



Windows Server 2022

Современная серверная
инфраструктура



Windows Server 2022. Современная серверная инфраструктура

Модернизация серверной инфраструктуры для соответствия меняющимся требованиям бизнеса и ИТ-среды

- **Виртуализация** с использованием Hyper-V и средств виртуализации
- **Высокая доступность** с отказоустойчивой кластеризацией
- **Программно-определяемая инфраструктура** с Windows Server 2022 Datacenter
- **Функции гибридного облака** со службами Azure

Виртуализация будет полезна вашим клиентам

Более эффективное использование оборудования



Консолидируйте серверы и рабочие нагрузки на меньшем количестве более производительных физических компьютеров — это позволит сократить потребление электроэнергии и сэкономить физическое пространство.

Повышение устойчивости бизнеса



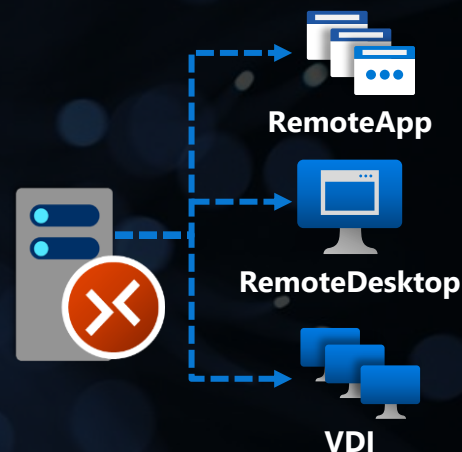
Минимизируйте последствия плановых и внеплановых простоев рабочих нагрузок.

Создание и развертывание частного облака



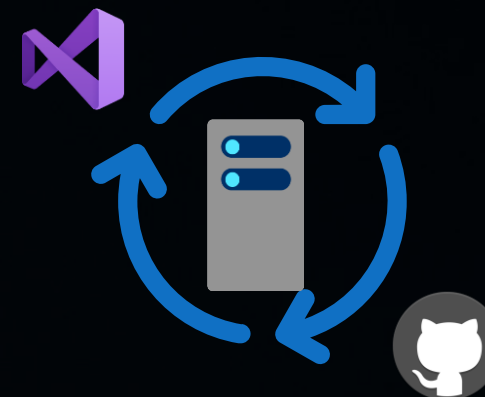
Реализуйте более гибкие ИТ-службы, доступные по требованию, перейдя на использование общих ресурсов (или расширив использование этих ресурсов). Регулируйте использование ресурсов в соответствии с потребностями.

Запуск служб удаленных рабочих столов



Централизованная стратегия использования рабочих столов на базе VDI позволяет повысить гибкость бизнес-процессов и уровень безопасности данных.

Повышение эффективности процессов разработки и тестирования



Организуйте различные вычислительные среды без приобретения и поддержки всего того оборудования, которое потребовалось бы при использовании только физических систем.

Архитектура Hyper-V

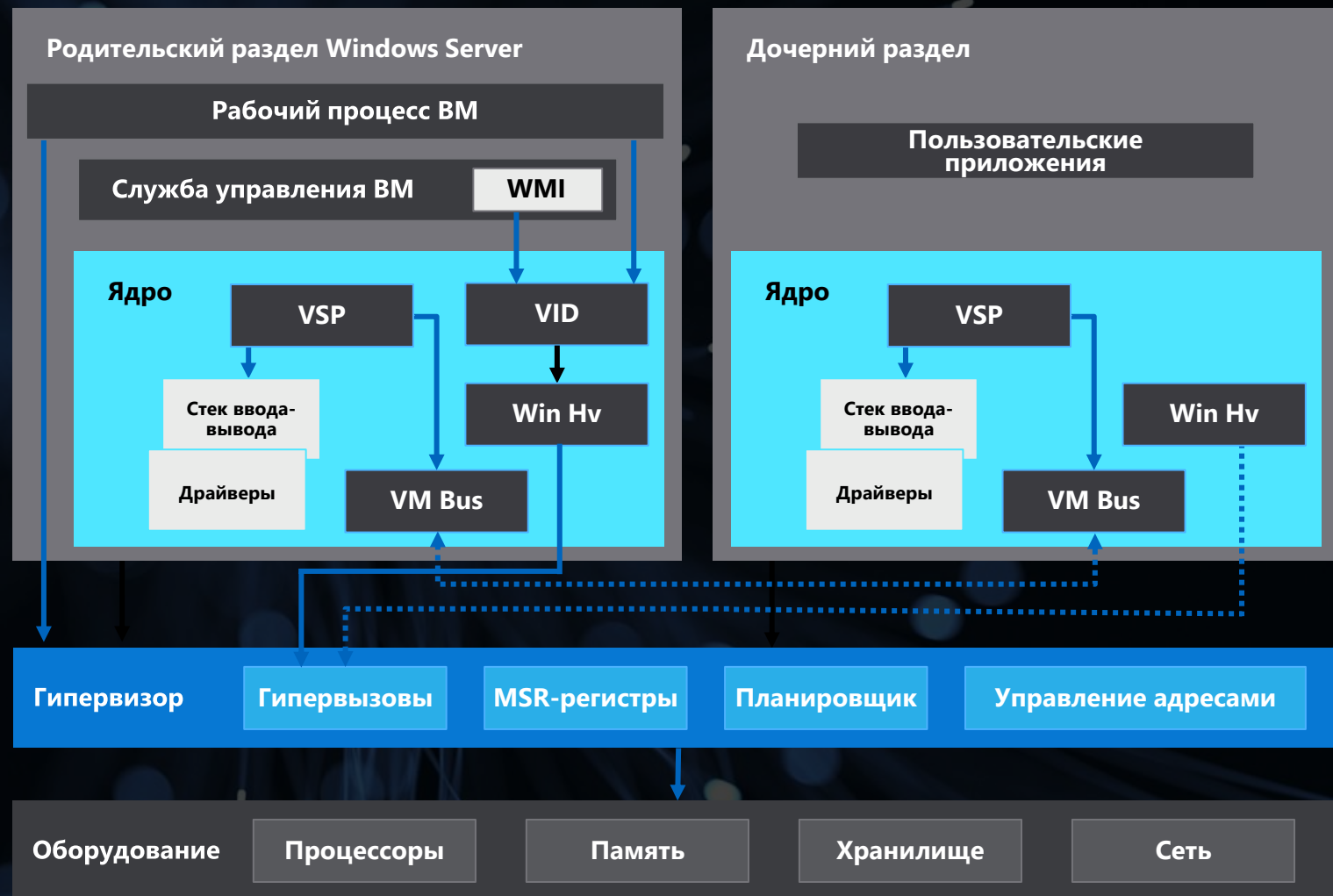
Hyper-V — это платформа аппаратной виртуализации корпорации Майкрософт

Hyper-V — это технология виртуализации на базе гипервизора для некоторых x64-версий Windows.

Гипервизор играет главную роль в процессе виртуализации. Он представляет собой платформу виртуализации для определенных процессоров, позволяющую нескольким изолированным операционным системам одновременно работать на одной аппаратной платформе.

