CimSession FS -Name SilverVM -PolicyType MultiInstance
-MaximumIops 200

# Deployment – Assign policy to VMs (on Hyper-V Host)
$Policy = Get-StorageQosPolicy –CimSession FS -Name SilverVM
Get-VM -Name VMName* | Get-VMHardDiskDrive | Set-VMHardDiskDrive –QoSPolicy $Policy

# Monitoring – Retrieve all flows (on File Server)
Get-StorageQosFlow

# Monitoring – Retrieve flows using the policy (on File Server)
Get-StorageQosPolicy -Name SilverVM | Get-StorageQosFlow
```

Дедупликация в Windows Server 2016

Возможности	Windows Server 2012 R2	Windows Server 2016
Изменение размера томов	Для масштабирования распределите файлы между несколькими томами, не более 8–10 ТБ	Используйте необходимый размер, до 64 ТБ
Оптимизация	Одно задание на том Один ЦП и одна очередь ввода/вывода	Несколько потоков на том Все файлы оптимизируются параллельно Автоматическая балансировка нагрузки для очередей ввода и ресурсов
Поддержка резервного копирования	Настройка отдельных томов и узлов вручную с помощью PowerShell	Настройка задается в пользовательском интерфейсе или через PowerShell

И другие возможности: интерфейсы SMAPI, поддержка последовательного обновления, поддержка Nano Server, встроенный в CSV механизм кэширования для оптимизации загрузки памяти, поддержка Defender…

Реплика хранилища

Реплика хранилища

Защита ключевых данных и рабочих нагрузок

Синхронная репликация

Независимое от хранилища зеркалирование данных на физических накопителях с защитой томов от сбоев гарантирует полную сохранность данных на уровне томов.

Повышение устойчивости

Открывает новые способы аварийного восстановления между кластерами в пределах города, а также географического распределения отказоустойчивых кластеров для автоматизации высокой доступности.

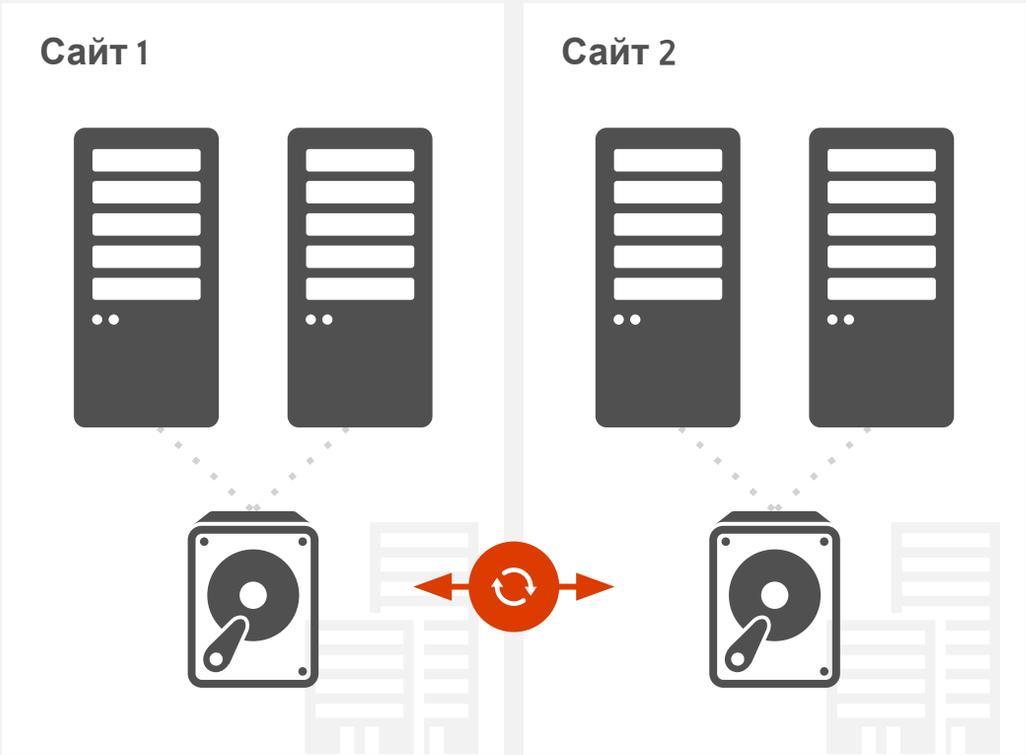
Комплексное решение

Законченное решение для хранения и кластеризации, включая Hyper-V, реплику хранилища, дисковые пространства, кластер, масштабируемый файловый сервер, SMB3, дедупликацию, файловую систему ReFS, NTFS и Windows PowerShell.

Упрощенное управление

Графические инструменты управления отдельными узлами и кластерами в Failover Cluster Manager и Azure Site Recovery.

Географически распределенные кластеры и передача данных между кластерами



Реплика хранилища

Синхронный и асинхронный режимы

Режим	Развертывание	Схема	Этапы
Синхронный RPO без потерь данных	• Критически важные приложения • Локальные и географически распределенные системы • Малое расстояние (< 5 мс, обычно < 30 км) • Обычно по выделенному соединению • Улучшенная пропускная способность		1. Запись приложения 2. Операция записи регистрируется в журнале, данные реплицируются на удаленный сайт 3. Регистрация записи данных на удаленном сайте в журнале 4. Подтверждение от удаленного сайта 5. Запись приложения подтверждена t, t[1]: Данные записываются на том, для журналов всегда используется сквозная запись
Асинхронный метод Практически нулевая потеря данных (зависит от множества факторов) для RPO	• Некритические приложения • В пределах региона/страны • Неограниченное расстояние • Обычно через глобальную сеть		1. Запись приложения 2. Регистрация записи данных в журнале 3. Запись приложения подтверждена 4. Данные реплицируются на удаленный сайт 5. Регистрация записи данных на удаленном сайте в журнале 6. Подтверждение от удаленного сайта t, t[1]: Данные записываются на том, для журналов всегда используется сквозная запись

