

Windows Server 2019

Сводная таблица сравнения технологий

Содержание

Windows Server 2019 — операционная система, соединяющая локальную среду и службы Azure	2
Как пользоваться этим сравнительным руководством	2
Сравнительная таблица	2
Уникальные возможности гибридной среды с поддержкой Azure	2
Иновационная гиперконвергентная инфраструктура	3
Расширенные возможности защиты	7
Ускоренная модернизация приложений	8
Начните работу	10

Windows Server 2019 — операционная система, соединяющая локальную среду и службы Azure

Windows Server 2019 — это операционная система, которая объединяет локальную среду и службы Azure, позволяя использовать гибридные сценарии с максимальной отдачей от существующей инфраструктуры. Повысьте безопасность и сократите риски благодаря множеству встроенных в ОС уровней защиты. Переведите свой ЦОД на гиперконвергентную инфраструктуру (HCI), чтобы достичь большей эффективности и масштабируемости. Разработчики и ИТ-специалисты смогут создавать собственные облачные приложения и улучшать существующие с помощью контейнеров и микрослужб.

Как пользоваться этим сравнительным руководством

Этот документ предназначен для руководителей высшего звена, лиц, принимающих деловые или технические решения, проектировщиков решений и ИТ-специалистов. В нем сравниваются отдельные функциональные возможности Microsoft Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 и Windows Server 2019. Это поможет заказчикам понять разницу между той версией, которую они используют сейчас, и новейшей версией Windows Server.

Сравнительная таблица

Сравнительная таблица охватывает различные области возможностей и соответствующие функции разных версий Windows Server. В таблице приведено краткое описание каждой функции, а также отмечено, насколько полно каждая функция поддерживается в разных версиях Windows Server. Ниже приведены используемые для этого условные обозначения.

Уровень поддержки функции

Функция	Не поддерживается	Частично поддерживается	Полностью поддерживается
<u>Название функции</u> — описание функции			

Уникальные возможности гибридной среды с поддержкой Azure

Расширьте центр обработки данных в Azure, чтобы получить максимальную отдачу от своих инвестиций и использовать новые возможности гибридной среды.

Переход в облако — длительный процесс. Зачастую компаниям требуется создание гибридной инфраструктуры, объединяющей локальные и облачные среды. Подход Майкрософт с применением возможностей гибридного облака — перспективная долгосрочная стратегия, поэтому он занимает центральное место в планах внедрения облачных технологий на ближайшее будущее. С переходом на Windows Server 2019 вы сможете легко интегрировать многочисленные службы Azure, включая Azure Backup, Azure File Sync, аварийное восстановление и многие другие, не прерывая работу приложений и инфраструктуры.

Функция и описание	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019
<u>Услуги по миграции хранилища</u> — помощь в инвентаризации и миграции данных, настроек безопасности и конфигураций из имеющихся систем в Windows Server 2019 и (или) Azure.				

Синхронизация файловых серверов в Azure —

централизация общих файловых ресурсов организации в службе Azure Files с такой же гибкостью, производительностью и совместимостью, как у локального файлового сервера.



Системная аналитика — встроенные локальные возможности прогнозной аналитики в Windows Server. Различные функции прогнозирования, подкрепленные моделями машинного обучения, локально анализируют системные данные Windows Server и предоставляют высокоточные прогнозы, которые помогают сократить операционные расходы на реактивное управление экземплярами Windows Server.

Сетевой адаптер Azure — простое подключение к виртуальным сетям Azure. Центр администрирования Windows берет на себя самые сложные этапы настройки VPN-подключения к новому сетевому адаптеру, соединяющему Windows Server 2019 с виртуальной сетью Azure через VPN-подключение типа «точка-сеть».

Улучшенная проверка подлинности в Azure AD — Windows Server 2019 может присоединиться к Azure Active Directory (Azure AD), открывая доступ к новым сценариям, в которых учетная запись компьютера может использоваться для аутентификации в облаке.

Защита ВМ — репликация рабочих нагрузок, выполняющихся в физических и виртуальных машинах (ВМ), с основного объекта в дополнительное расположение.

Инновационная гиперконвергентная инфраструктура

Эволюция инфраструктуры центра обработки данных — путь к повышению эффективности и безопасности.