Компоненты платформы:

- Гипервизор Windows
- Служба управления виртуальными машинами Hyper-V
- Шина VMbus
- Поставщик служб виртуализации
- Драйвер виртуальной инфраструктуры



Консоль диспетчера Hyper-V

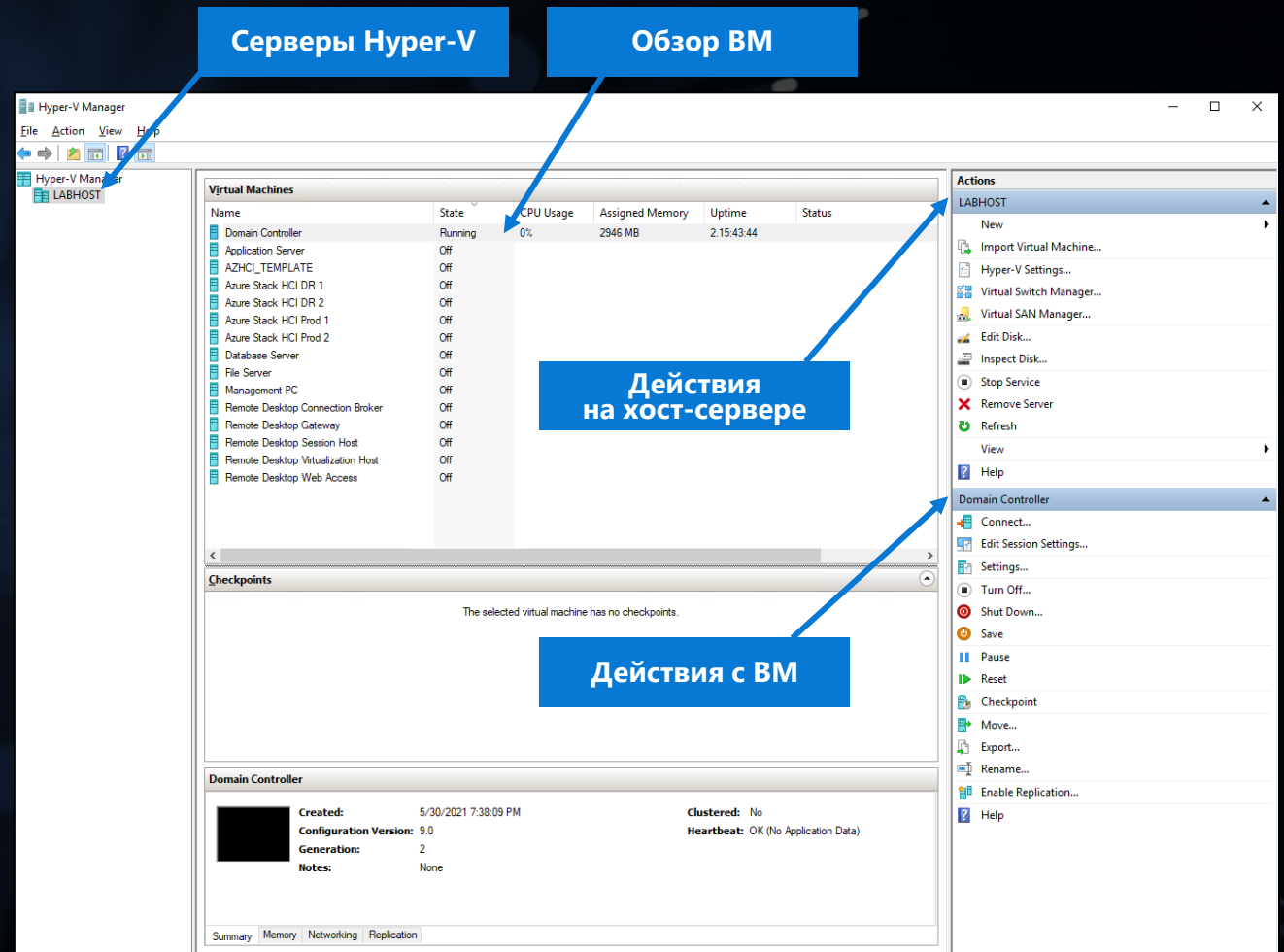
Наиболее распространенный инструмент, используемый для взаимодействия с Hyper-V

Основные функции диспетчера Hyper-V:

- Настройка параметров функций Hyper-V, например динамической миграции
- Создание, удаление и настройка виртуальных машин Hyper-V
- Создание, удаление и контроль виртуальных жестких дисков
- Прямое управление функциями виртуальной машины
- Создание, удаление, применение и отмена контрольных точек
- Настройка и контроль репликации Hyper-V

Диспетчер Hyper-V состоит из трех панелей:

- **Левая панель** содержит список всех соединений с серверами Hyper-V.
- На **центральной панели** отображается информация о виртуальных машинах, размещенных на сервере Hyper-V, выбранном на левой панели.
- На **правой панели** могут отображаться действия, относящиеся к серверу Hyper-V или любой виртуальной машине, выбранной на центральной панели.



Функции безопасности Hyper-V

Диспетчер Hyper-V помогает защитить «состояние» и «данные» виртуальных машин

Безопасная загрузка

- Предотвращение запуска неразрешенных микропрограмм, операционных систем или драйверов UEFI во время загрузки.
 - Включено по умолчанию.

Поддержка шифрования

- **Включение доверенного платформенного модуля (TPM)** — предоставление виртуальной машине доступа к виртуализированному модулю TPM.
 - Шифрование диска виртуальной машины с помощью функции BitLocker.
- **Шифрование состояния и трафика миграции виртуальной машины** — шифрование сохраненного состояния VM и трафика при динамической миграции VM.

Политика безопасности

Включение экранирования — запрет функций управления, таких как подключение к консоли, PowerShell Direct, а также некоторых компонентов интеграции.



Виртуальная сеть

Диспетчер Hyper-V помогает защитить «состояние» и «данные» виртуальных машин

Базовые сетевые возможности в Hyper-V весьма просты

Существует всего 2 компонента виртуальной сети:

Виртуальный коммутатор

Виртуальный коммутатор подключает виртуальные машины к любой Ethernet-сети.

В Hyper-V имеется 3 типа виртуальных коммутаторов:

1. **Внешний** — подключается к проводной или беспроводной физической сети путем привязки к физическому сетевому адаптеру.
2. **Внутренний** — подключается к сети, которая может использоваться только виртуальными машинами, работающими на хост-сервере, и между хост-сервером и виртуальными машинами.
3. **Частный** — подключается к сети, которая может использоваться только виртуальными машинами, работающими на хост-сервере.

Виртуальный сетевой адаптер

Виртуальный коммутатор устанавливает соединение через свой определенный порт.

Имеется 2 типа виртуальных сетевых адаптеров:

1. **Специальный сетевой адаптер Hyper-V** — разработан специально для Hyper-V и требует наличия драйвера, который входит в комплект поставки.
2. **Устаревший сетевой адаптер** — эмулирует адаптер на базе Intel 21140 и используется для определенных целей.

Виртуальные жесткие диски

Определение вариантов организации хранилища для виртуальных машин

Стоит обратить внимание на следующие факторы:

Производительность

Виртуальные жесткие диски (VHD) могут располагаться в локальном или удаленном хранилище. В случае удаленного хранилища необходимо обеспечить достаточную пропускную способность и минимальное время задержки. Если сетевое соединение с хранилищем медленное, результатом будет низкая производительность виртуальных машин.

Устройство хранения, на котором располагаются VHD, должно обладать отличными характеристиками ввода-вывода. Для обеспечения максимальной производительности и избыточности используйте гибридные твердотельные накопители (SSD) в массивах RAID 1+0.

Избыточность

Том, на котором хранятся файлы VHD, должен быть отказоустойчивым независимо от того, хранится ли VHD на локальном диске или на удаленном устройстве NAS или SAN. Сбои в работе жестких дисков — не такое редкое явление, однако виртуальная машина и хост Hyper-V должны сохранять работоспособность после подобных инцидентов. Замена сбойных дисков не должна влиять на работу хоста Hyper-V или виртуальных машин.

Поддержка корпоративных решений для хранения данных

Поддержка оптоволоконного канала для сетей SAN

Адаптер оптоволоконного канала Hyper-V — это виртуальный аппаратный компонент, который можно добавить в виртуальную машину для обеспечения доступа к хранилищу в сетях хранения данных через оптоволоконный канал. Для развертывания виртуального оптоволоконного канала:

- на хосте Hyper-V необходимо настроить адаптер шины (HBA) оптоволоконного канала или сетевой адаптер Fiber Channel over Ethernet (FCoE);
- адаптер шины (HBA) оптоволоконного канала должен иметь драйвер, поддерживающий виртуальный оптоволоконный канал.

Виртуальные адаптеры оптоволоконного канала поддерживают виртуализацию портов через открытие портов адаптера шины в гостевой ОС. Это позволяет виртуальной машине получать доступ к SAN, используя стандартное WWN-имя, связанное с данной VM.