Рекомендации для синхронного режима

Задержка в сети

≤ 5 мс в среднем

- При передаче данных со скоростью света в вакууме за 5 мс сигнал пройдет ~1500 км
- В реальности скорость сигнала в оптоволоконном кабеле меньше на ~ 35%, сигнал проходит через коммутаторы, маршрутизаторы, межсетевые экраны и т. п.
- Финансовые ограничения, доступность

Результат: для большинства клиентов дистанция составляет 30–50 км

Пропускная способность сети

Сеть ≥1 Гбит/с — на всех участках — для начала между серверами (требуется Windows Server logo 1 ГБ NIC)

Зависит от интенсивности ввода/вывода и загруженности канала (SR может быть не единственным трафиком для сайта DR)

Изучите специфику операций ввода/вывода (125 МБ/с для операций ввода/вывода = ~1 ГБ/с трафика в сети)

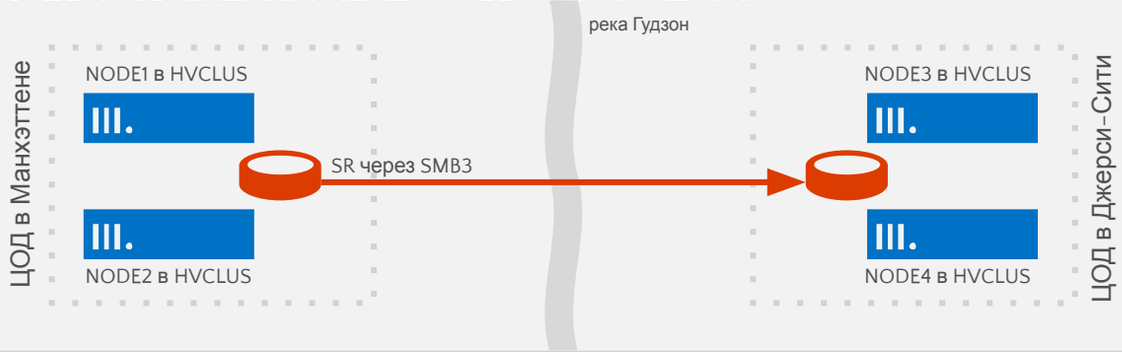
Производительность и размер тома журнала

Флеш-накопитель (SSD, NVME и др.)

Чем больше журнал, тем быстрее можно восстановить данные после крупных сбоев за меньшее число операций. Однако такой журнал занимает много места

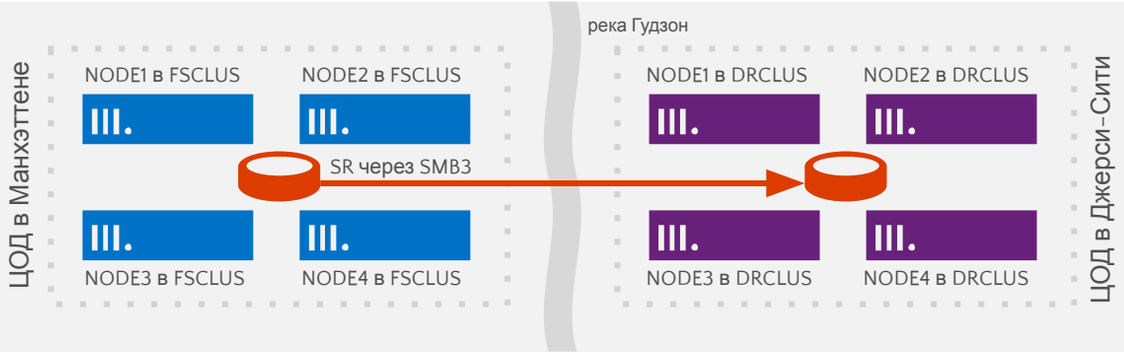
Географически распределенный кластер

- Один кластер
- Автоматический переход на другой ресурс



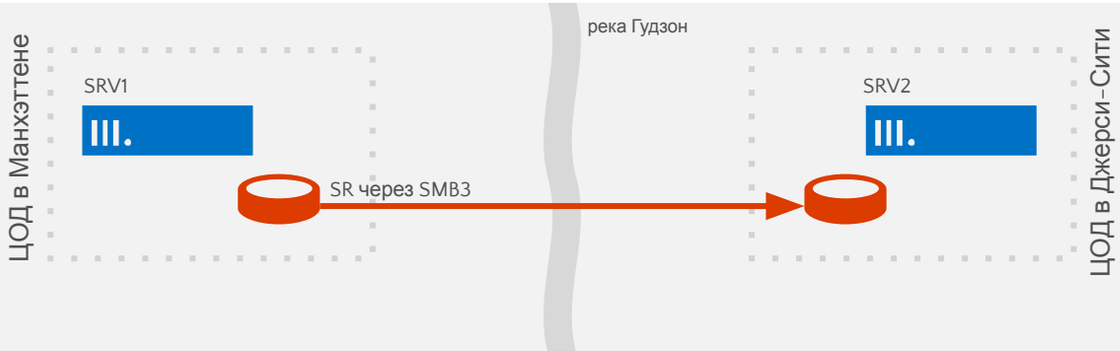
Между кластерами

- Два отдельных кластера
- Переход на другой ресурс вручную
- Синхронный или асинхронный режим



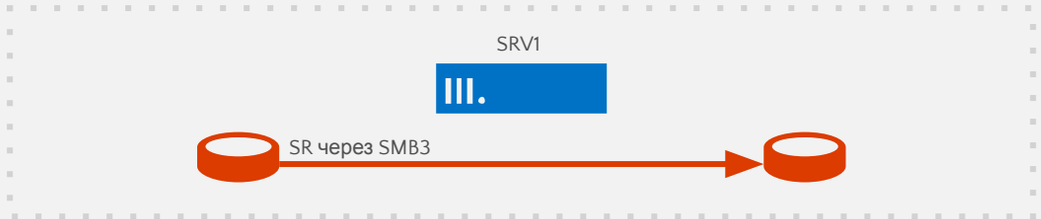
Между серверами

- Два отдельных сервера
- Переход на другой ресурс вручную
- Синхронный или асинхронный режим



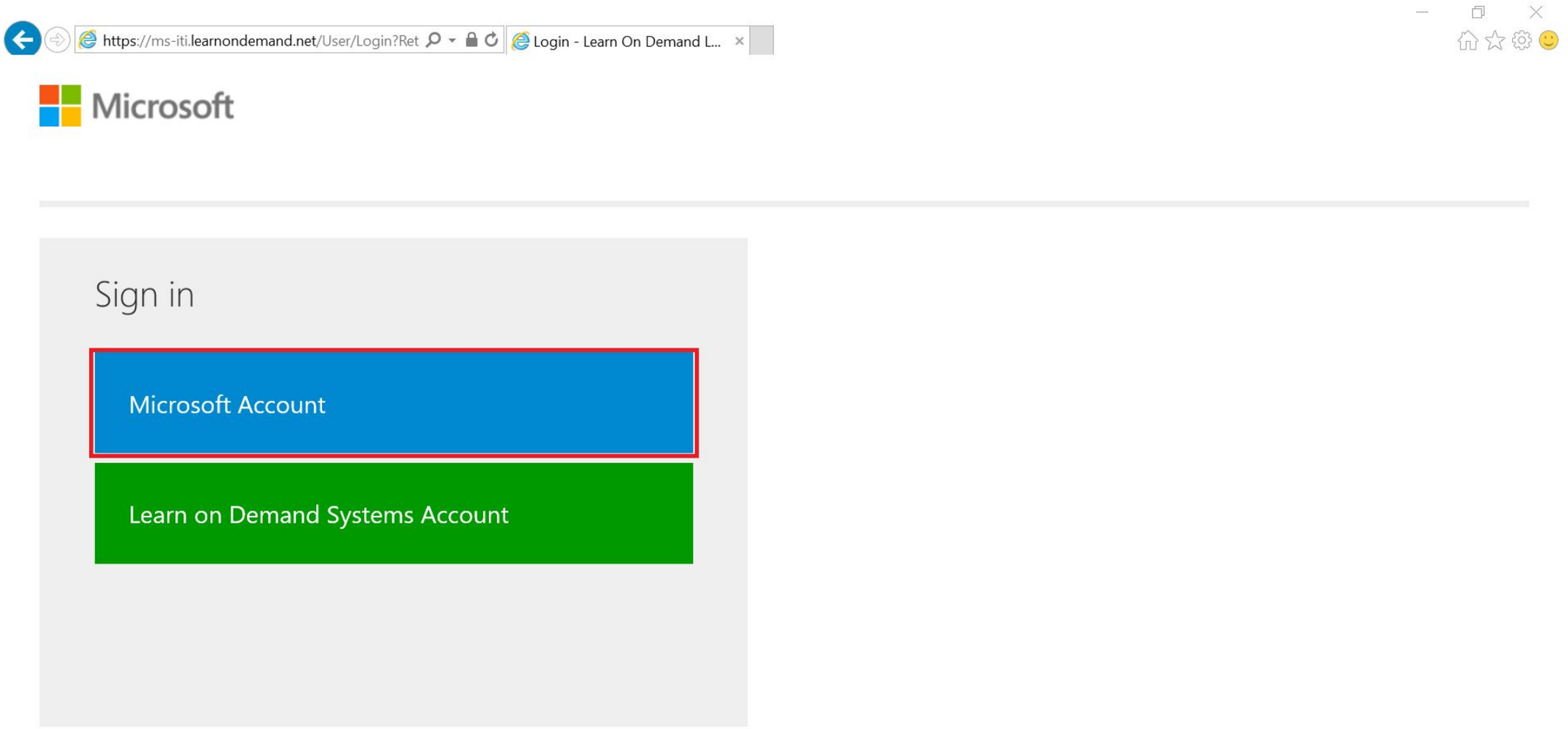
В пределах сервера

- Внутренняя репликация на сервере (одного тома на другой)
- Помещение данных в хранилище для отправки



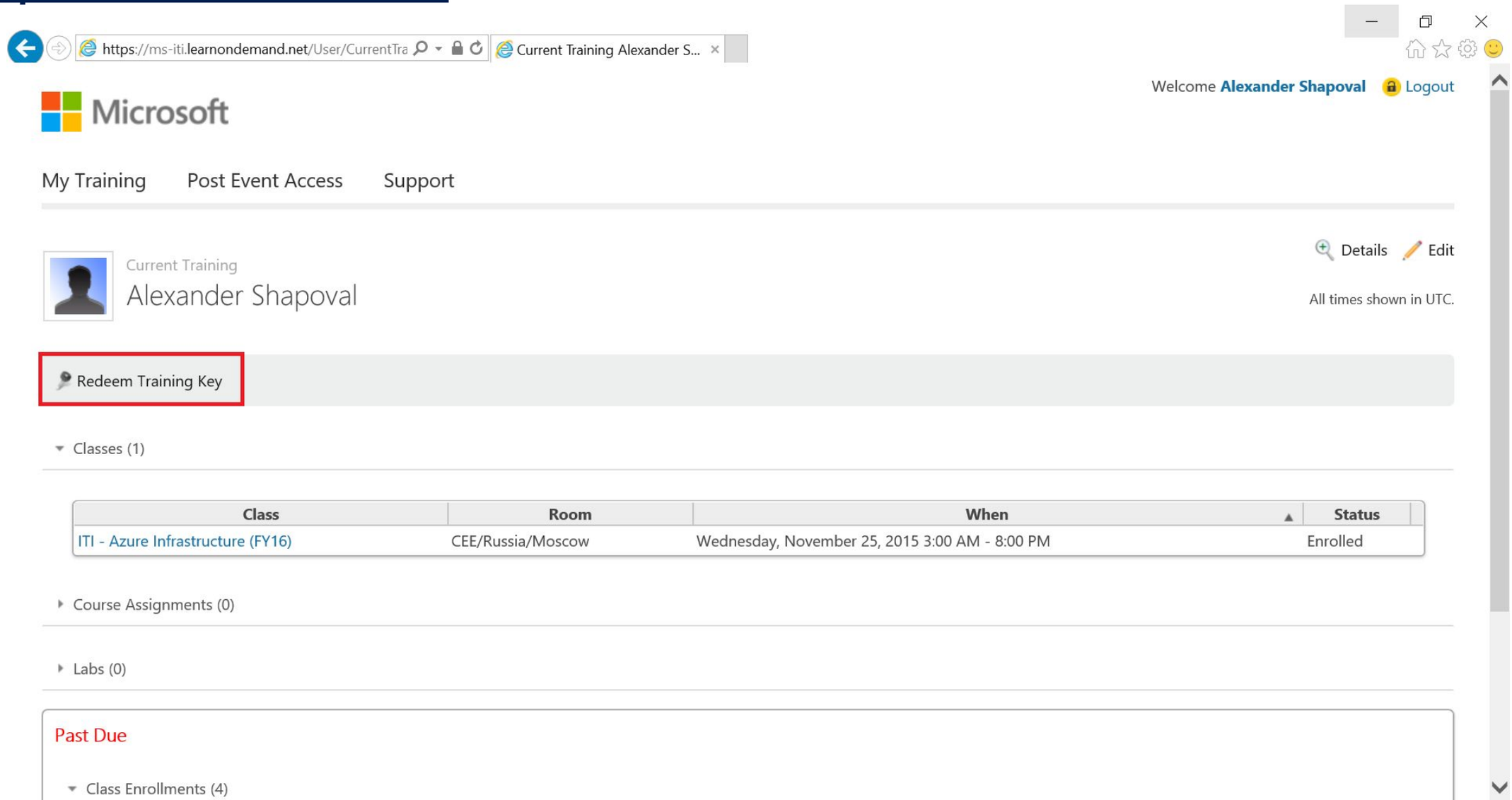
Подключение к лаб. работам

http://aka.ms/iti



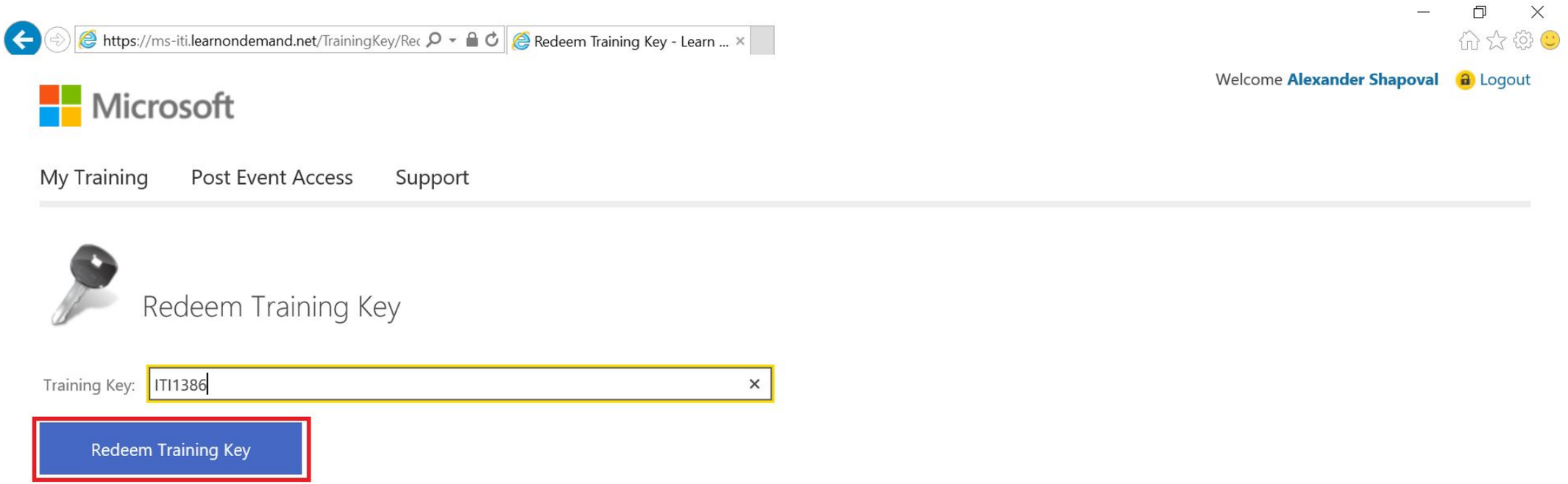
Подключение к лаб. работам

http://aka.ms/iti



Подключение к лаб. работам

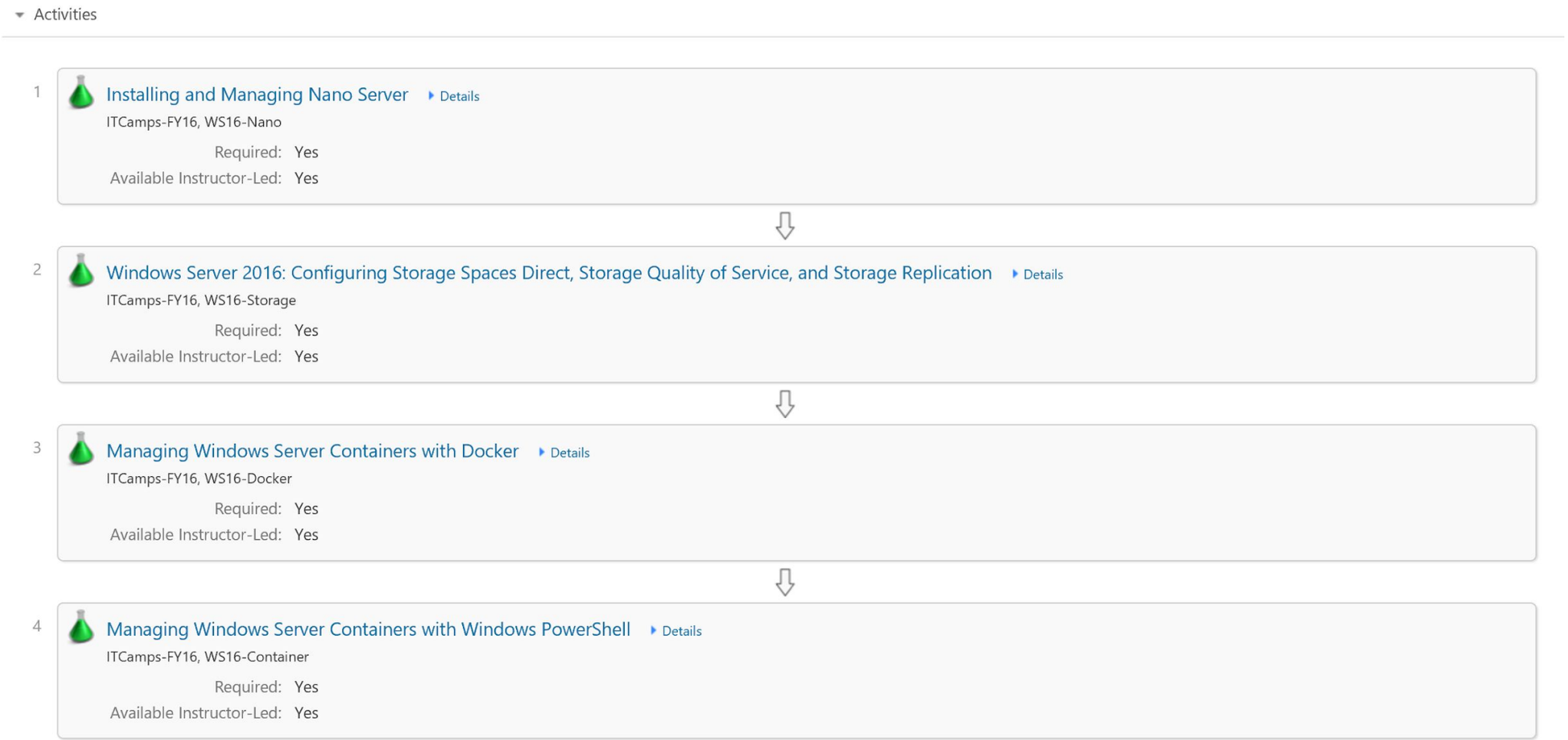
http://aka.ms/iti



Training Key:ITI1549

Подключение к лаб. работам

http://aka.ms/iti



SAN или Microsoft SDS

Традиционная сеть SAN

Блочная структура протоколов

Сеть FC с низкой задержкой

Управление LUN

Дедупликация данных

Группы устойчивости RAID

Объединение дисков в пулы

Высокий уровень доступности

Выгрузка копии, моментальные снимки

Разбиение хранилищ данных на уровни

Постоянный кэш с обратной

Программно определяемое хранилище от «Майкрософт»

Файловая структура протоколов

Низкая задержка благодаря SMB3Direct

Управление общими ресурсами

ДОБАВЛЕНО В R2

Дедупликация данных

Гибкие возможности управления устойчивостью

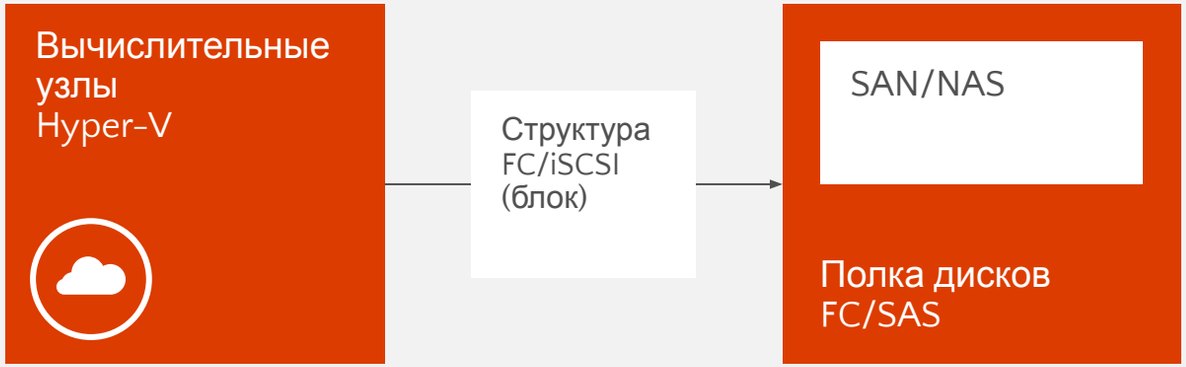
Объединение дисков в пулы

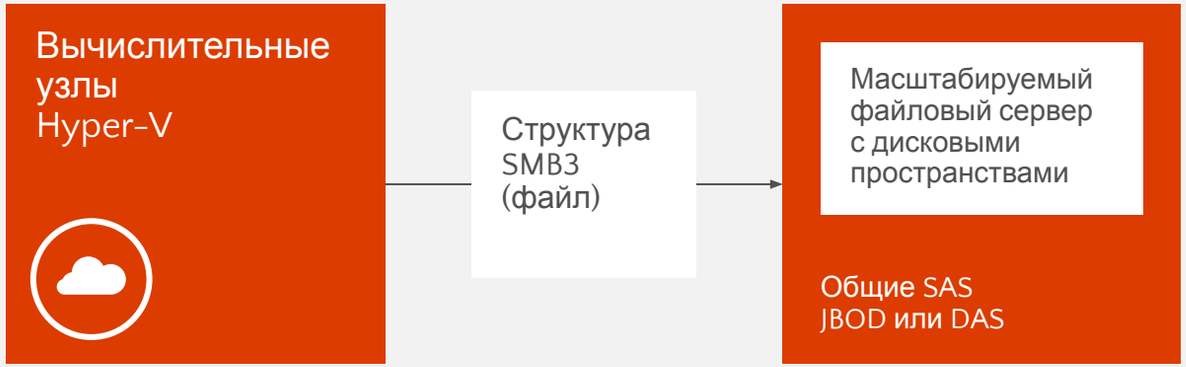
ДОБАВЛЕНО В 2016

Непрерывная доступность

Выгрузка копии через SMB, моментальные снимки

Разбиение на уровни для повышения производительности



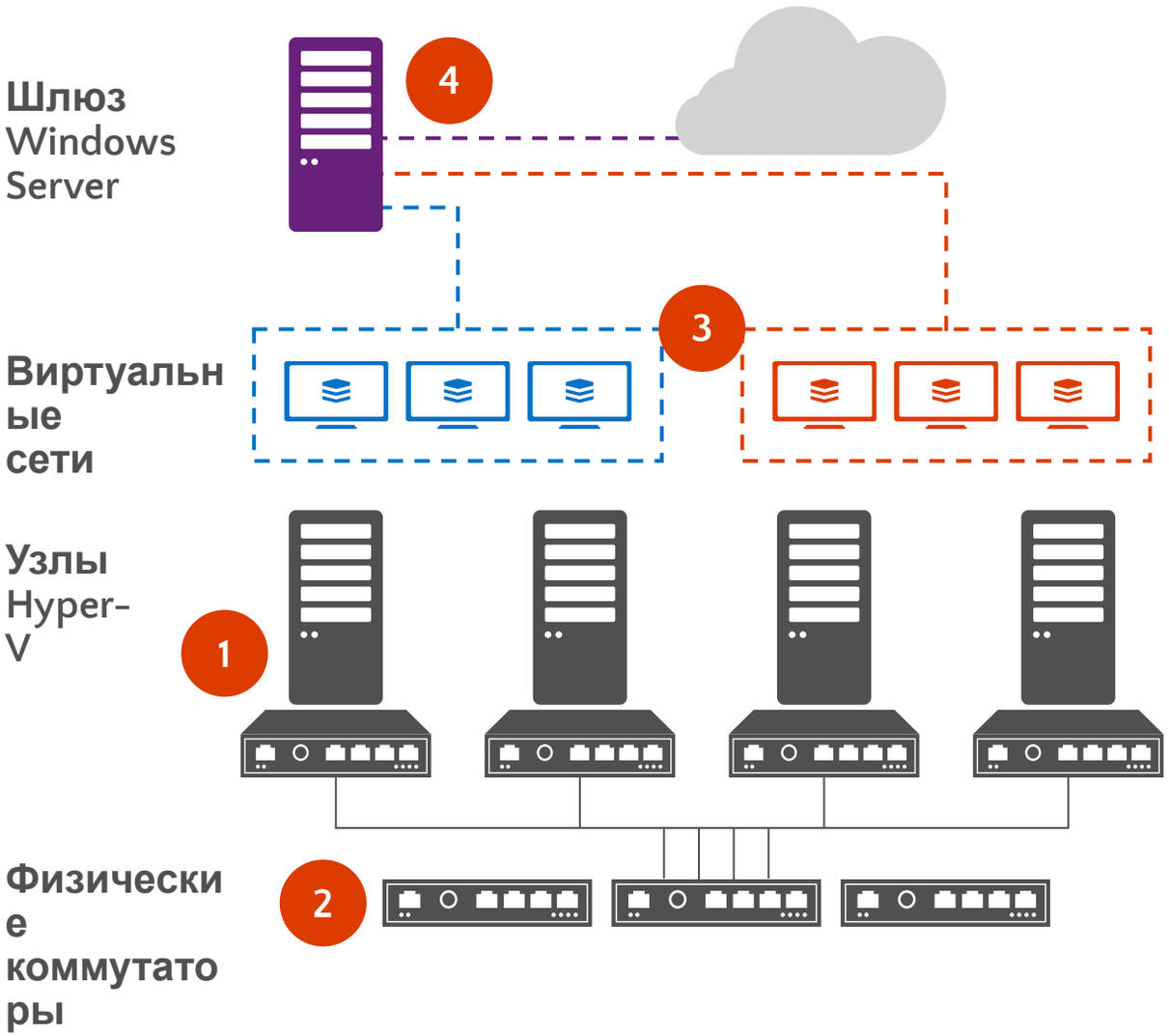


Microsoft

Сетевая инфраструктура

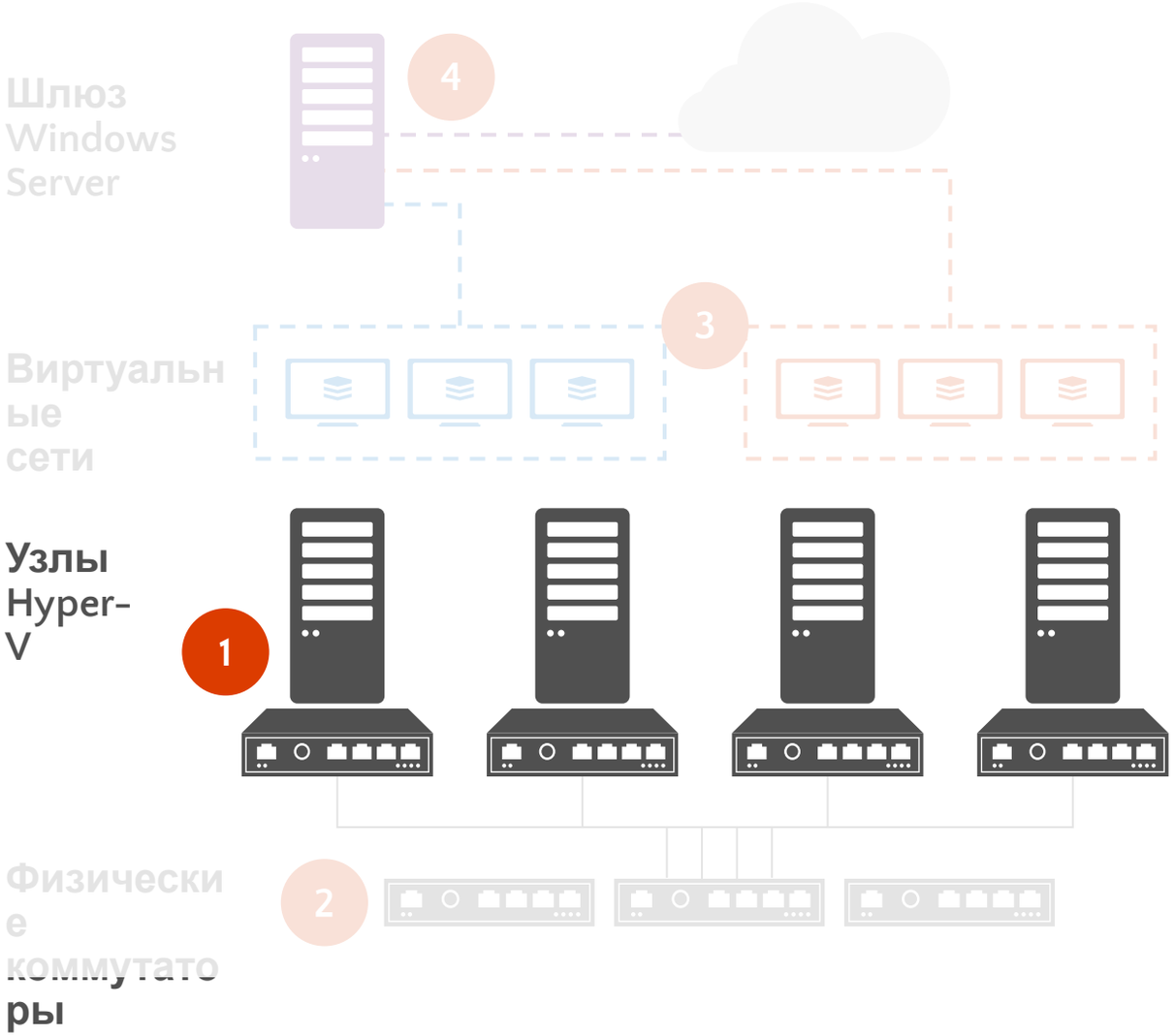
Александр Шаповал
Microsoft

Предыстория



1. Расширяемый коммутатор Hyper-V
   - Объединение сетевых карт
   - Протокол SMB 3.0
   - Аппаратная разгрузка
   - Конвергентные сети
2. Управление сетевыми коммутаторами с помощью OMI
3. Виртуализованные сети с NVGRE
4. Шлюз Windows Server

Предыстория: сети на основе узлов



Расширяемый коммутатор

Сетевой коммутатор L2 для подключения виртуальных машин. Расширения предоставляются партнерами: Cisco, 5nine, NEC и InMon.