Хранение виртуальных машин на файловых ресурсах SMB 3.0

Hyper-V поддерживает хранение данных виртуальной машины (например, конфигурационных файлов VM, контрольных точек и виртуальных жестких дисков) на файловых ресурсах SMB 3.0.

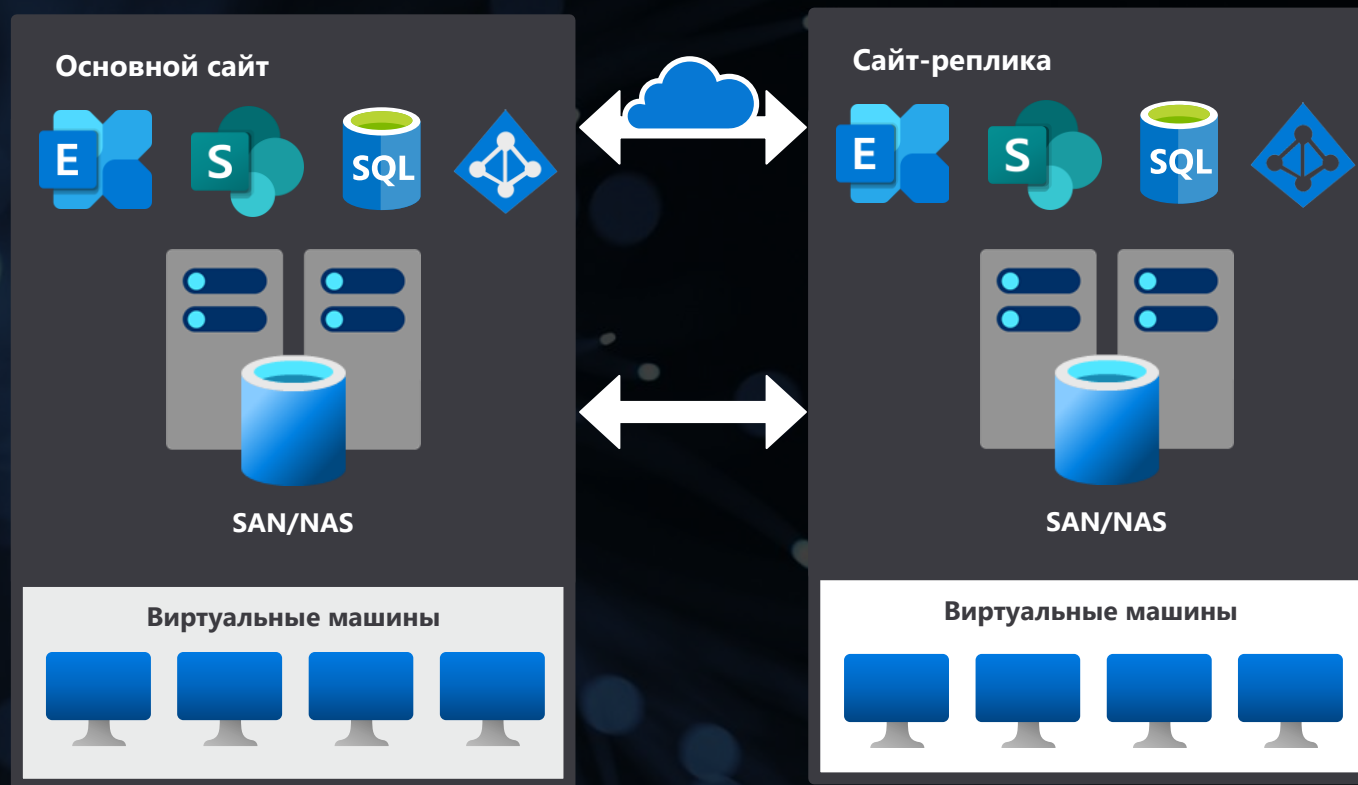
Чтобы обеспечить высокую доступность общих файловых ресурсов, используйте масштабируемый файловый сервер (SOFS). SOFS предоставляет резервные серверы для доступа к файловым ресурсам.

Реплика Hyper-V

Внедрение доступного по цене решения BCDR для виртуальных сред

Защита от потери данных при перебоях в работе сайта

- Копирование работающих виртуальных машин между хостами:
 - Если основной хост недоступен, для поддержания рабочих нагрузок доступна реплика VM.
- Репликация виртуальных машин на другой сайт, на ресурс другого хостинг-провайдера или в службу Azure:
 - Если произошел сбой на сайте основного сервера, реплику Hyper-V можно использовать для переключения VM на сервер-реплику на сайте дополнительного сервера.
 - Это обеспечит минимальный простой.



Варианты отработки отказов

Три типа отработки отказов

Тестовая отработка отказа

Задача, позволяющая размещать VM на сервере-реплике во время работы основной VM без прерывания репликации.

Может быть инициирована только на реплицированной VM.

При инициировании тестовой отработки отказа на реплицированной VM создается новая контрольная точка, которую можно использовать в качестве точки восстановления.

Тестовая виртуальная машина по умолчанию остается отключенной во избежание конфликтов.

Плановая отработка отказа

Может быть запущена для перемещения основной VM на сервер-реплику, например в следующих случаях:

- перед обслуживанием сайта;
- перед ожидаемым сбоем.

Потери данных не происходит, но виртуальная машина становится недоступной на некоторое время в ходе настройки.

После запланированной отработки отказа виртуальная машина будет работать на сервере-реплике и не будет реплицировать изменения на исходный хост.

Отработка отказа

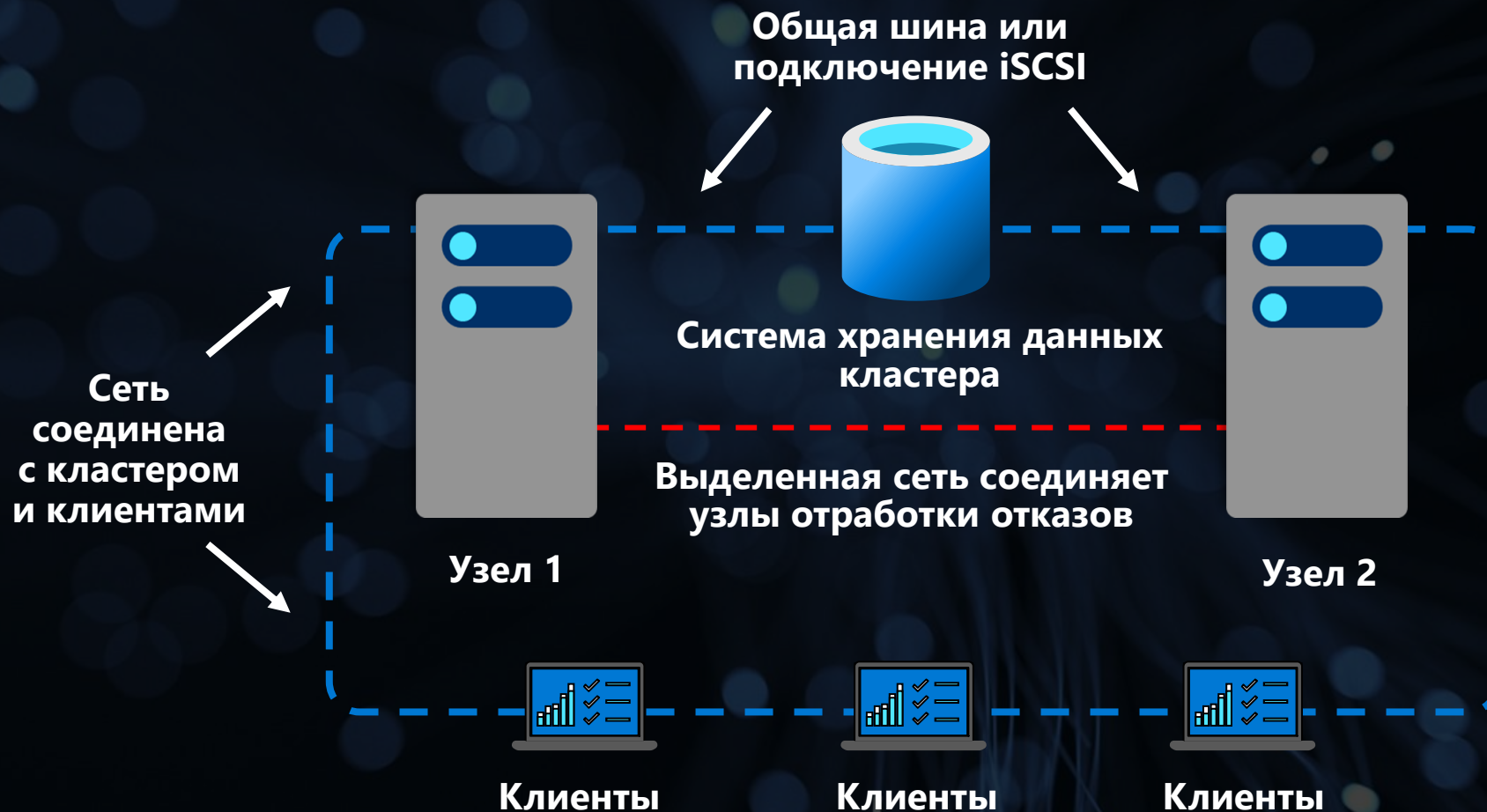
Если на основном сервере произошел сбой и основная VM перестала работать, может быть инициирована отработка отказа.

Отработка отказа может быть инициирована на сервере-реплике, на реплицированной VM и ТОЛЬКО в том случае, если основная VM недоступна или отключена.

Отработка отказа — это незапланированное событие, которое может привести к потере данных, поскольку изменения на основной VM могли быть не реплицированы до возникновения сбоя.

Отказоустойчивая кластеризация

Отказоустойчивый кластер состоит из следующих элементов:



Динамическая миграция Hyper-V

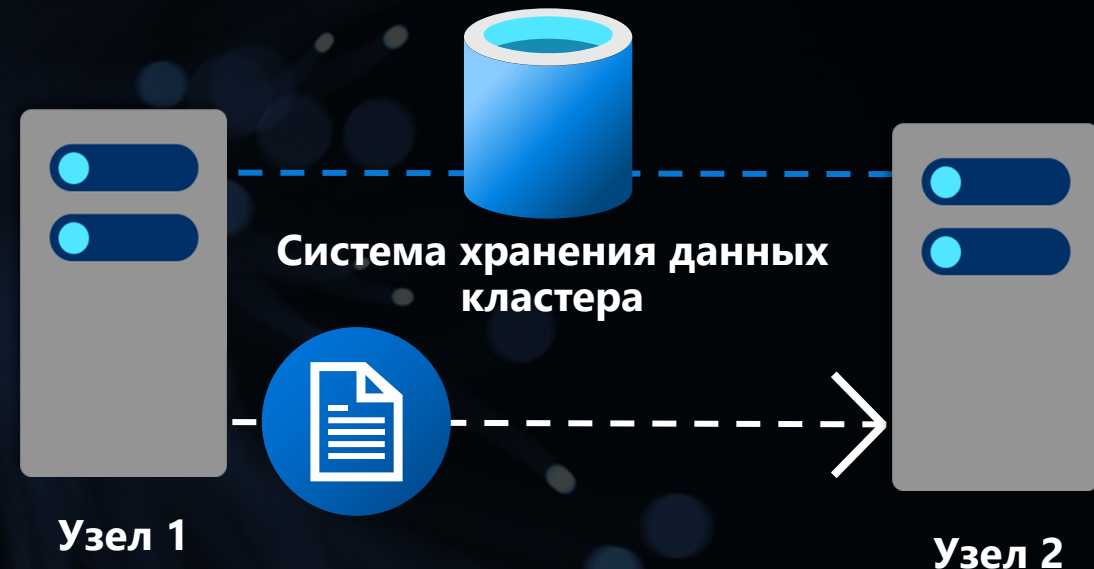
Беспроblemное перемещение работающих виртуальных машин с одного хоста Hyper-V на другой

Автономность или высокая доступность

- **Динамическая миграция «без разделения ресурсов»** — миграция работающих виртуальных машин с одного физического сервера с непосредственно подключенным хранилищем на другой сервер с непосредственно подключенным хранилищем
- **«Высокая доступность»** — использование кластеризации Hyper-V с «общим хранилищем» для создания высокодоступных виртуальных машин.

Как устроен этот процесс

1. Настройка миграции
2. Перенос содержимого памяти VM
3. Перенос состояния
4. Очистка



Что такое программно-определяемая инфраструктура?

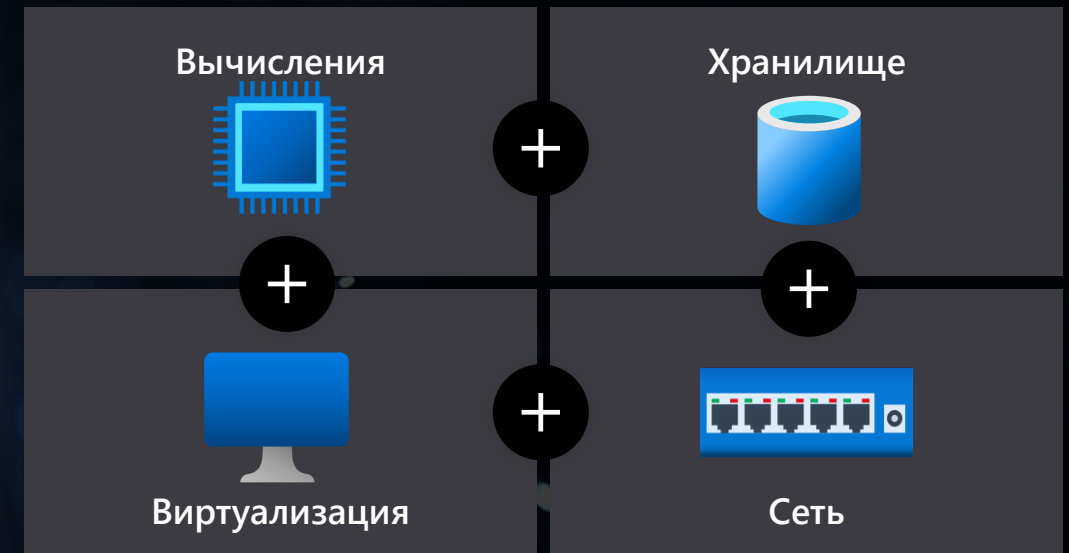
«Новое поколение» распределенных рабочих нагрузок

Программно-определяемая инфраструктура — это применяемый в Windows Server 2022 подход к гиперконвергентным решениям, в которых технологии хранения, вычислительные технологии, сетевые технологии и технологии виртуализации интегрированы в физическое устройство, управляемое как единый модуль.