Объединение сетевых карт

Встроенные гибкие варианты конфигурации и алгоритмы распределения нагрузки, включая новый динамический режим.

Протокол SMB Multichannel

Повышение производительности и устойчивости сети путем одновременного использования нескольких сетевых подключений.

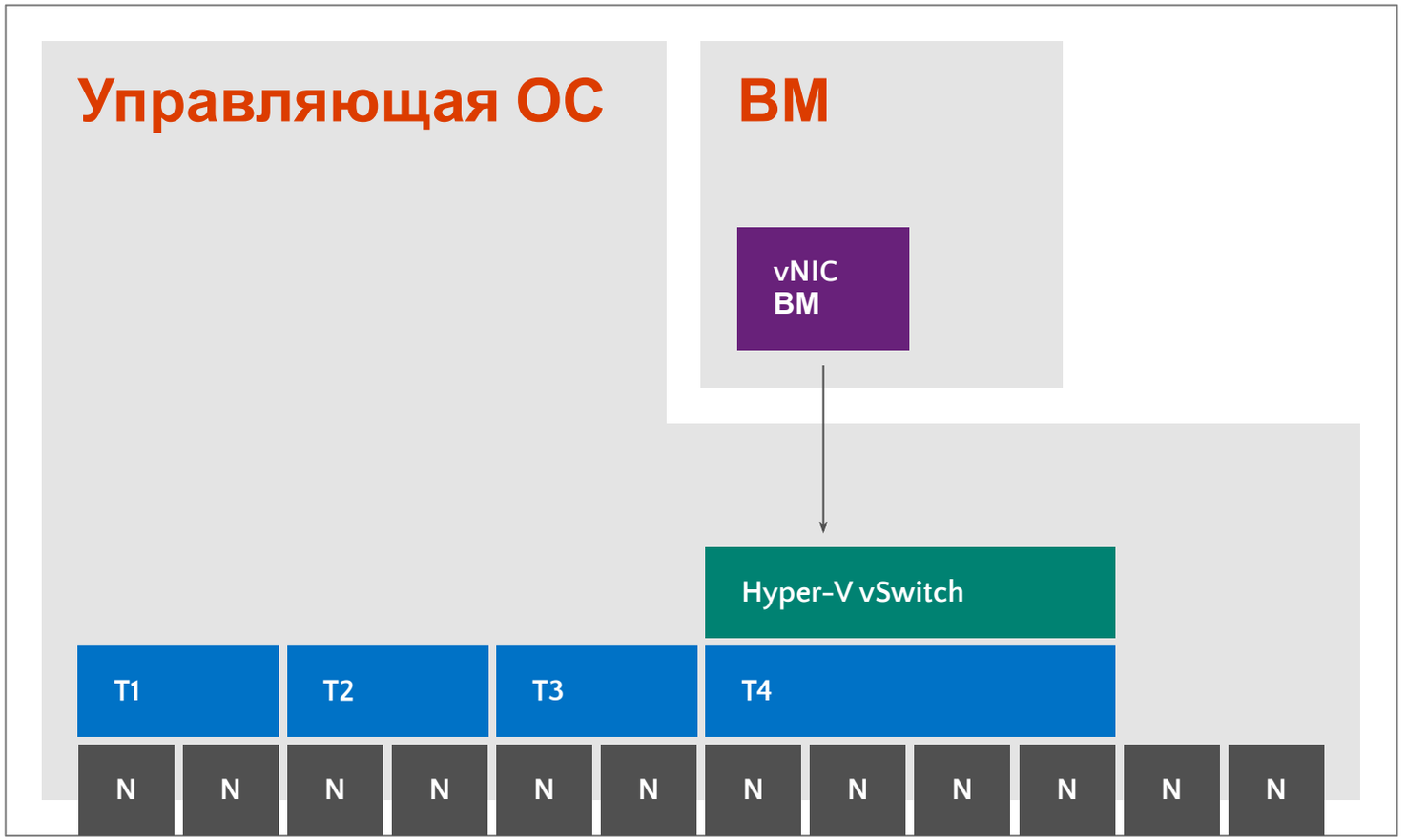
Протокол SMB Direct

Использование NIC с поддержкой технологии Remote Device Memory Access (RDMA) обеспечивает высочайшую производительность, высокую скорость и низкие задержки.

Аппаратная разгрузка

Динамическая фильтрация VMQ позволяет выполнять сбалансированную обработку трафика несколькими ЦП. Благодаря vRSS виртуальные машины могут использовать несколько виртуальных ЦП для поддержки высочайшей скорости передачи данных.

Конвергентные сети



Стандартный узел Hyper-V
(неконвергентный)
Пример: 12 x 1GbE NIC

N — Физическая сетевая плата

T x — Группа

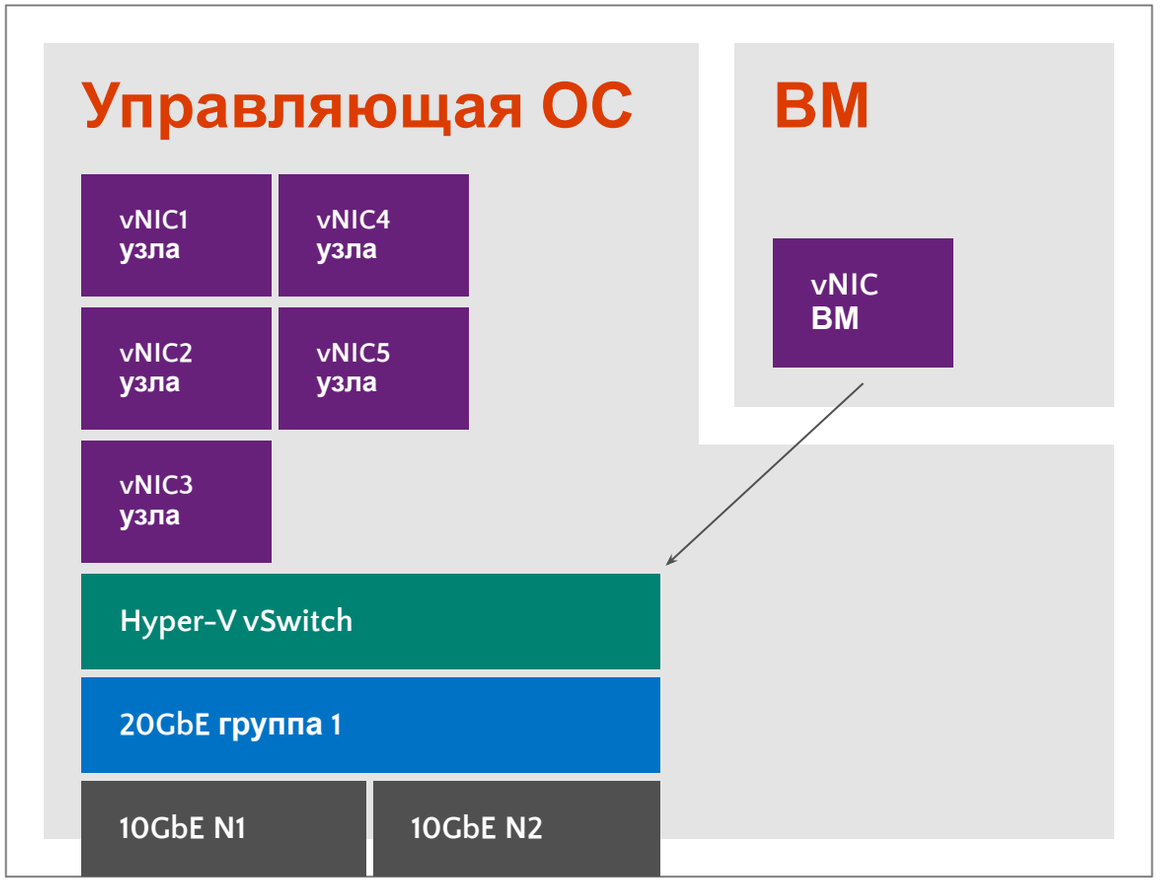
Каждому узлу требуются отдельные сети для выполнения следующих функций:

Трафик управления (агенты, RDP)
Кластеризация (CSV, работоспособность)
Динамическая миграция
Хранение данных (две подсети с SMB/SAN)
Трафик виртуальных машин

Результат

Множество кабелей. **Множество** портов. **Множество** коммутаторов. **Приемлемая** пропускная способность.

Конвергентная сеть 10GbE



Узел WS2012 R2 Hyper-V **(конвергентный)**
Пример: 2 x 10GbE NIC

vNIC1 узла — Трафик управления

vNIC2 узла — Кластер

vNIC3 узла — Динамическая миграция

vNIC4 узла — Подсеть хранения данных 1

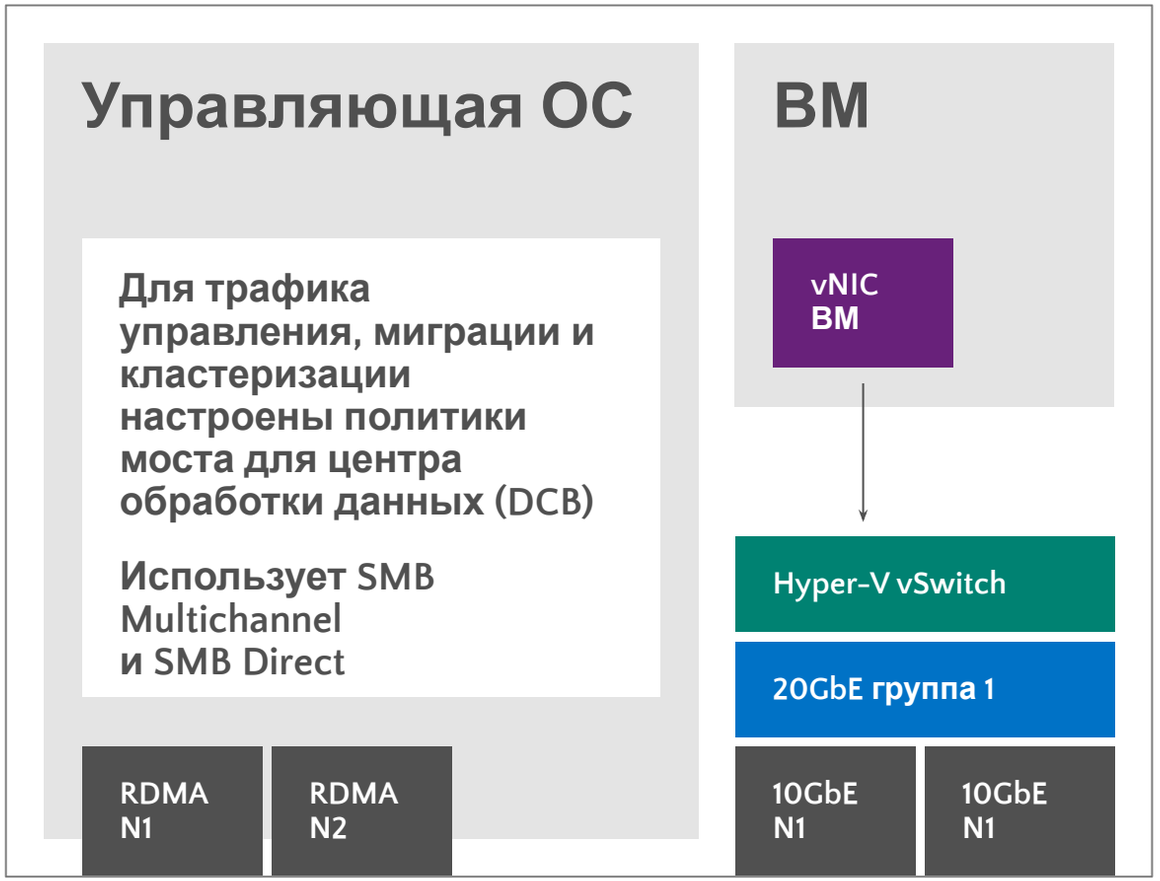
vNIC5 узла — Подсеть хранения данных 2

Для распределения пропускной способности между различными сетями используется QoS.

```
Set-VMNetworkAdapter
-ManagementOS -Name “Management”
-MinimumBandwidthWeight 5
```

vNIC узлов при необходимости можно размещать в различных VLAN.

Конвергентная сеть с 10GbE + RDMA



Узел WS2012 R2 Hyper-V **(конвергентный)**
Пример: 2 x 10GbE + 2 x 10GbE RDMA NIC

Узел подключен к двум сетям для выполнения собственных задач посредством NIC с поддержкой RDMA .

Для ВМ выделены 10GbE NIC.

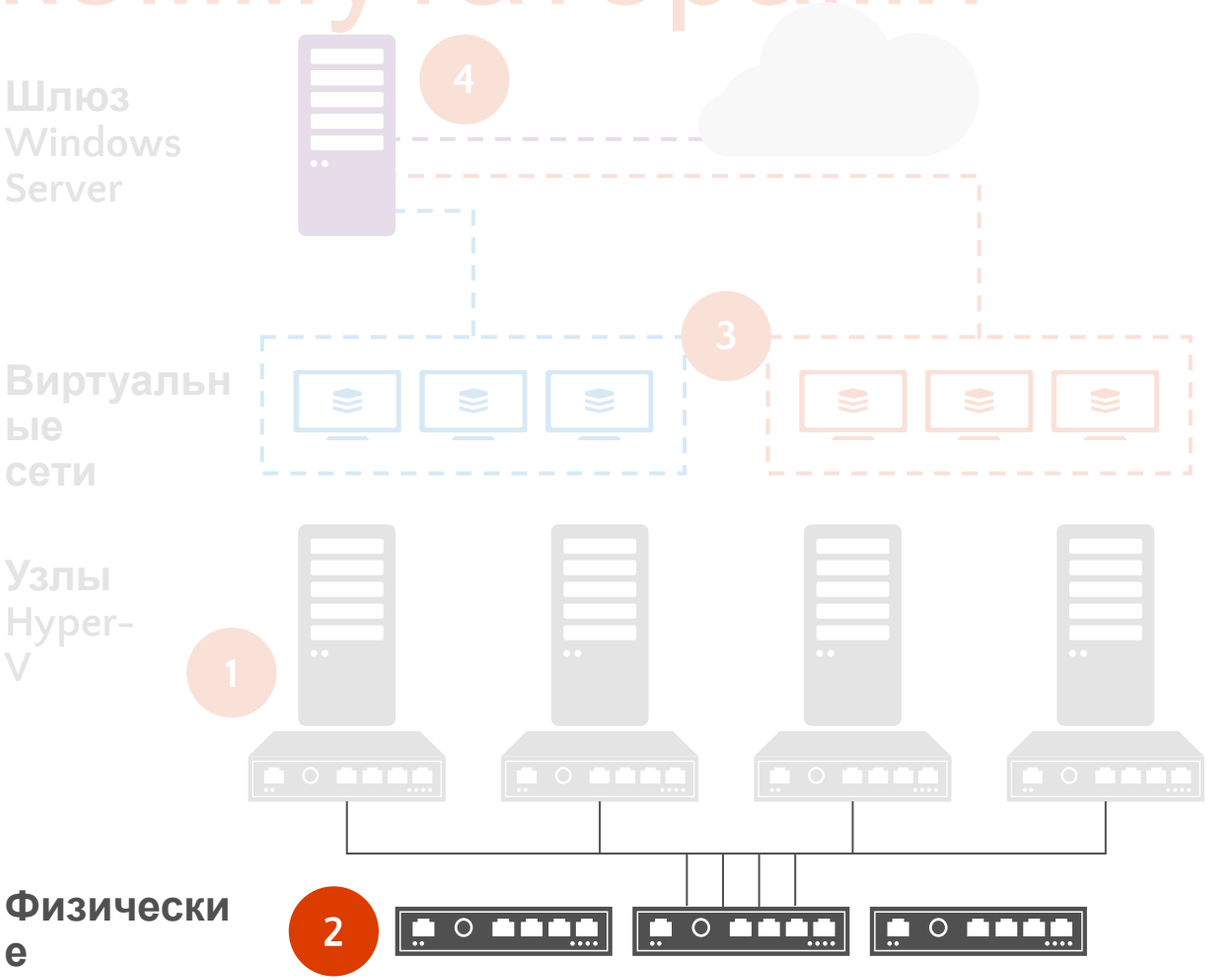
RDMA **не позволяет объединять сетевые карты и подключать** vSwitch.

С помощью мостов ЦОД и политик качества обслуживания создаются отдельные «сети».

```
New-NetQosTrafficClass “Live
Migration” -Priority 5
-Algorithm ETS -Bandwidth 30
```

При использовании RoCE **необходимо настроить** PFC **для всей сети.**

Предыстория: управление коммутаторами



OMI

OMI —портативный, не требующий много ресурсов, высокопроизводительный диспетчер объектов с открытым исходным кодом CIM Object Manager.

Открытый инструмент стандартизованного управления — CIM и WSMAN.

Симметрия API с WMI V2.

Поддерживается Arista, Cisco и другими компаниями.

Уровень абстракции поверх центра обработки данных

Любым устройством или сервером, который реализует стандартный протокол и схему, можно управлять с помощью стандартных инструментов совместимости, подобных PowerShell.

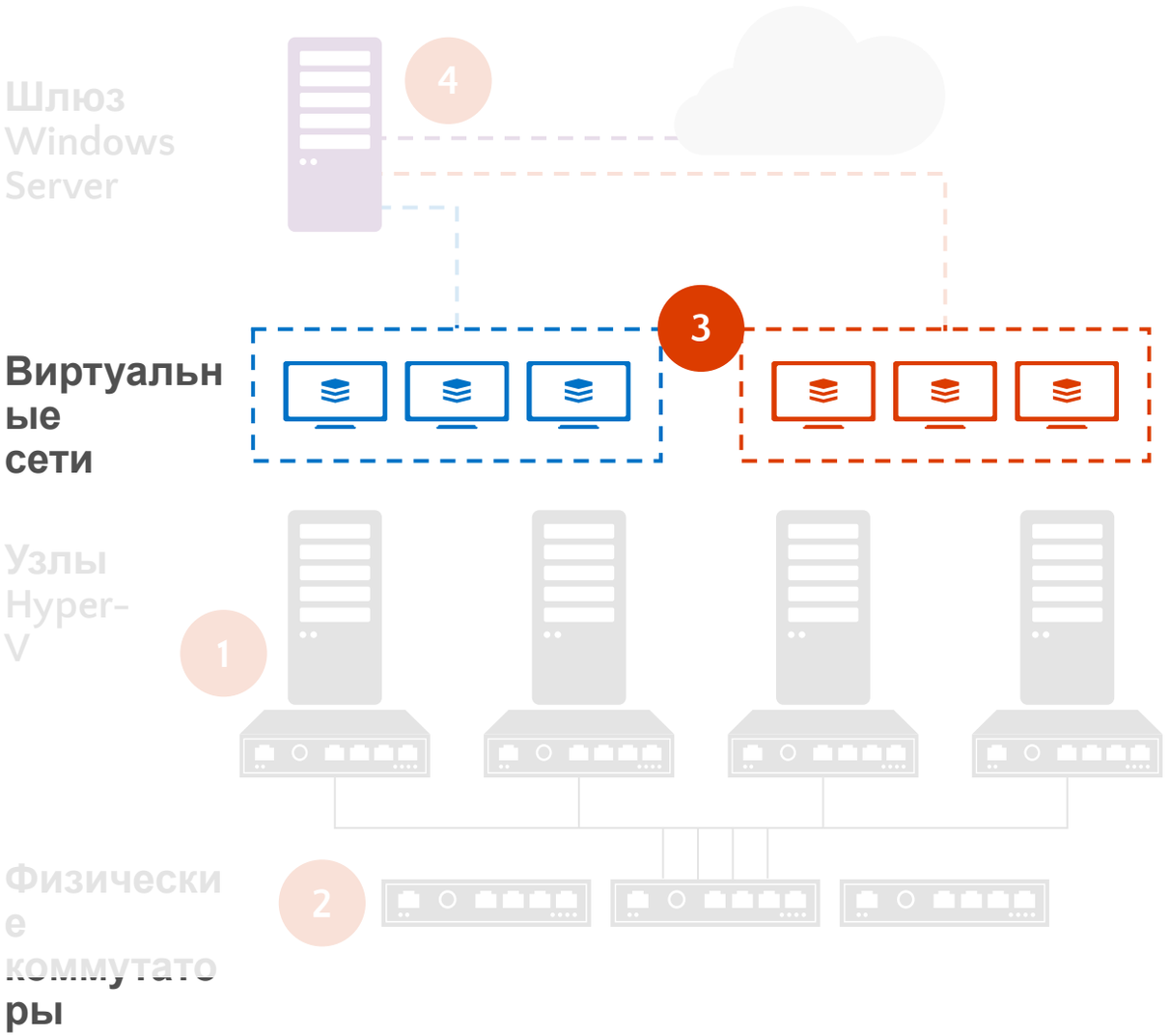
Стандартизация

Общий интерфейс управления для решений различных поставщиков сетевых технологий.

Автоматизация

Упрощенное управление предприятием в масштабах всей инфраструктуры.

Предыстория: виртуальные сети



Виртуализация сети

Наложение нескольких виртуальных сетей в общей физической сети.

Используется стандартный протокол Generic Routing Encapsulation (NVGRE).

VLAN

Устранение ограничений, связанных с масштабом, ошибками конфигурации и малой гибкостью подсетей.

Мобильность

Полная мобильность ВМ в центре обработки данных для новых и существующих нагрузок.

Перекрывающиеся IP-адреса различных клиентов могут существовать в одной инфраструктуре.

Поддерживается динамическая миграция ВМ между физическими подсетями.

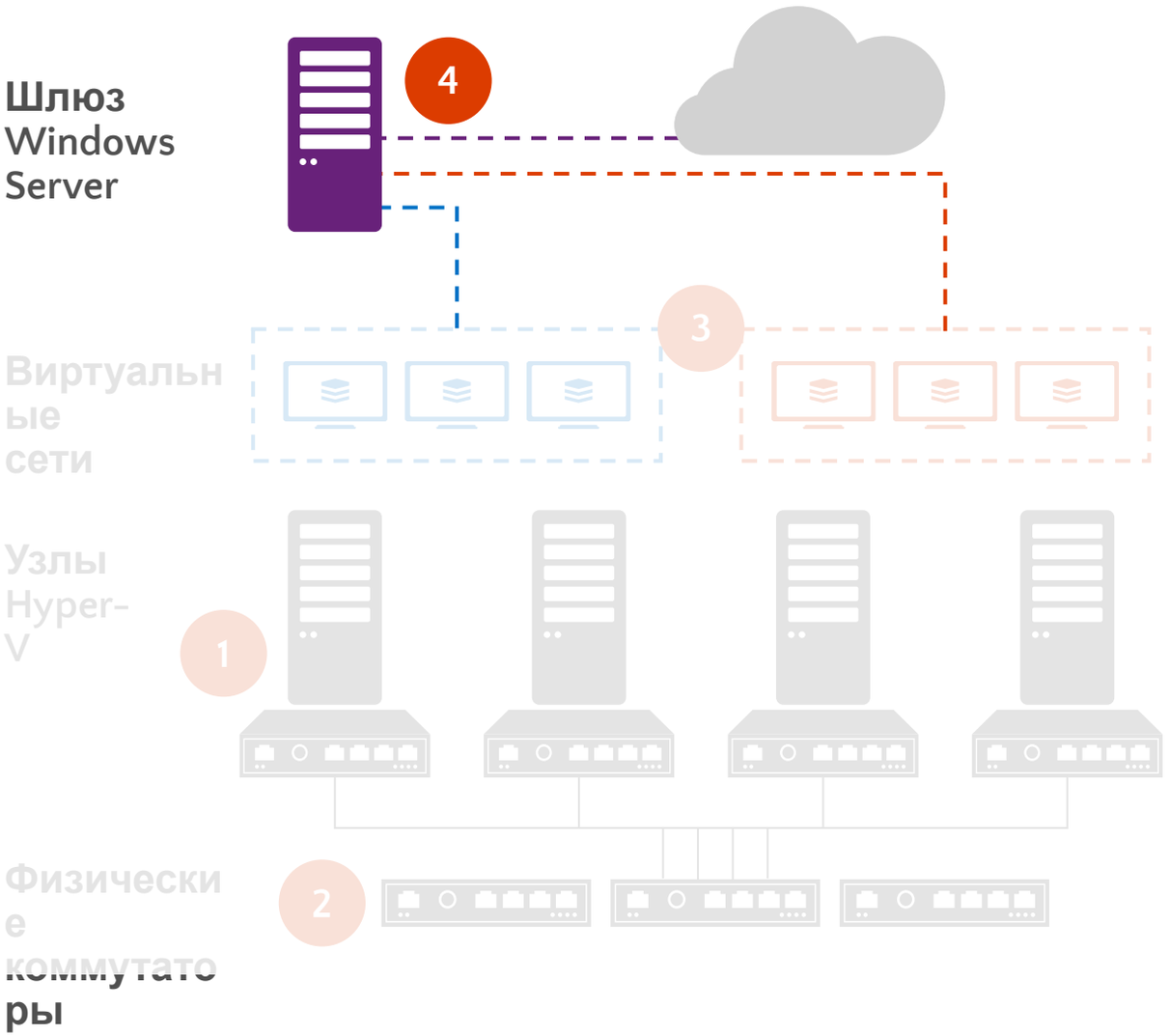
Автоматизация

Упрощенное управление предприятием в масштабах всей инфраструктуры.

Совместимость

Поддерживает современные технологии центров обработки данных.

Предыстория: шлюзы



Шлюзы

Возможность соединения сред с виртуализованными сетями с сегментами без виртуализации сети.

Множество различных типов: коммутаторы, выделенные устройства, встроенные компоненты Windows Server.

System Center

Шлюз Windows Server можно развернуть и настроить с помощью SCVMM.

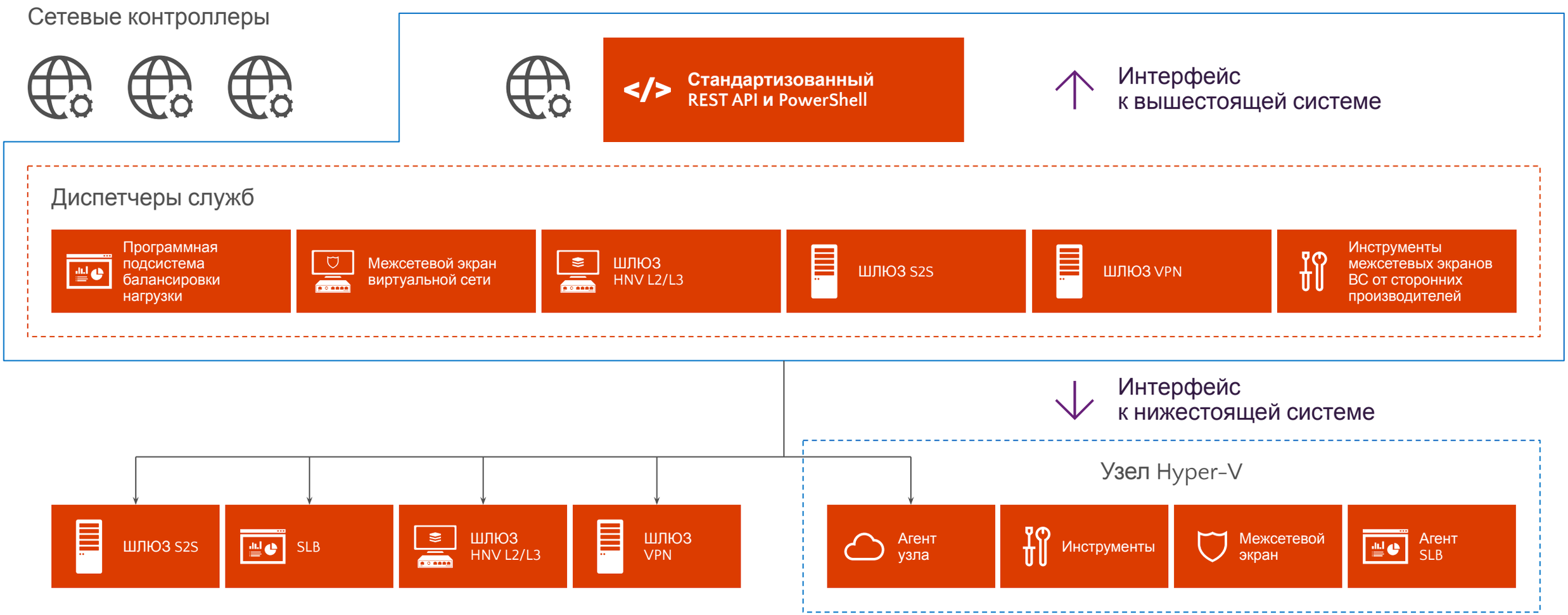
В TechNet доступен шаблон служб, позволяющий упростить развертывание.

Варианты развертывания

Поддерживается переадресация для частных облаков, NAT для подключения ВМ к Интернету и S2S VPN для гибридных сред.

Новые сетевые возможности и технологии

Общий обзор


Сетевые контроллеры
</>
Стандартизованный
REST API и PowerShell
Интерфейс
к вышестоящей системе
Диспетчеры служб
Программная подсистема балансировки нагрузки
Межсетевой экран виртуальной сети
ШЛЮЗ
HNV L2/L3
ШЛЮЗ S2S
ШЛЮЗ VPN
Инструменты межсетевых экранов ВС от сторонних производителей
Интерфейс
к нижестоящей системе
ШЛЮЗ S2S
SLB
ШЛЮЗ
HNV L2/L3
ШЛЮЗ
VPN
Узел Hyper-V
Агент
узла
Инструменты
Межсетевой
экран
Агент
SLB

Основы облачного масштабирования

Технология Switch-Embedded Teaming (SET)

Новый способ развертывания конвергентных сетей

Средства тиминга интегрированы в Hyper-V vSwitch

Режимы объединения: не зависящий от коммутатора (статические компоненты и LACP в этом выпуске отсутствуют).

Балансировка нагрузки: в этом выпуске — только для портов Hyper-V или динамическая.

Управление: SCVMM или PowerShell; графический интерфейс объединения сетевых карт в этом выпуске отсутствует.

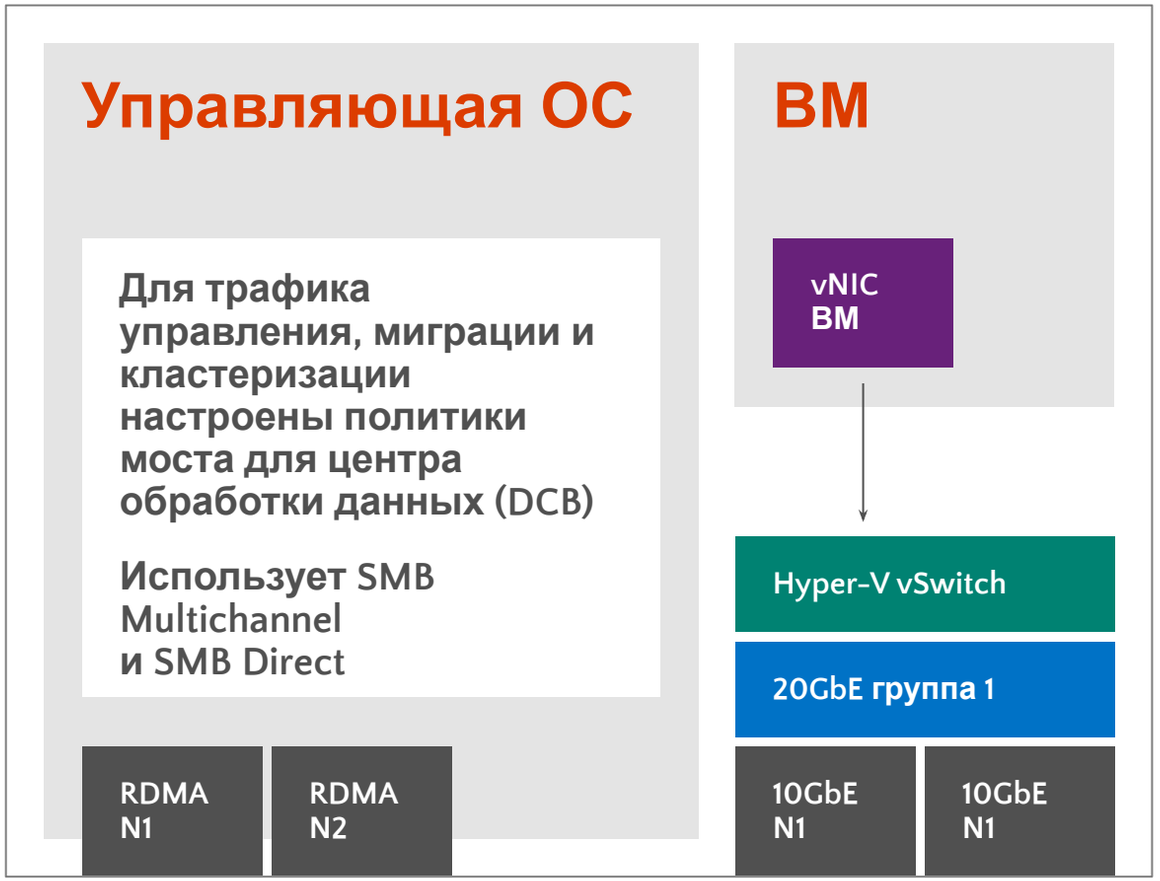
До восьми каналов на SET: один производитель, один драйвер, одинаковыетвозможности (например, двухпортовые NIC).