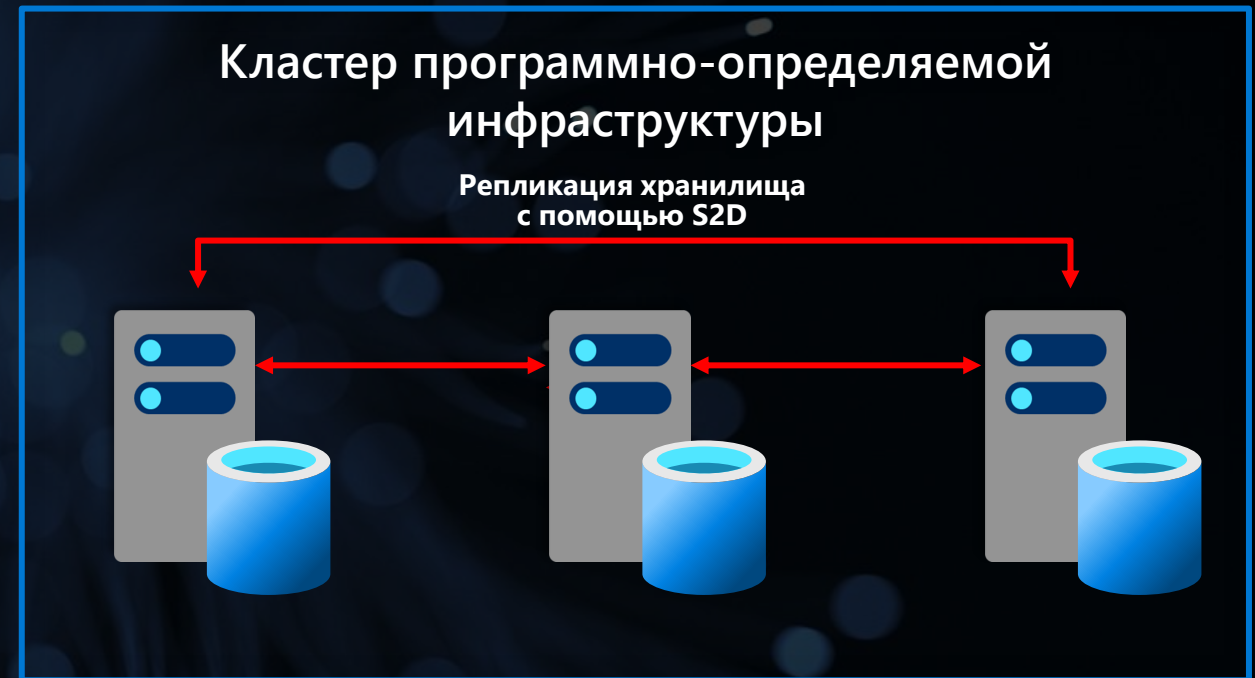
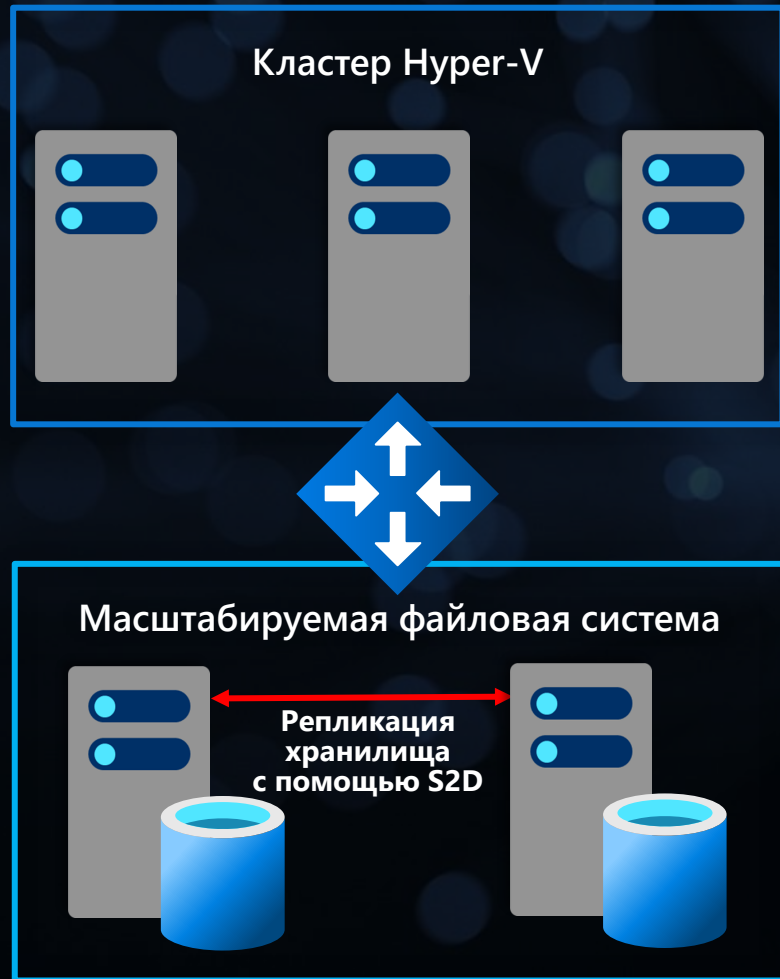
Программно-определяемые решения могут быть очень быстро и легко развернуты администраторами, а также используются ими в качестве единого центра управления всеми аппаратными и программными компонентами.

Компоненты платформы:

- Виртуализация
- Отказоустойчивая кластеризация
- Программно-определяемое хранилище
- Программно-определяемая сеть



Конвергентные и гиперконвергентные решения

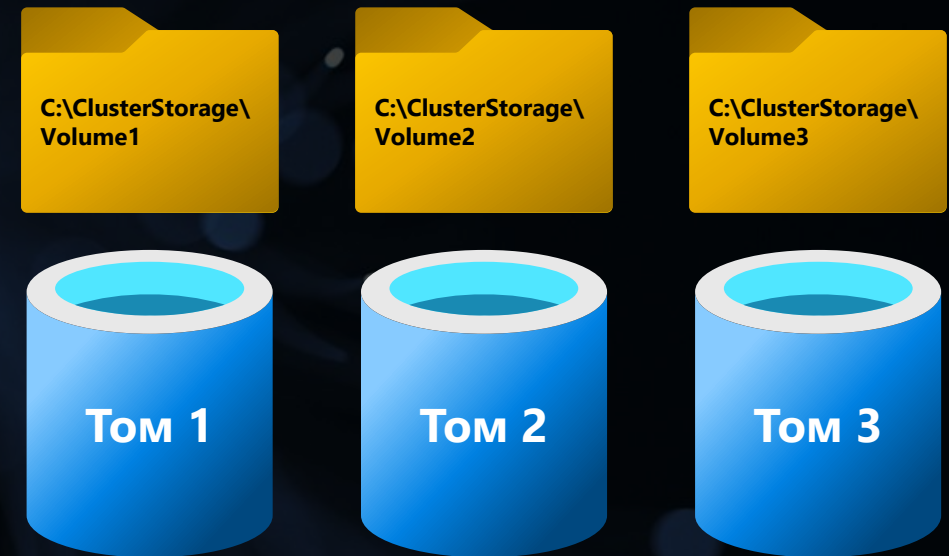


Что такое программно-определяемое хранилище?

Один из ключевых компонентов программно-определяемых решений Майкрософт

Это не продукт, а дополнительный набор функций, включающий в себя:

- Дисковые пространства
- Локальные дисковые пространства
- Общие тома кластера (CSV)
- SMB
 - SMB Multichannel
 - SMB Direct
- Масштабируемый файловый сервер (SoFS)
- Реплика хранилища



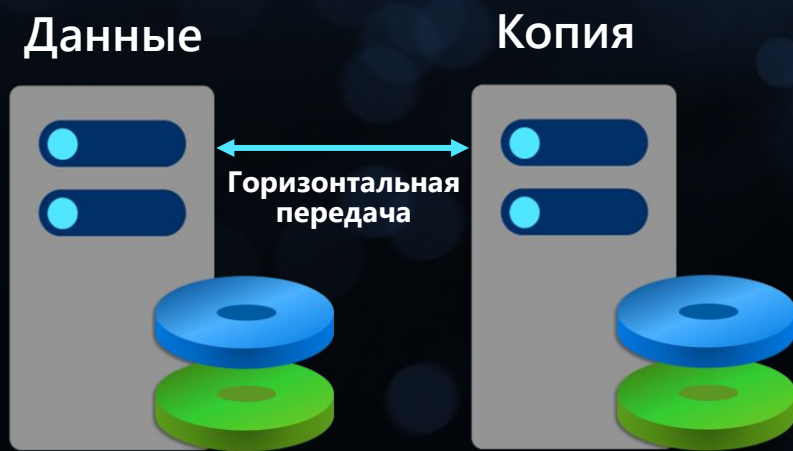
Устойчивость и зеркалирование

Обеспечение отказоустойчивого хранения данных путем создания их нескольких копий

Двустороннее зеркало

Двухсерверная конфигурация

- Записывается по 2 копии любых данных
- Эффективность хранения — 50 %
 - Для записи 1 ТБ данных требуется 2 ТБ пространства