Объединять сетевые карты больше не нужно

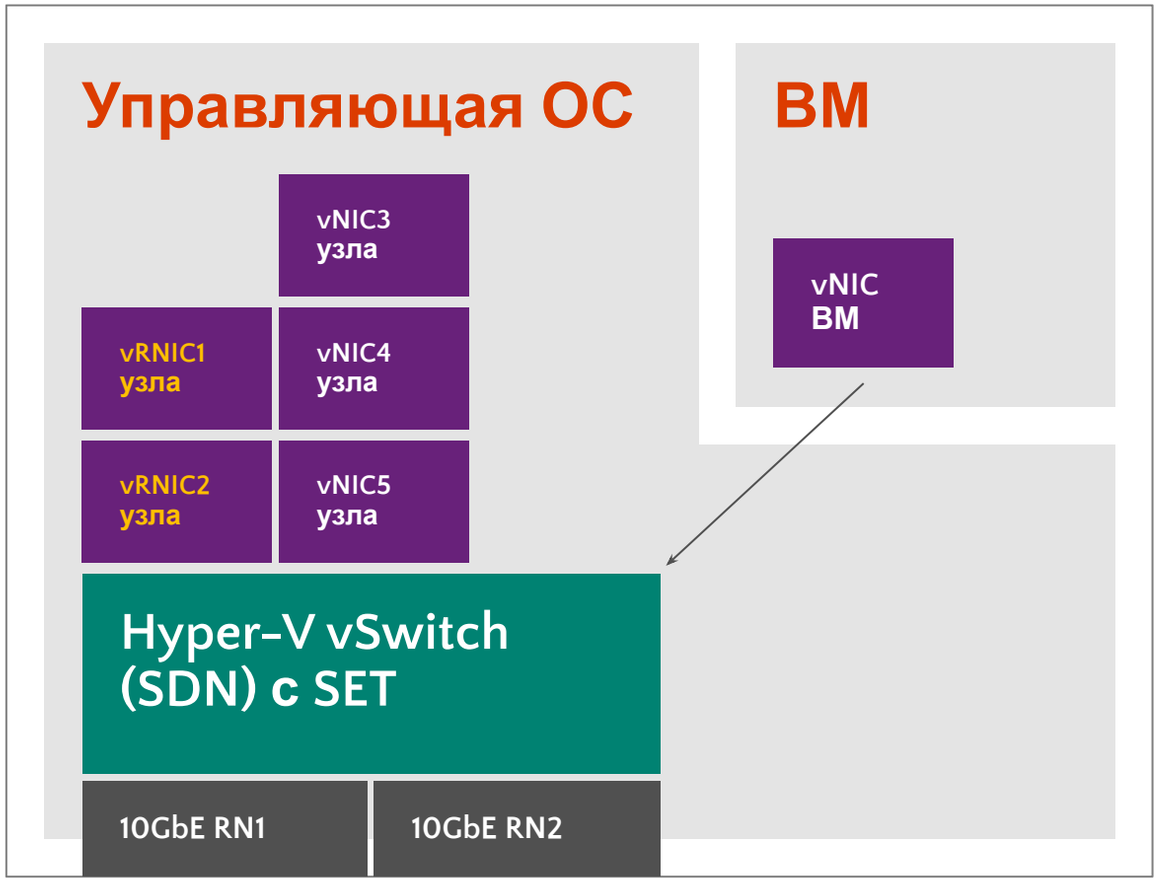
Коммутатор необходимо создать в режиме SET (SET нельзя добавить к существующему коммутатору)

```
New-VMSwitch -name SETswitch
–NetAdapterName “NIC1”,“NIC2”
-EnableEmbeddedTeaming $true
```

Конвергентные сети в выпуске 2016



Узел WS2012 R2 Hyper-V **(конвергентный)**
Пример: 2 x 10GbE + 2 x 10GbE RDMA NIC



Узел WS2016 Hyper-V **(конвергентный)**
Пример: 2 x 10GbE RDMA NIC

Создание коммутаторов

В WS2016 можно связать RDMA NIC с коммутатором Hyper-V vSwitch, **используя SET или без него**

Пример 1: создание виртуального коммутатора Hyper-V с RDMA vNIC

```
New-VMSwitch -name RDMAswitch -NetAdapterName "SLOT 2"
Add-VMNetworkAdapter -SwitchName RDMAswitch -Name SMB_1 -managementOS
Enable-NetAdapterRDMA "vEthernet (SMB_1)"
```

Пример 2: создание коммутатора Hyper-V Virtual Switch с SET и несколькими RDMA vNIC

```
New-VMSwitch -name SETswitch -NetAdapterName "SLOT 2","SLOT 3"
Add-VMNetworkAdapter -SwitchName SETswitch -Name SMB_1 -managementOS
Add-VMNetworkAdapter -SwitchName SETswitch -Name SMB_2 -managementOS
Enable-NetAdapterRDMA "vEthernet (SMB_1)","vEthernet (SMB_2)"
```

Конвергентные сети – RDMA

Разрешает vNIC узла предоставлять возможности RDMA процессам ядра (например, SMB Direct)

При использовании SET позволяет нескольким RDMA NIC предоставлять возможности RDMA нескольким vNIC (SMB Multichannel через SMB Direct)

При использовании SET поддерживает обработку отказов RDMA для SMB Direct (если предоставлены две vNIC с поддержкой RDMA)

Работает на полной скорости с производительностью реального RDMA

PacketDirect (PD)

Современный NDIS для Windows

Платформа общего назначения — универсальный стек TCP/IP

Поддержка клиентских систем и центров обработки данных

Имеющихся возможностей NDIS недостаточно для 100G

Что можно улучшить?

Средства ввода-вывода общего назначения.

Оперативная память.

Приложению доступны не все возможности управления своими пакетами.

Уделить внимание приложениям, которые интенсивно нагружают сеть (DDoS, SLB, vSwitch и т. п.) — обычно они анализируют и переадресуют пакеты.

Аналог технологии Data Path Data Kit от Intel

Становится стандартом ускорения путей данных.

Интенсивно применяется в устройствах NFV.

PacketDirect (PD)

Высокоскоростная модель ввода-вывода без блокировок.

Можно использовать параллельно со стандартной NDIS.

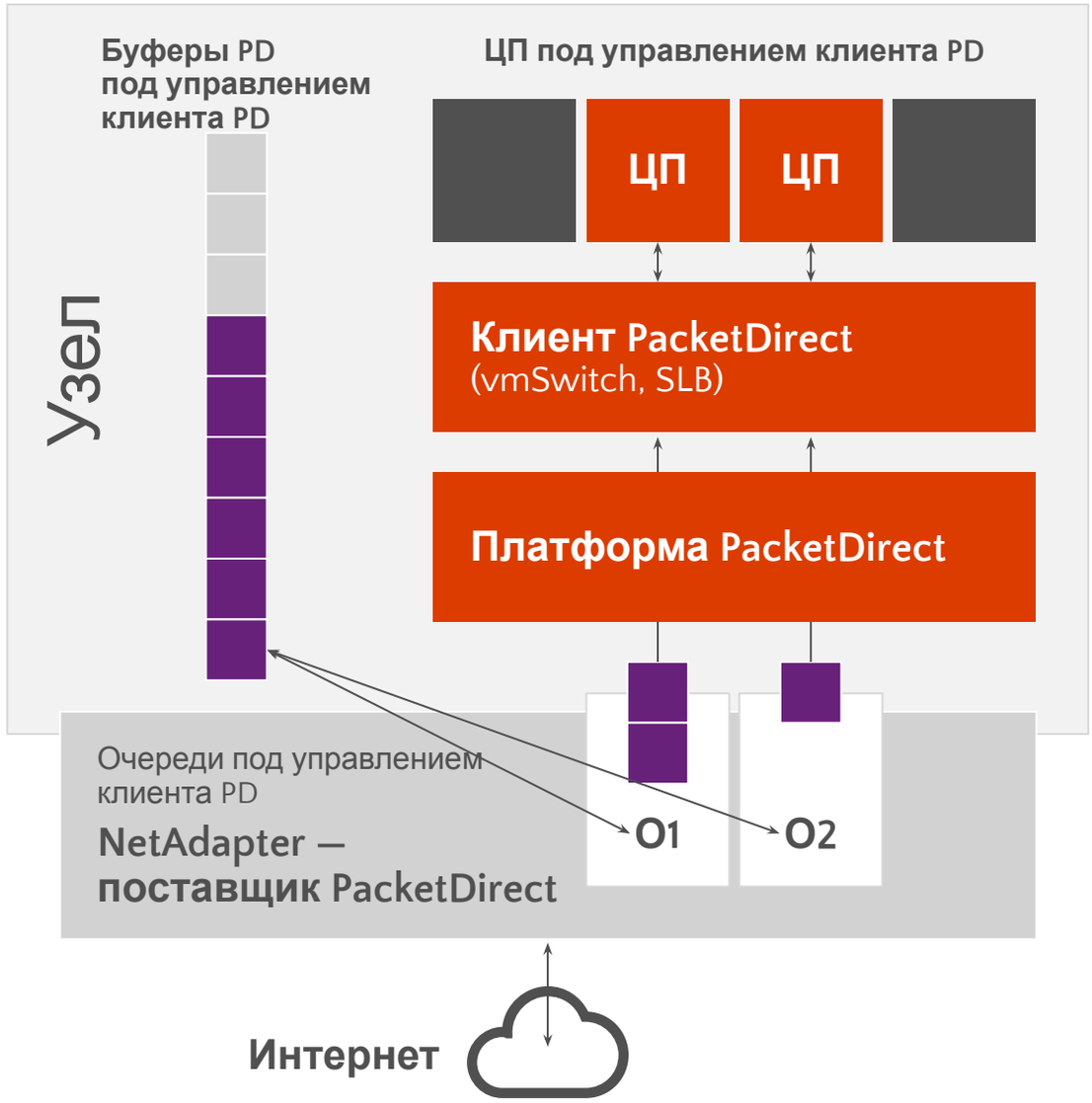
Предоставляет приложениям прямой доступ к ЦП, памяти и функциям NIC.

Теперь приложение может выбирать время приема и отправки с помощью механизмов опроса.

Имеется функция управления буфером.

Приложение управляет вводом-выводом для NFV.

Совместимо с большей частью 10G NIC.



Инфраструктура SDN

Обновленная и улучшенная

Гибкая инкапсуляция

Эти технологии работают на уровне данных и поддерживают как Virtual Extensible LAN (VxLAN), так и Network Virtualization Generic Routing Encapsulation (NVGRE).

VXLAN поддерживается в режиме MAC distribution (Floodless).

Hyper-V vSwitch

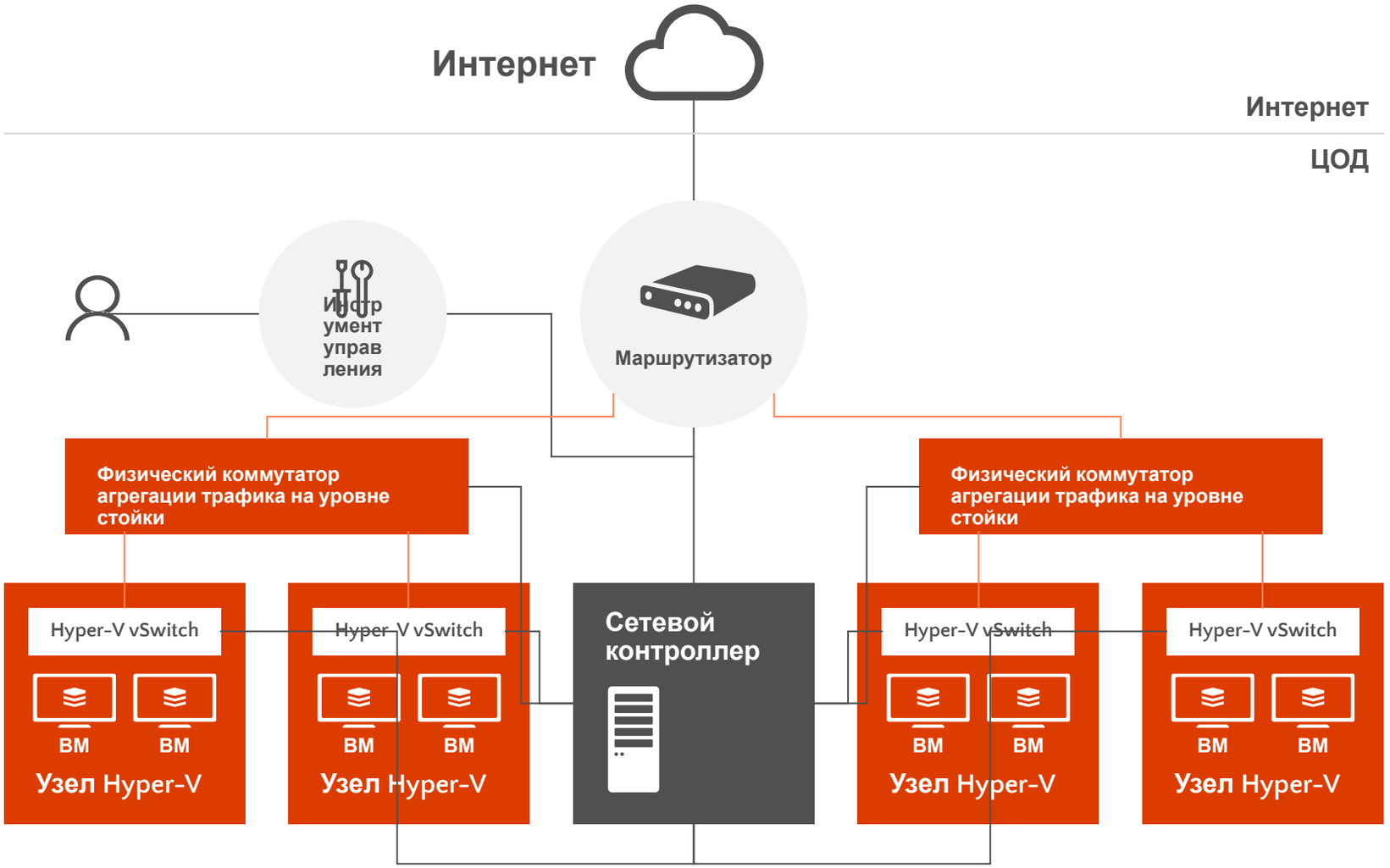
Высокопроизводительные распределенные средства коммутации и маршрутизации, а также уровень принудительного применения политик, согласованный и совместимый с Microsoft Azure.

В коммутаторе Hyper-V vSwitch используется тот же механизм потоков, что в Microsoft Azure — его эффективность в крупных средах уже проверена.

Стандартизованные протоколы

REST, JSON, OVSDB, WSMAN/OMI, SNMP, NVGRE/VXLAN

Сетевой контроллер



Централизованная, программируемая точка автоматизации с возможностями управления, настройки, мониторинга и устранения неполадок виртуальной и физической сетевой инфраструктуры ЦОД.

Можно развернуть на одной ВМ (для тестирования), в виде кластера из трех физических серверов (без Hyper-V) или на трех ВМ из отдельных узлов.

Сетевой контроллер – общие сведения

Роль сервера с высокой доступностью и масштабируемостью

API для взаимодействия сетевых контроллеров с сетью.

API для взаимодействия с сетевыми контроллерами.

API для нижестоящих систем

Сетевой контроллер может обнаруживать сетевые устройства, определять конфигурации служб и собирать всю необходимую информацию о сети.

Позволяет отправлять информацию (например, внесенные в конфигурацию изменения) в сетевую инфраструктуру.

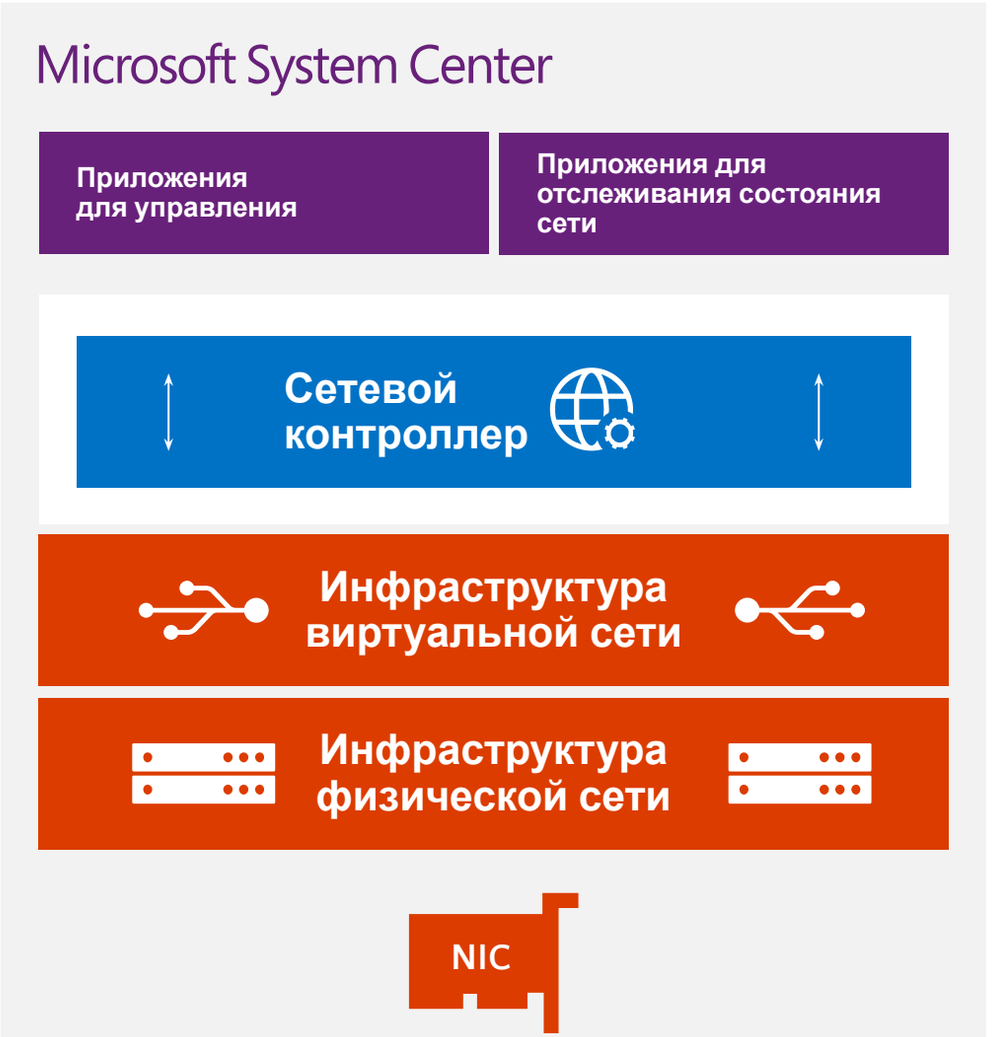
API для вышестоящих систем (интерфейс REST)

Позволяет собирать информацию о сети с сетевых контроллеров и применять ее для мониторинга и настройки сети.

Возможности настройки, мониторинга, устранения неполадок и развертывания новых устройств в сети с помощью Windows PowerShell, REST, SCVMM, SCOM и т. п.

Функции управления

Виртуальные машины и коммутаторы Hyper-V, физические сетевые коммутаторы и маршрутизаторы, программные межсетевые экраны, шлюзы VPN, включая RRAS, подсистемы балансировки нагрузки…



Возможности сетевого контроллера

Управление структурой сети

Подсети IP.

Виртуальные локальные сети.

Коммутаторы L2 и L3.

NIC узлов.

Управление межсетевыми экранами

Правила блокировки и разрешения.

Вертикальные и горизонтальные подключения.

Правила межсетевого экрана связаны с портом vSwitch виртуальных машин.

Правила для входящего и исходящего трафика.

Ведение журналов разрешенного и запрещенного трафика.

Сетевая топология

Автоматическое обнаружение элементов сети и взаимосвязей между ними.

Построение цепочек служб

Правила перенаправления трафика одному или нескольким физическим устройствам.

Программная подсистема балансировки нагрузки

Централизованная конфигурация политик SLB.

Мониторинг сети

Физические и виртуальные.