Трехстороннее зеркало

Трехсерверная конфигурация

- Записывается по 2 копии любых данных
- Эффективность хранения — 33 %
 - Для записи 1 ТБ данных требуется 3 ТБ пространства



Четность

Обеспечение отказоустойчивости с помощью кодирования процесса удаления и защиты от ошибок

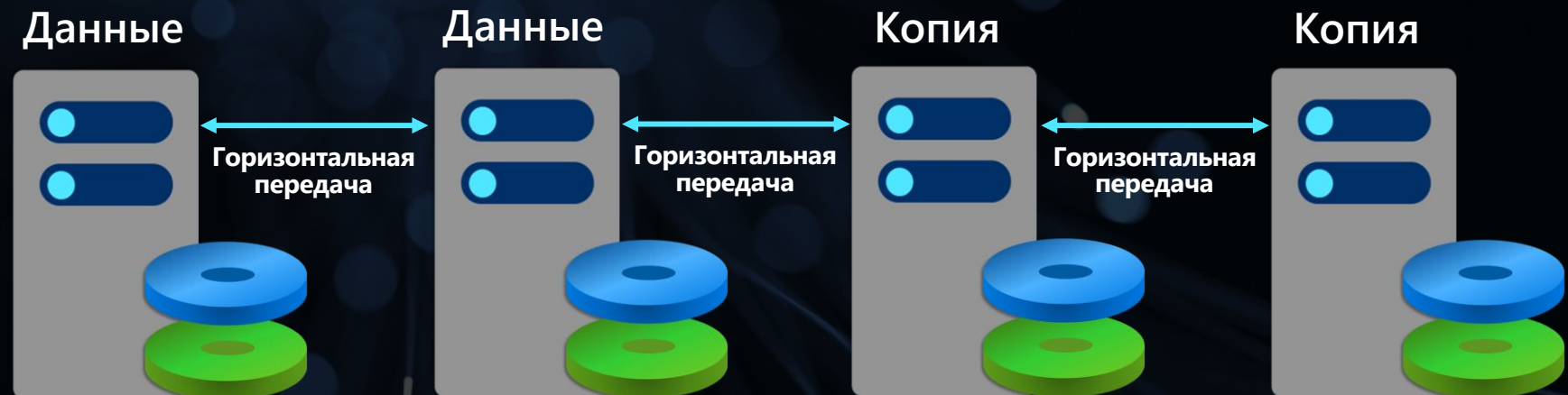
Двойная четность

Четырехсерверная конфигурация

- Записывается по 2 копии любых данных
- Масштабируемая эффективность хранения — от 50 % и выше
 - Для записи 2 ТБ данных требуется 4 ТБ пространства

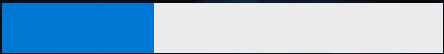




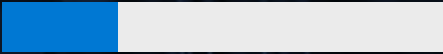
Чем больше узлов добавляется, тем выше становится эффективность хранения.

- 7 серверов => эффективность 66,7 %
- 16 серверов => эффективность до 80 %



Подбор подходящего варианта для клиентов

Выбор типа устойчивости зависит от требований рабочей нагрузки

Тип устойчивости	Эффективность хранения	Скорость	Рабочие нагрузки
Зеркало	 <p>Двустороннее зеркало: 50 % Трехстороннее зеркало: 33 %</p>	 <p>Высокая производительность</p>	<ul style="list-style-type: none">• Виртуализированные рабочие нагрузки• Базы данных• Другие высокопроизводительные рабочие нагрузки
Четность с зеркальным ускорением	 <p>Зависит от соотношения зеркалирования и четности</p>	 <p>Значительно медленнее зеркалирования, но в 2 раза быстрее, чем двойная четность Оптимально при продолжительных операциях последовательной записи и последовательного чтения</p>	<ul style="list-style-type: none">• Резервное копирование/ архивирование• Инфраструктура виртуальных рабочих столов
Двойная четность	 <p>4 сервера: 50 % 16 серверов: до 80 %</p>	 <p>Наибольшие значения задержки ввода-вывода и загрузки ЦП при записи Оптимально при продолжительных операциях последовательной записи и последовательного чтения</p>	<ul style="list-style-type: none">• Резервное копирование/ архивирование• Инфраструктура виртуальных рабочих столов

Что такое программно-определяемая сеть?

Централизованное управление сетевыми устройствами

Используйте SDN-совместимые устройства для обеспечения более глубокой интеграции в физические и виртуальные сети

- Централизованная настройка и управление физическими и виртуальными сетевыми устройствами
- Обеспечение более глубокой интеграции между виртуальными и физическими сетями с помощью следующих средств:
 - Виртуальный коммутатор Hyper-V
 - Виртуализация сети Hyper-V
 - Шлюз RAS

Программно-определяемая сеть позволяет:

- динамически создавать, защищать и подключать сеть, чтобы обеспечить соответствие растущим требованиям приложений;
- ускорить развертывание рабочих нагрузок без прерывания работы;
- предотвратить распространение уязвимостей безопасности по сети;
- задавать и контролировать политики, регулирующие работу физических и виртуальных сетей;
- последовательно внедрять сетевые политики в нужном масштабе.



Windows Server 2022: удаленная работа

Организируйте безопасную удаленную работу с учетом всех потребностей клиентов, включая виртуализированные приложения, безопасный доступ с мобильных устройств и удаленный доступ к рабочему столу

- **Доступ** к внутренним корпоративным ресурсам из любого места и с любого устройства
- **Инфраструктура виртуальных рабочих столов** со службами удаленных рабочих столов
- Доступ к приложениям и службам с помощью **удаленного рабочего стола**
- **Масштабирование** в Azure для гибридных развертываний

Службы удаленных рабочих столов

Оптимальная платформа для создания решений по виртуализации для любых потребностей клиентов

Локальный, облачный или гибридный вариант

Локальное развертывание, развертывание в Azure либо использование гибридной стратегии, когда службы существуют в обоих вариантах.

Доступ из любого места

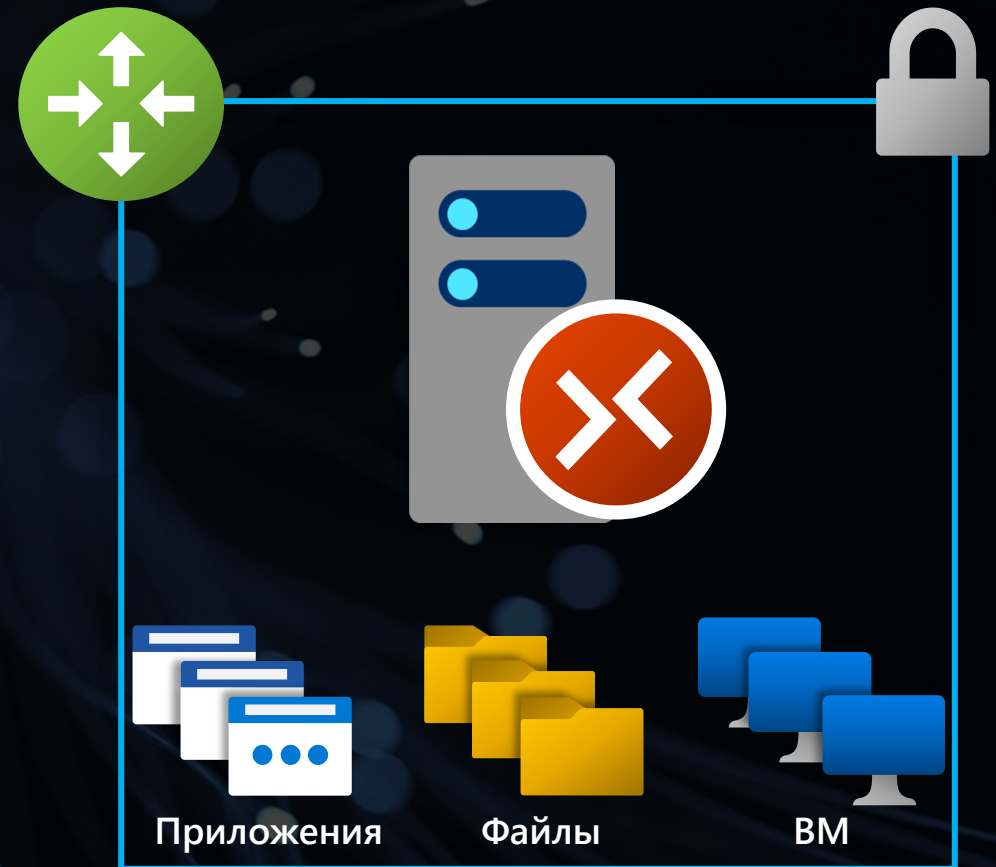
Через шлюз удаленных рабочих столов конечный пользователь может безопасно подключаться к ресурсам внутренней сети, находясь за периметром корпоративного брандмауэра

Сеансовая виртуализация

Используйте вычислительную мощь Windows Server для создания экономически выгодной многосеансовой среды для запуска повседневных рабочих нагрузок пользователей.