Данные о текущем состоянии сети: потери в сети, задержка, базовые показатели, отклонения.

Локализация сбоев.

Данные об элементах: опросы и ловушки SNMP.

Ограниченный объем критической информации посредством общедоступных баз информации об управлении (Management Info Base, MIB), в т. ч. состояние канала, сведения о перезапусках системы, состояние узлов BGP.

Работоспособность устройства (коммутатора, маршрутизатора) и группы устройств (стойки, подсети и т. п.).

Агрегация данных о потерях в сети, задержке, использовании ЦП и памяти устройствами, загруженности каналов и отброшенных пакетах.

Анализ воздействия для наложенных сетей, которые зависят от работоспособности не устойчивой к ошибкам базовой физической сети, на основе сведений о топологии — для определения используемых ресурсов и работоспособности vNext.

Интеграция System Center Operations Manager — для получения сведений о работоспособности и статистической информации.

Управление виртуальными сетями

Развертывание технологий виртуализации сетей средствами Hyper-V.

Развертывание виртуального коммутатора Hyper-V.

Развертывание виртуальных сетевых адаптеров на виртуальных машинах.

Хранение и распределение политик для виртуальных сетей.

Поддержка NVGRE и VXLAN.

Управление шлюзами в Windows Server

Функции развертывания, настойки и управления для шлюзов Windows Server -> узел и ВМ.

S2S VPN с IPsec, S2S VPN с GRE.

P2S VPN, переадресация L3, маршрутизация BGP.

Балансировка нагрузки для подключений S2S и P2S по виртуальным машинам шлюза + ведение журналов изменений в конфигурациях и состояниях.

Виртуализация сетевых функций (NFV)

Мощная платформа для виртуальных устройств

Сетевые контроллеры

3

Развертывание и настройка виртуальных устройств, а также управление ими с помощью сетевого контроллера

</> Стандартизованный REST API и PowerShell

Интерфейс к вышестоящей системе

2

Развертывание виртуальных устройств от выбранных вами поставщиков

Диспетчеры служб

- Программная подсистема балансировки нагрузки
- Межсетевой экран виртуальной сети
- ШЛЮЗ HNV L2/L3
- ШЛЮЗ S2S
- ШЛЮЗ VPN
- Инструменты межсетевых экранов ВС от сторонних производителей

Интерфейс к нижестоящей системе

4

В Hyper-V можно разместить необходимые гостевые ОС

Узел Hyper-V

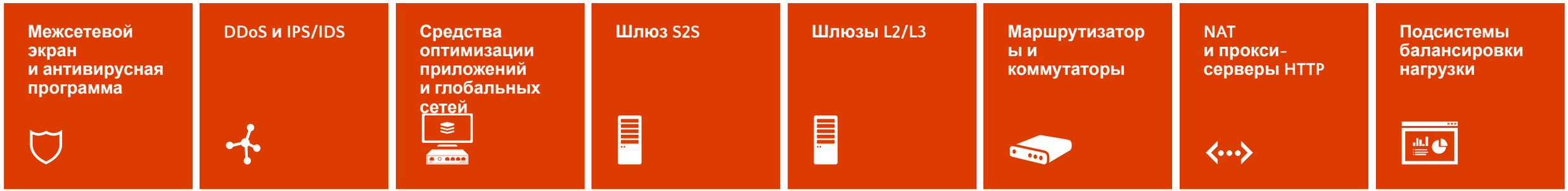
- Агент узла
- Инструменты
- Межсетевой экран
- Агент SLB

- ШЛЮЗ S2S
- SLB
- ШЛЮЗ HNV L2/L3
- ШЛЮЗ VPN

1

В Windows Server реализованы ключевые функции виртуализованных сетей

Виртуализация функций сети



Функции сети, выполняемые аппаратными устройствами, все чаще виртуализуются с помощью виртуальных устройств.

Новый рынок виртуальных устройств стремительно развивается.

Эти устройства отличаются динамичностью и простотой модификации, поскольку представляют собой готовые настроенные виртуальные машины.

Виртуальное устройство может быть одной или несколькими виртуальными машинами, упакованными, обновляемыми и обслуживаемыми как единое целое:

- **Его можно с легкостью перемещать и масштабировать.**
- **Оно намного проще в эксплуатации.**

Начиная с версии Windows Server 2012 R2, в системе реализован отдельный шлюз в виде виртуального устройства.

Программная подсистема балансировки нагрузки (SLB)

Машстабируемость и доступность

Проверено в Azure — масштабирование на множество экземпляров мультиплексоров (MUX) с балансировкой миллиардов потоков.

Высокая скорость обмена данными между мультиплексорами и виртуальными сетями.

Высокая доступность.

Поддержка вертикальной и горизонтальной балансировки нагрузки.

Технология Direct Server Return обеспечивает высокую производительность .

Гибкая и интегрированная

Мультитенантность позволяет сократить капитальные затраты.

Доступ к ресурсам физической сети из клиентской виртуальной сети.

Балансировка нагрузки на уровнях 3 и 4.

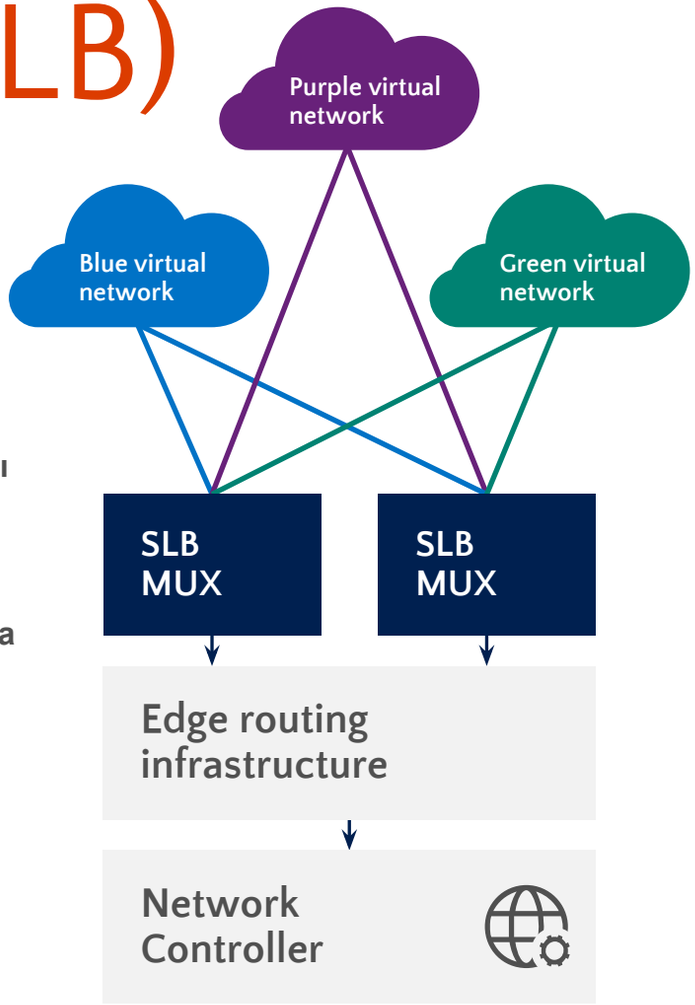
Поддержка NAT.

Простота в управлении

Удобное управление посредством сетевого контроллера.

Простое развертывание структуры с помощью SCVMM.

Интеграция с существующими порталами самообслуживания посредством сетевого контроллера — REST API или PowerShell.



Межсетевой экран центра обработки данных

Входит в состав Windows Server.

Этот межсетевой экран работает на сетевом уровне, обрабатывает пять идентификаторов подключения, отслеживает состояние и поддерживает мультитенантные среды.

Протокол.

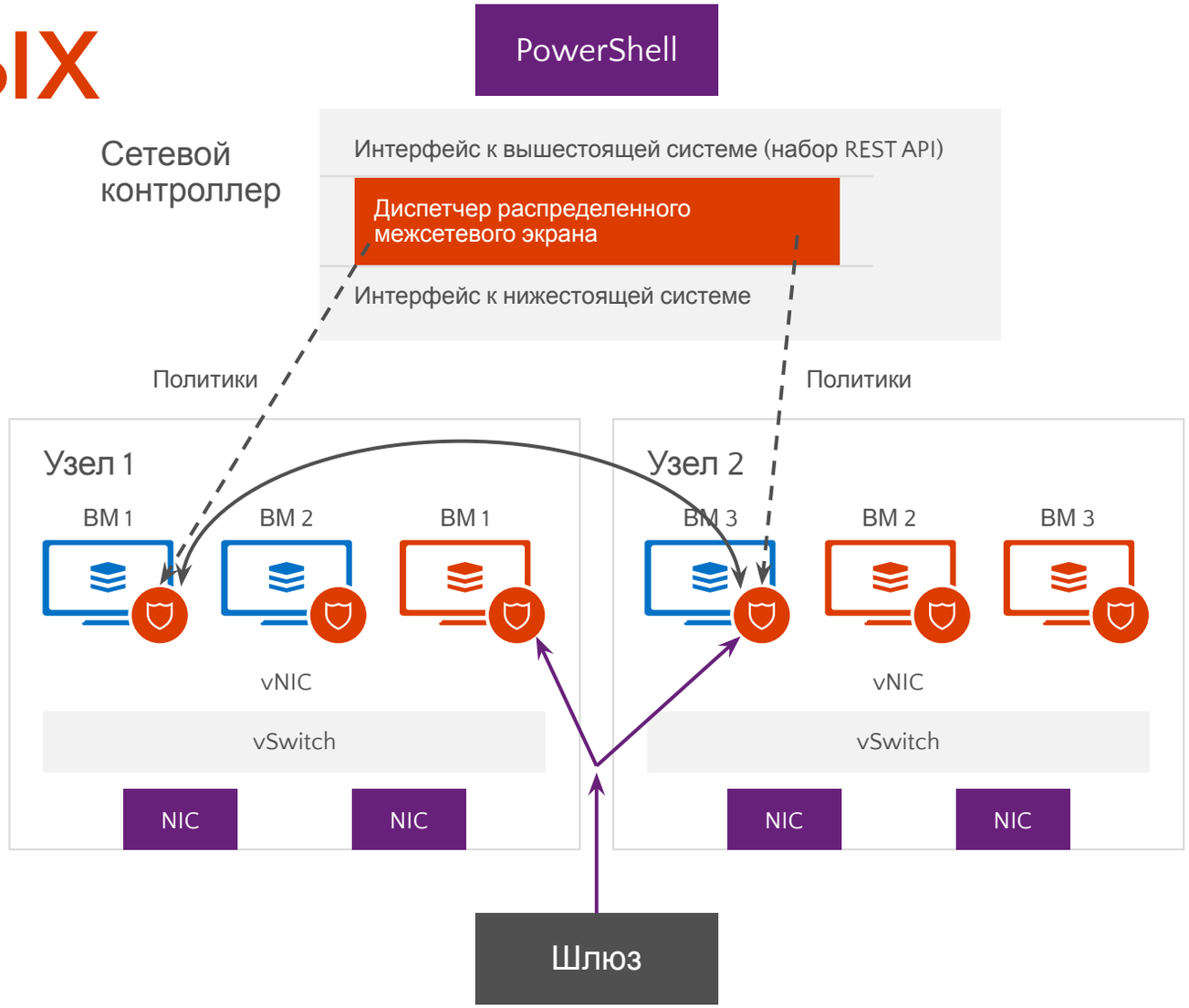
Номера портов отправителя и получателя.

IP-адреса отправителя и получателя.

Тенант-администраторы могут устанавливать и настраивать политики межсетевого экрана для защиты своих виртуальных сетей.

Управление посредством сетевого контроллера и API для вышестоящих систем.

Защита горизонтальных и вертикальных



Межсетевой экран центра обработки данных

Масштабируемый, управляемый программный межсетевой экран с простым обнаружением неполадок

Позволяет перемещать клиентские виртуальные машины на различные вычислительные узлы без нарушения клиентских политик межсетевого экрана.

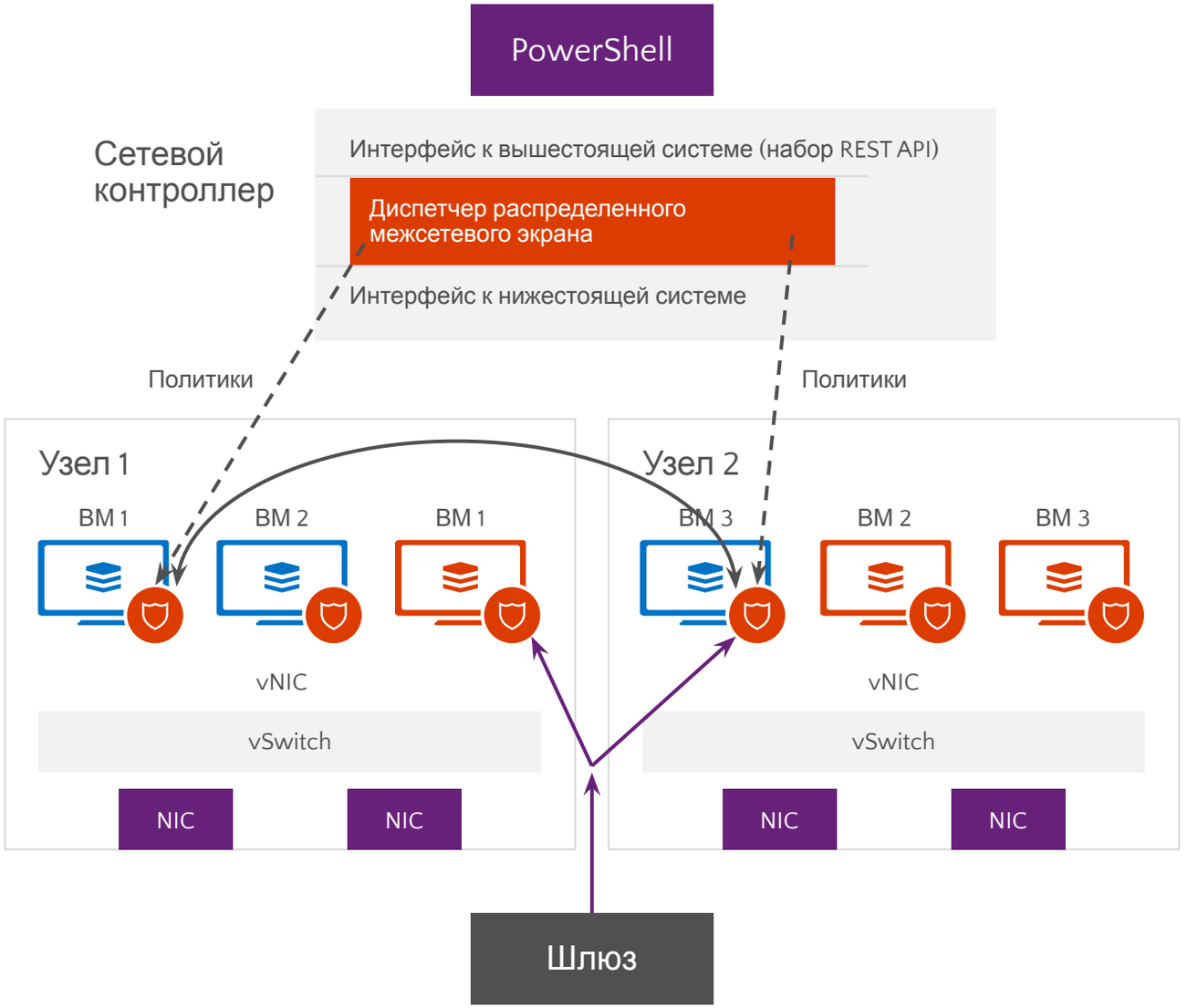
Развертывается как агент межсетевого экрана для портов узла vSwitch.

Клиентские виртуальные машины получают политики, назначенные соответствующему агенту межсетевого экрана узла vSwitch.

Правила межсетевого экрана настраиваются для каждого порта vSwitch,
вне зависимости от узла, в котором выполняется виртуальная машина.

Не зависит от гостевой ОС.

Защищает трафик между ВМ в одной и в различных подсетях L2.



Microsoft

Nano Server

Александр Шаповал
Microsoft

Проблемы клиента

Перезагрузки мешают работать

Почему нужно перезагружать систему для установки патча к компоненту, которым я никогда не пользуюсь?
Если необходима перезагрузка, то система должна вернуться в рабочее состояние в кратчайший срок.

Образы серверных систем очень большие

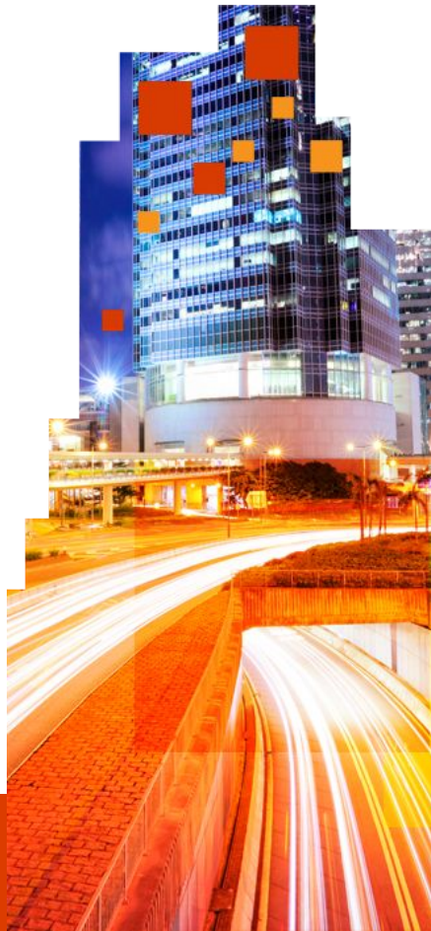
На установку и настройку образов большого размера уходит много времени.
Передача образов значительно снижает пропускную способность сети.
Для хранения образа требуется много места на диске.

Инфраструктура требует слишком много ресурсов

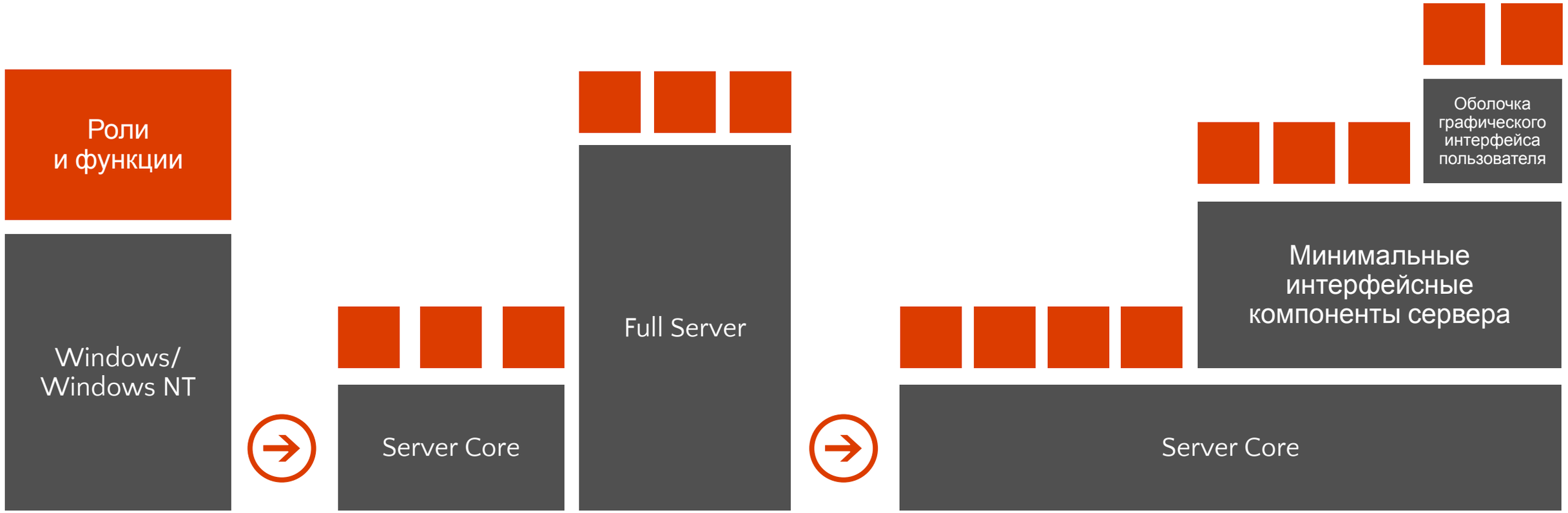
Если операционная система будет потреблять меньше ресурсов, я смогу увеличить плотность виртуальных машин (ВМ).

Увеличив плотность ВМ, я смогу снизить затраты, повысить эффективность и прибыльность

«Я хочу получить только **необходимые** компоненты и ничего больше».



Предыстория

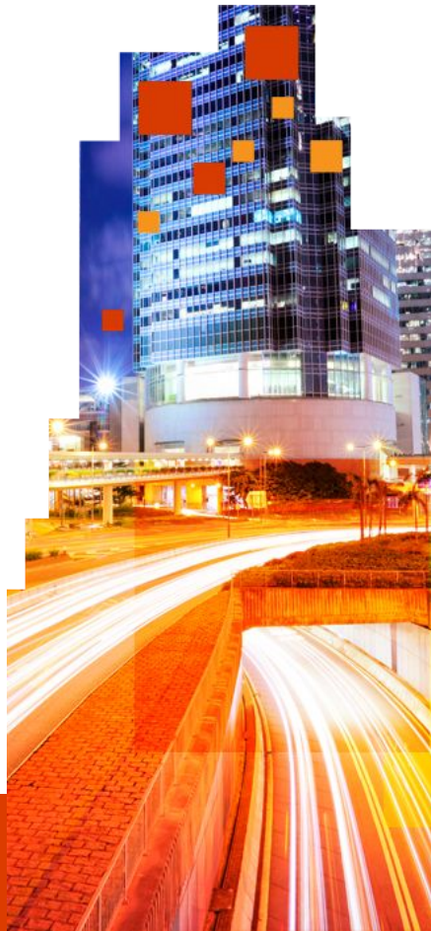


От Windows NT
до Windows Server 2003

Windows Server 2008
и Windows Server 2008
R2

Windows Server 2012
и Windows Server 2012 R2

«Нам нужна конфигурация сервера, **оптимизированная для облака**».



Следующий этап развития

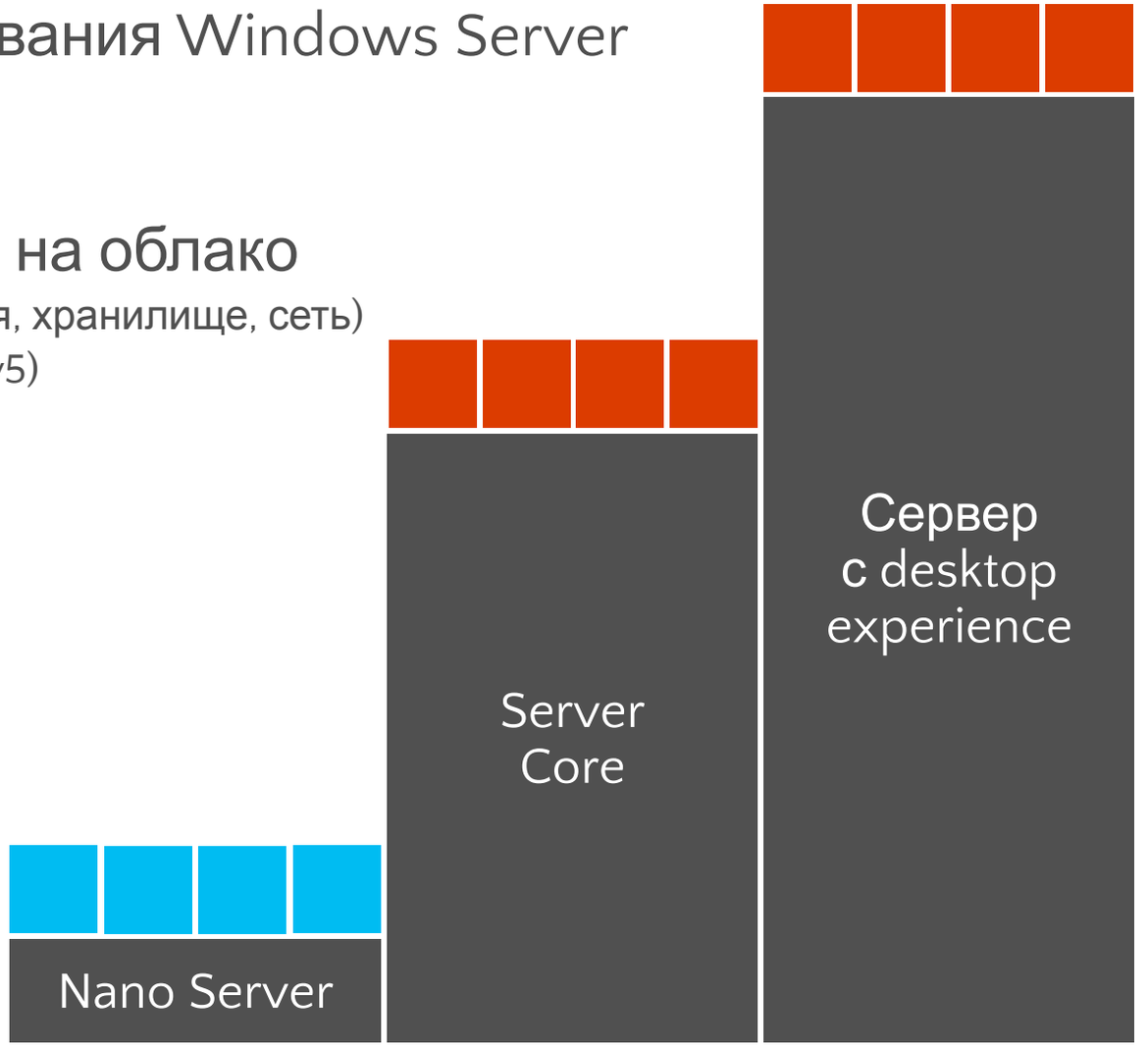
Nano Server: новый вариант развертывания Windows Server (только для 64-разрядных систем)

Глубокий рефакторинг с ориентацией на облако

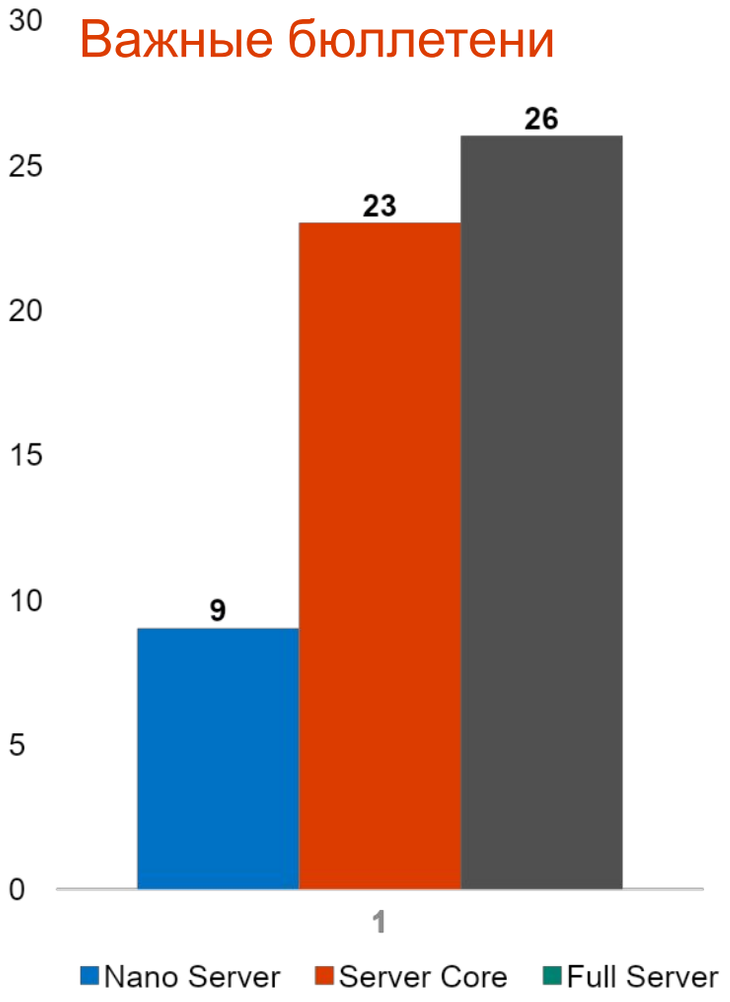
- Облачная структура и инфраструктура (кластеризация, хранилище, сеть)
- Созданные для облака приложения (PaaS v2, ASP.NET v5)
- ВМ и контейнеры (Hyper-V и Docker)

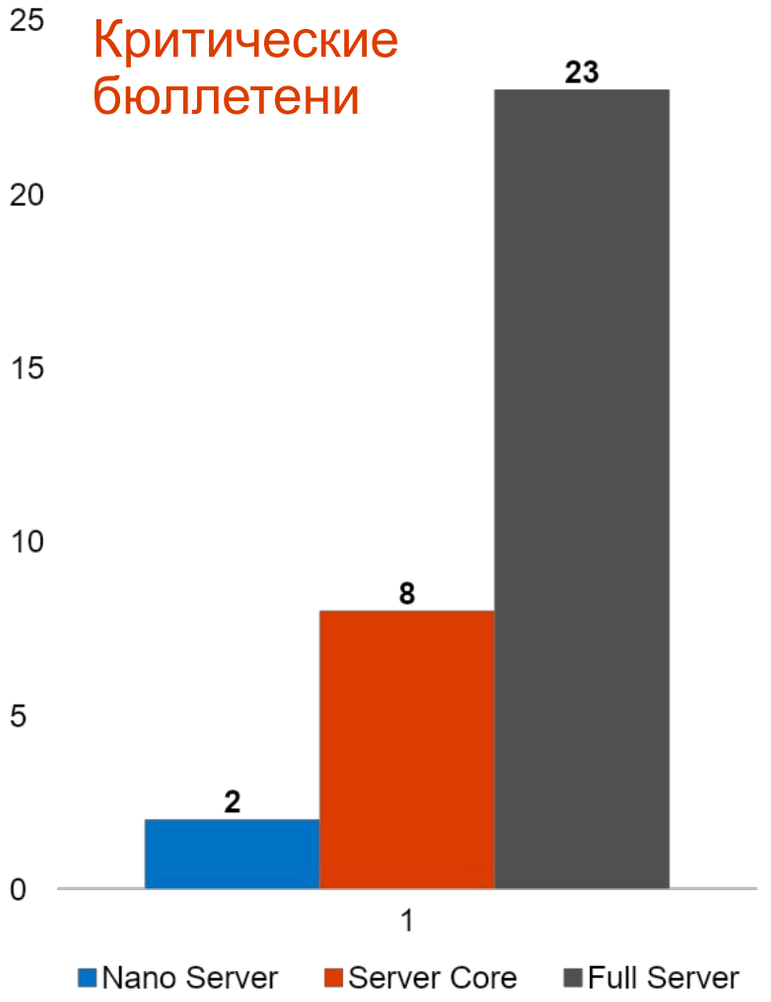
Развитие идеи Server Core

- Роли и компоненты находятся вне Nano Server
- В образе ОС отсутствуют соответствующие файлы и метаданные
- Отдельные пакеты устанавливаются как приложения
- Полная поддержка драйверов
- Защита от вредоносных программ



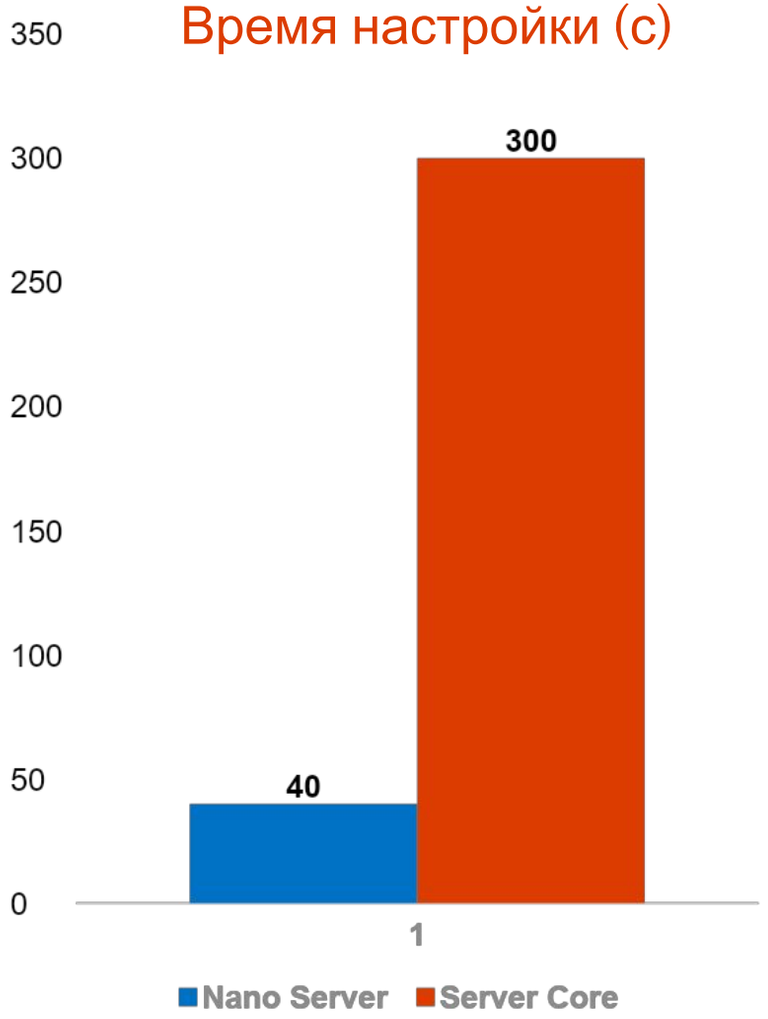
Улучшения в обслуживании*

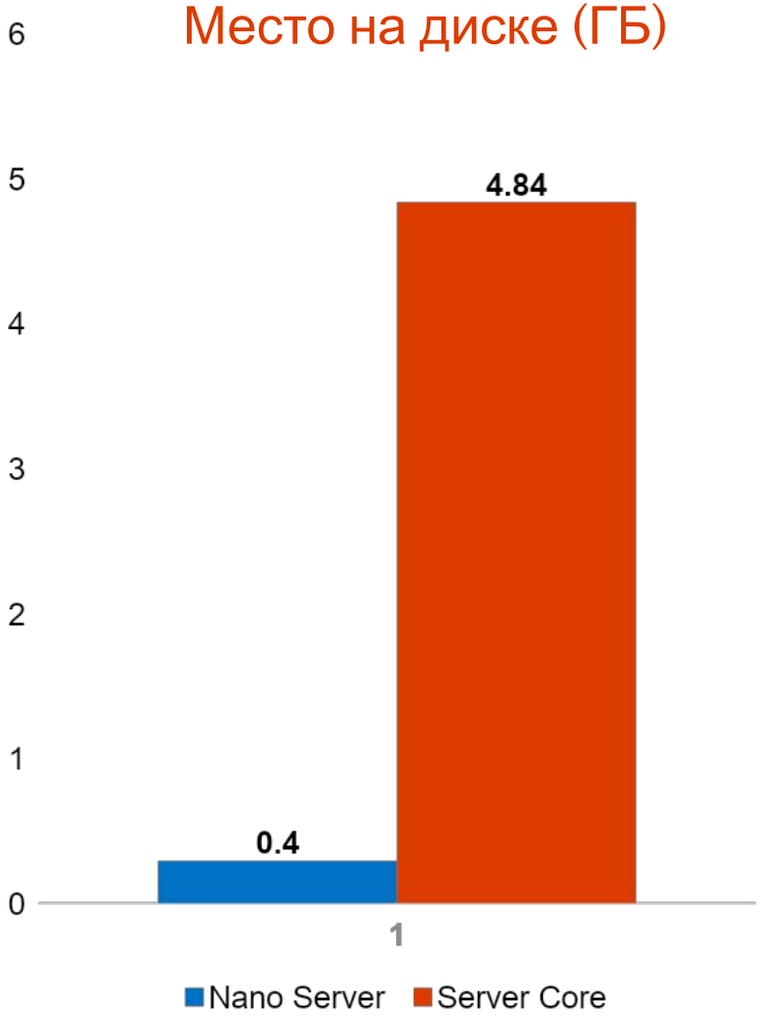


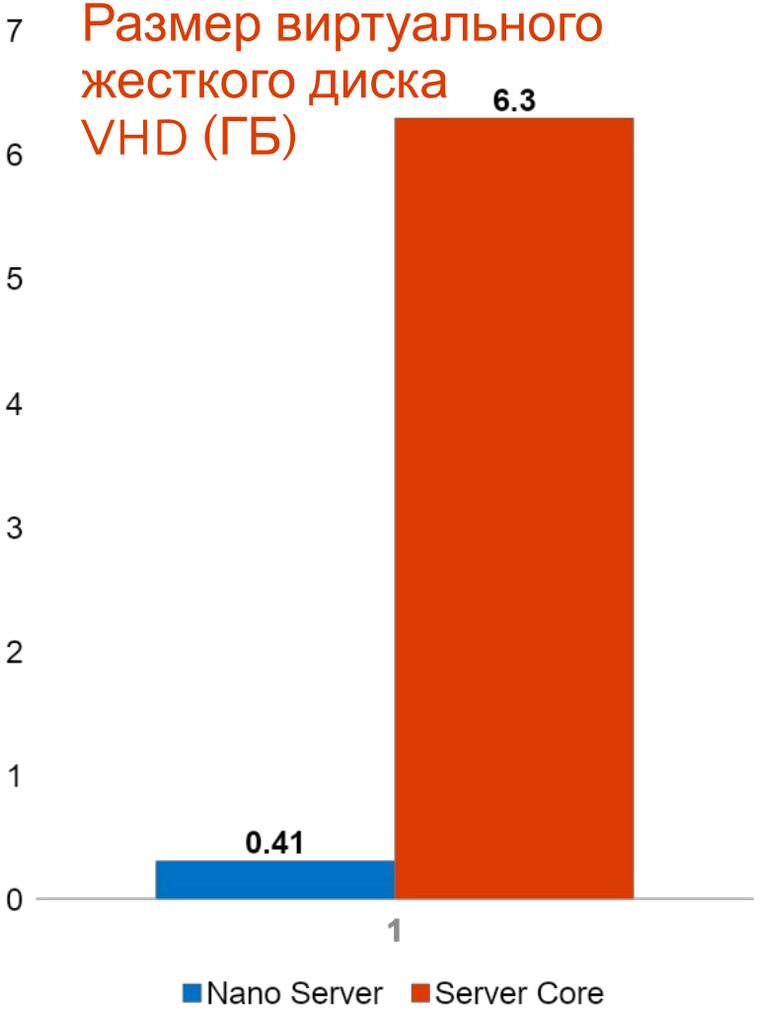


* На основе анализа пакетов исправлений, выпущенных в 2014 году

Улучшения в развертывании







Начало работы
с Nano Server

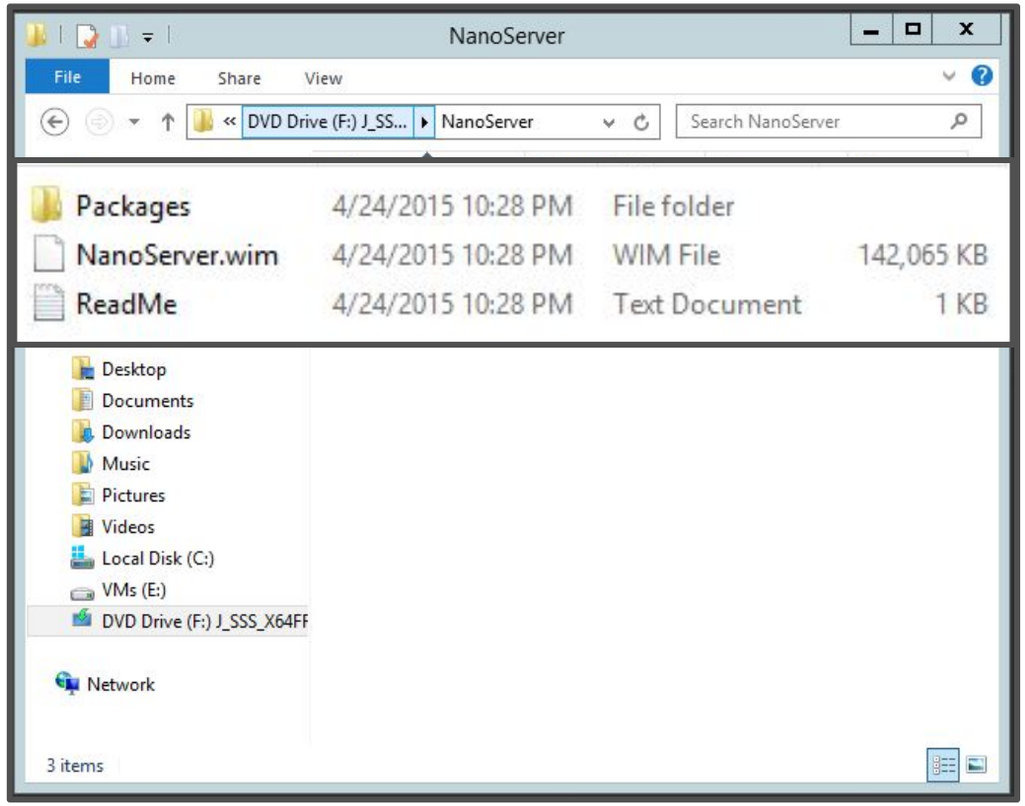
Начало работы

Nano Server — это вариант установки

Как Server Core, но его нельзя выбрать при установке
Требуется выборка нужных драйверов
Размещается на носителе Windows Server

Доступно в версии

Windows Server Technical Preview



Nano Server

Модель zero-footprint

- Серверные роли и дополнительные функции находятся вне Nano Server
- Нужные пакеты устанавливаются как приложения

Ключевые роли и функции

- Hyper-V, системы хранения (SoFS) и кластеризация
- Core CLR, ASP.NET 5 и PaaS

Полная поддержка драйверов Windows Server

Защита от вредоносных программ в виде необязательного компонента

Быстрый запуск Nano Server

- Сценарии, размещенные в каталоге Nano Server, позволяют с легкостью создать собственный образ Nano Server
  - New-NanoServerImage.ps1
  - Convert-WindowsImage.ps1
- Сценарии позволяют создавать образы Nano Serve для различных систем:

ФИЗИЧЕСКИЙ КОМПЬЮТЕР

ВИРТУАЛЬНАЯ МАШИНА

Настройка Nano Server

Обязательно

- Добавить корректный набор драйверов для устройств или виртуальной машины*
- Добавить необходимые роли или компоненты роли сервера*
- Настроить пароль администратора*
- Преобразовать WIM в VHD*

Необязательно

- Задать имя компьютера*
- Выполнить команды при первой загрузке, например задать статический IP-адрес
- Присоединить к домену*
- Двухвариантная загрузка
- Включить службы аварийного управления (EMS)*
- Установить агенты и инструменты

* Поддерживается New-NanoServerImage.ps1

Роли и компоненты Nano Server

В каталоге Nano Server есть подкаталог packages

Роль или компонент	Файл пакета
Роль Hyper-V	Microsoft-NanoServer-Compute-Package.cab
Отказоустойчивая кластеризация	Microsoft-NanoServer-FailoverCluster-Package.cab
Роль файлового сервера и другие компоненты хранилища	Microsoft-NanoServer-Storage-Package.cab
Защитник Windows (средство борьбы с вредоносными программами) и файл сигнатур по умолчанию	Microsoft-NanoServer-Defender-Package.cab
Драйверы OEM: выберите драйверы, поставляемые с Server Core	Microsoft-NanoServer-OEM-Drivers-Package.cab
Библиотеки обратной совместимости для приложений, например стандартные платформы приложений, в т. ч. Ruby, Node.js и т. п.	Microsoft-OneCore-ReverseForwarders-Package.cab