Инфраструктура виртуальных рабочих столов

Используйте клиент Windows, чтобы обеспечить высокую эффективность работы, совместимость приложений и знакомую пользователям среду, к которой они привыкли при работе с Windows.



Постоянно работающая виртуальная частная сеть (Always On VPN)

Единое целостное решение для удаленного доступа

Интеграция с платформой

Решение Always On VPN обеспечивает улучшенную интеграцию с операционной системой Windows и решениями сторонних производителей и является надежной платформой, поддерживающей огромное множество продвинутых сценариев подключения.

Безопасность

Always On VPN имеет новые расширенные функции безопасности, позволяющие вводить ограничения по типу трафика, указывать, какие приложения могут использовать VPN-соединение и какие методы проверки подлинности можно использовать для установки соединения.

Сетевые возможности VPN

Решение Always On VPN с туннелем между устройствами или без него обеспечивает возможность автоматического подключения к VPN-сети.

Средства управления сетью

Always On VPN позволяет администраторам задавать политики маршрутизации на более детальном уровне — вплоть до уровня отдельных приложений, что идеально подходит для бизнес-приложений, которым требуется специальный удаленный доступ.



Windows Server 2022: гибридный центр обработки данных

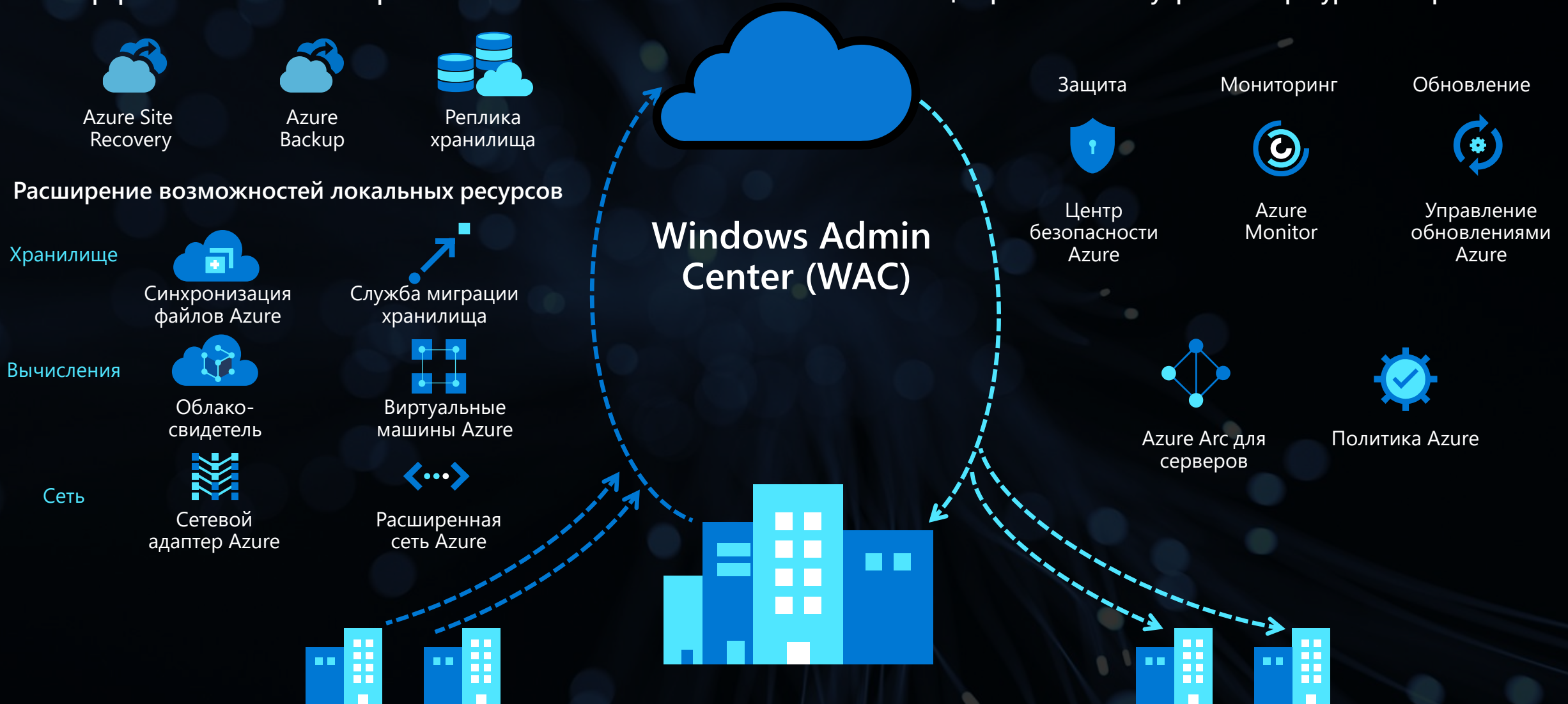
Используйте Azure для служб с простым управлением, которые расширяют ваш центр обработки данных до общедоступного облака

- **Оптимизация расходов на ИТ-среду** за счет использования Azure Backup и отказа от устаревших решений для резервного копирования
- **Репликация** виртуальных машин в Azure для целей резервного копирования и хранения
- **Устранение последствий сбоев** с помощью Azure Site Recovery