Драйверы Hyper-V для гостевых систем, позволяющие размещать Nano Server как виртуальную машину	Microsoft-NanoServer-Guest-Package.cab

Dism /Add-Package /PackagePath:.\packages\<package>

Dism /Add-Package /PackagePath:.\packages\en-us\<package>

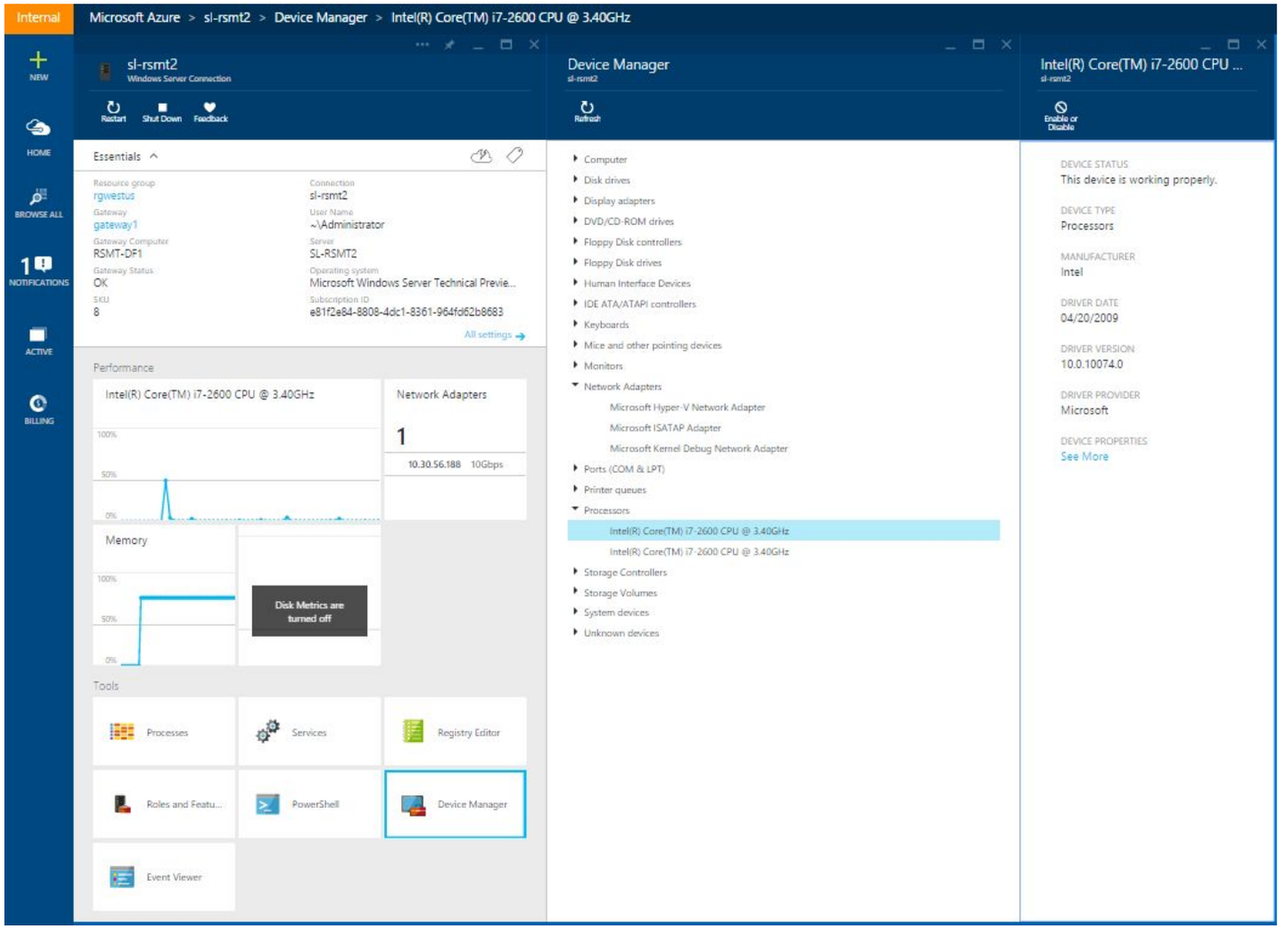
Удаленное управление
Nano Server

Удаленное управление Nano Server

Графические средства удаленного управления и веб-инструменты	Удаленное взаимодействие с PowerShell	Управление ВМ и контейнерами	Развертывание и мониторинг	Партнеры и платформы
• Диспетчер сервера • Инструменты портала Azure • Диспетчер задач • Редактор реестра • Проводник • Конфигурация сервера • Просмотр событий • Диспетчер дисков • Управление устройствами и драйверами • Производительность • Пользователи и группы	• Базовый механизм PowerShell, язык и командлеты • Командлеты Windows Server (сеть, хранилище и т. п.) • PowerShell DSC • Удаленная передача файлов • Удаленная разработка и отладка сценариев • Веб-доступ к PowerShell	• Диспетчер Hyper-V • Командлеты Hyper-V • PowerShell Direct через PSRP • Поддержка CimSession • Docker • Агент и консоль SCVMM • Агенты и консоли сторонних поставщиков	• Поддержка сетевых операций DISM и VHD • Автоматическая установка • Интеграция с Visual Studio • Диспетчер локальных конфигураций DSC • Обработка событий установки и загрузки • Агент SCOM • Инструменты VSO App Insights • Инструменты Azure Op Insights	• Интеграция с Chef • .NET Core и CoreCLR • ASP.NET 4.5. • Python, PHP, Ruby, Node.js • Классы PowerShell • Анализатор сценариев PS • Коллекция PowerShell • PowerShellGet

Инструменты для удаленного управления сервером

- Больше не нужно сидеть перед сервером
- На основе веб-технологий
- Замена локальных инструментов
  - Диспетчер задач, редактор реестра
  - Просмотр событий, диспетчер устройств
  - Sconfig
  - Панель управления, Проводник
  - Системный монитор, диспетчер дисков
  - Управление пользователями/группами
- Управление Server Core и Server с помощью графического пользовательского интерфейса



Core PowerShell в Nano Server

- Разработано на основе среды выполнения .NET Core
  Экономичный, модульный, кросс-платформенный инструмент с открытым исходным кодом
- Занимает меньше места на диске — всего 55 МБ
  CoreCLR (45 МБ) + PowerShell (8 МБ) + модули (2 МБ)
- Все возможности языка, ограниченный набор компонентов, большая часть командлетов
- Удаленное управление PowerShell (только на стороне сервера)
  - Обратная совместимость с существующими клиентами удаленного управления PowerShell (до PS 2.0)
  - Удаленная передача файлов через PowerShell
  - Удаленная разработка сценариев и отладка в ISE
- Командлеты для управления компонентами Nano Server

Устранение неполадок
Nano Server

Сбор событий установки и загрузки

Повышенная прозрачность среды

Повышенная прозрачность

Удаленный просмотр ошибок отладки, событий процесса развертывания, загрузчика, ОС и служб

Устранение неполадок без физического доступа

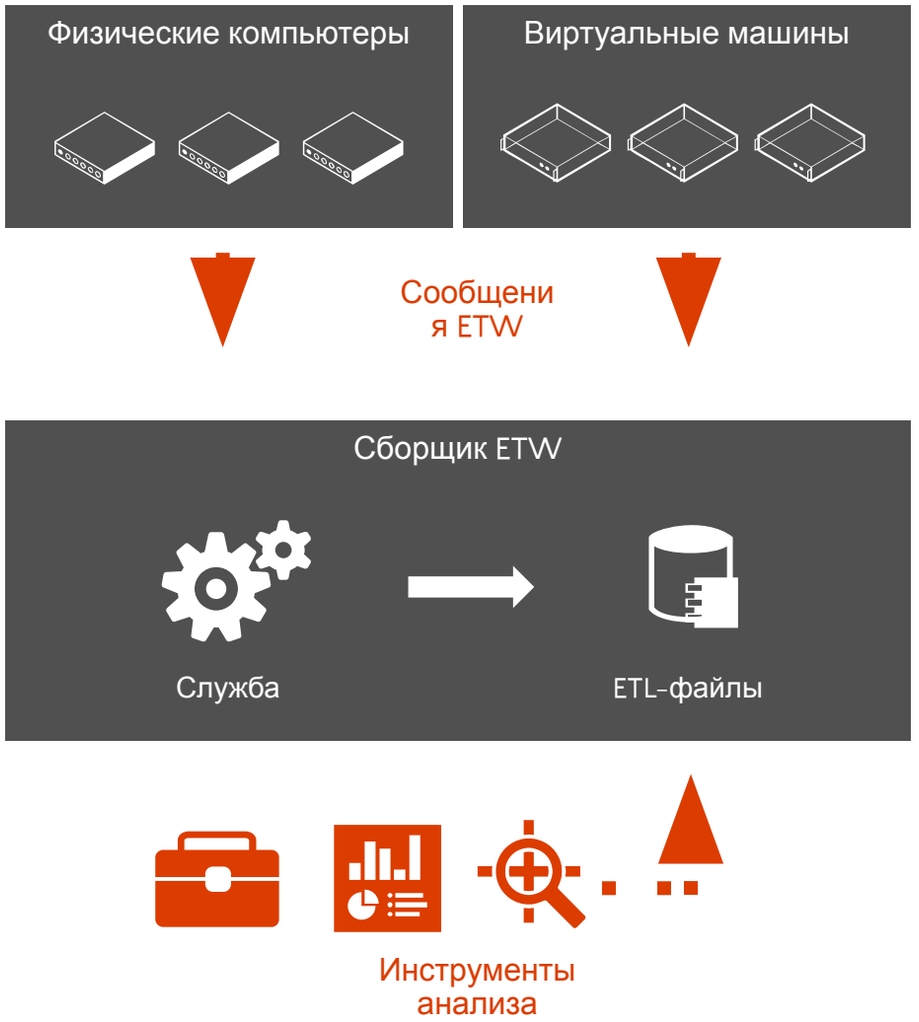
Простая настройка

Поддерживаются как физические компьютеры, так и виртуальные машины

Требуется небольшое количество дополнительных ресурсов; можно установить с помощью PowerShell или файла автоматической установки

Уменьшенное время восстановления после отказа (MTTR)

Доступ к данным осуществляется в реальном времени; информацию можно соотносить с другими диагностическими данными, чтобы быстрее выявлять проблемы



Консоль аварийного управления

- Добавлена в версии Technical Preview 3
- Является локальным механизмом доступа к основным настройкам конфигурации и сети:
  - Имя компьютера
  - Имя домена или рабочей группы
  - Ipconfig/all информация для каждого сетевого адаптера
- В будущем выпуске запланирована поддержка изменения сетевых настроек