Windows Server 2022: гибридный центр обработки данных

Непрерывность бизнеса и аварийное восстановление

Централизованное управление ресурсами через Azure



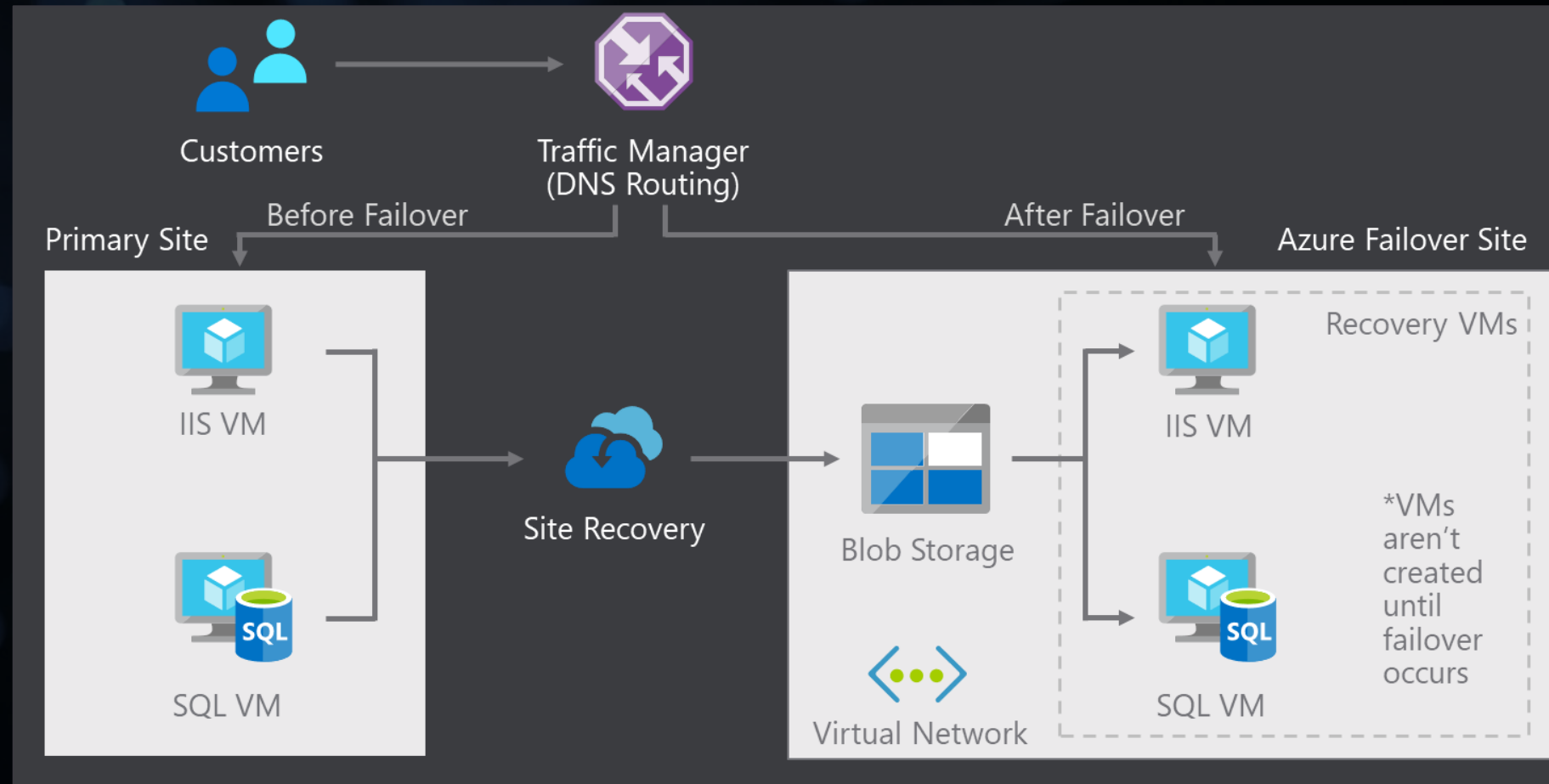
Azure Site Recovery

Сведение простоев к минимуму с Azure Site Recovery

Компании малого и среднего бизнеса могут **использовать облако** для реализации экономически эффективной стратегии аварийного восстановления, которая отличается безопасностью, высокой доступностью, наличием исправлений и обновлений.

Расширьте свой центр обработки данных в Azure с помощью следующих управляемых служб Azure:

- **Azure Site Recovery**
- **Диспетчер трафика**
- **Виртуальная сеть**
- **Хранилище BLOB-объектов**



Репликация хранилища в Azure для аварийного восстановления

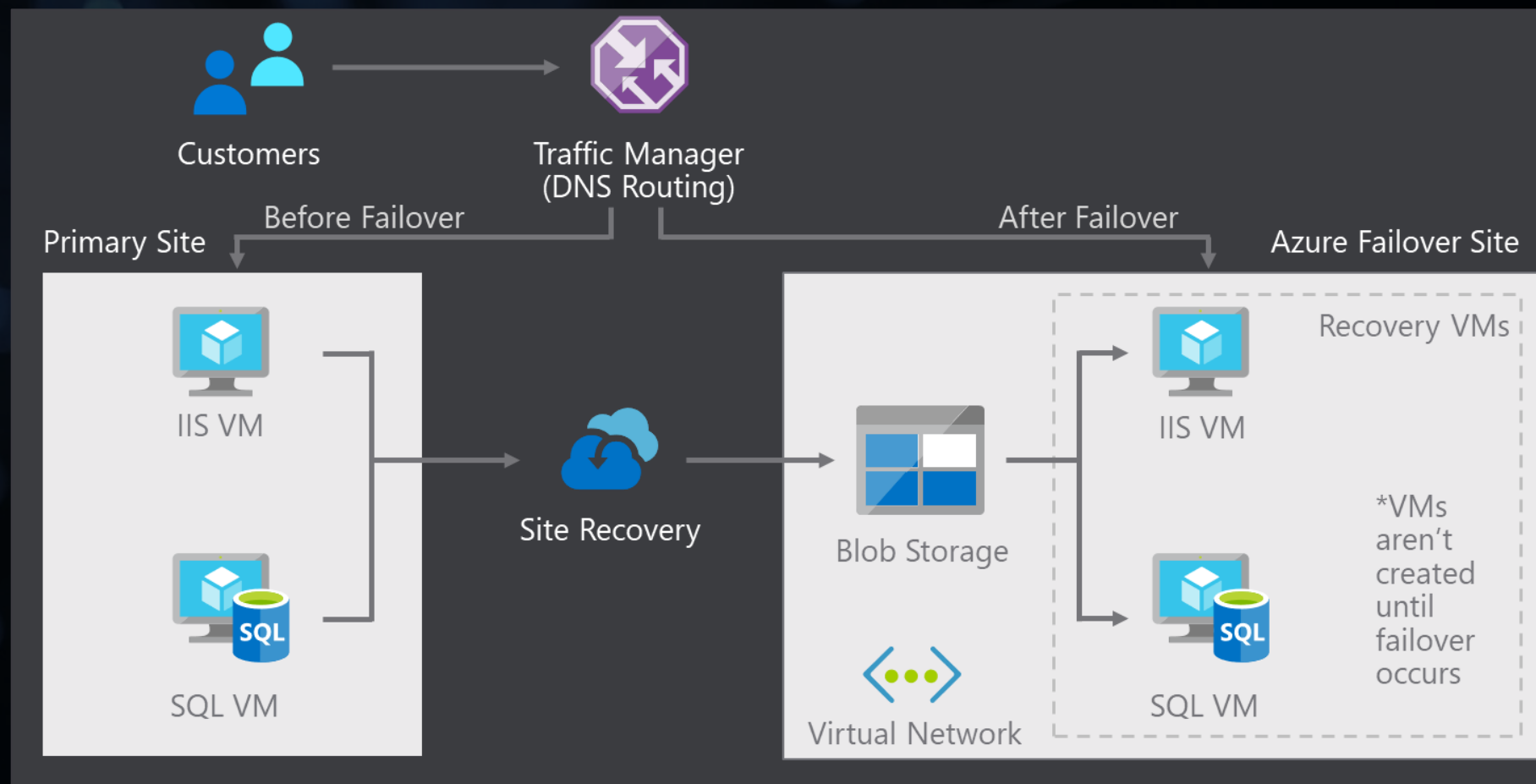
Настройка новых виртуальных машин Azure «на лету» с помощью Windows Admin Center

Компании малого и среднего бизнеса могут **использовать облако** для реализации экономически эффективной стратегии аварийного восстановления, которая отличается безопасностью, высокой доступностью, наличием исправлений и обновлений.

Репликация виртуальных машин

в Azure с помощью следующих управляемых служб Azure:

- **Виртуальные машины**
- **ExpressRoute**
- **Виртуальная сеть**
- **Хранилище BLOB-объектов**



Гибридные службы Azure с Windows Server 2022

Защита

Резервное копирование и защита локальных серверов и виртуальных машин в Azure



Защита виртуальных машин Hyper-V с помощью **Azure Site Recovery**



Резервное копирование серверов Windows в облако с помощью **Azure Backup**



Репликация виртуальных машин в Azure с помощью **реплики хранилища**

Расширение

Расширение возможностей локальных ресурсов благодаря Azure



Синхронизация файловых серверов с облаком с помощью функции **синхронизации файлов Azure**



Использование Azure для достижения кворума на отказоустойчивых кластерах с помощью **облака-свидетеля**



Подключение локальных серверов к виртуальной сети Azure с помощью **сетового адаптера**

Управление

Централизованное управление гибридной средой в Azure



Мониторинг и получение предупреждений с помощью **Azure Monitor**



Централизованное управление обновлениями ОС с помощью функции **управления обновлениями**



Повышение уровня защиты от продвинутых угроз благодаря использованию **Центра безопасности**