Гиперконвергентная инфраструктура (HCI) — одна из последних тенденций в серверной индустрии. По данным IDC, в 2016 г. рынок решений для гиперконвергентной инфраструктуры вырос на 64 %, а по прогнозам Gartner, к 2019 г. объем этого рынка достигнет 5 млрд долларов США. В рамках HCI корпорация Майкрософт консолидирует программно-определяемые вычисления, хранилища и сети в единый кластер, предлагающий высокопроизводительную, выгодную и легко масштабируемую виртуализацию. Корпорация Майкрософт объединила усилия с ведущими поставщиками оборудования, чтобы предоставить доступное и в то же время мощное надежно спроектированное решение HCI. В Windows Server 2019 специалисты Майкрософт использовали его как основу и добавили возможности масштабирования, отличную производительность и повышенную надежность наряду со средствами управления развертываниями HCI, чтобы упростить администрирование и повседневные задачи.

Функция и описание	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019
Единое управление — Центр администрирования Windows представляет собой наглядный веб-интерфейс для удаленного управления HCI, включающий средства конфигурирования и мониторинга программно-определяемых сетей.				

Дисковые пространства — обеспечивают защиту данных при выходе носителей из строя и позволяют расширять хранилище по мере добавления носителей в серверы.



Улучшенные локальные дисковые пространства (S2D) — позволяют создавать программно-определяемые хранилища на основе стандартных серверов с локальными дисками, способные масштабироваться до емкости 1 ПБ в одном пуле носителей на Windows Server 2016 и до 4 ПБ в одном пуле носителей и 64 ТБ в одном томе на Windows Server 2019.



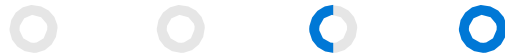
Четность с зеркальным ускорением — позволяет создавать тома с зеркалированием и контролем четности, обеспечивающие вдвое лучшую производительность локальных дисковых пространств. При записи данные сначала помещаются в область с зеркалированием и постепенно переносятся в область с контролем четности.



Вложенная четность с зеркальным ускорением — обеспечивает устойчивость граничных двухузловых кластеров ко множеству одновременных сбоев в работе.



Память класса хранилища — обеспечивает поддержку нового поколения серверного оборудования, включая память класса хранилища, которая значительно повышает производительность серверных приложений.



USB-накопитель (как свидетель кластера) — поддержка использования USB-накопителей в качестве свидетелей кластера позволяет реализовать настоящие двухузловые развертывания HCI без каких-либо дополнительных зависимостей.



Реплика хранилища — обеспечивает синхронную и асинхронную репликацию между серверами на уровне блоков в любых хранилищах в целях аварийного восстановления, а также поддерживает растягивание отказоустойчивого кластера для достижения высокой доступности.



Качество обслуживания хранилища (QoS) — с помощью политик определяет и отслеживает минимальные и максимальные значения ввода-вывода ВМ для их согласованной работы.



Дедупликация данных — экономит до 90 % места на томе благодаря хранению дубликатов файлов в одном экземпляре с использованием логических указателей. В Windows Server 2019 добавлена поддержка дедупликации на томах ReFS.



Дедупликация данных в системе ReFS — теперь дедупликация данных поддерживается на томах ReFS, позволяя оптимизировать на них свободное пространство путем анализа данных на наличие дублирующихся участков.



Отказоустойчивость хранилища виртуальной машины — использует интеллектуальные инструменты для сохранения статуса сеансов ВМ, чтобы уменьшить последствия от небольших перерывов в обслуживании.



Облако-свидетель — позволяет хранилищу больших двоичных объектов Azure выступать свидетелем в кворуме для растянутого кластера. Кроме того, на Windows Server 2019 теперь можно



создавать файловый ресурс-свидетель, который вместо объекта имени кластера (CNO) просто использует локальную учетную запись пользователя на сервере, к которому подключен.

Мониторинг работоспособности хранилища —

обеспечивает непрерывный контроль, составление отчетности и обслуживание локальных дисковых пространств.



Мониторинг всего кластера — отслеживает использование памяти и ЦП, емкость хранилища, показатели IOPS, пропускную способность и задержку в режиме реального времени, предоставляя наглядные уведомления о потенциальных проблемах.



Наборы кластеров — упрощают создание (развертывание и удаление) крупных масштабируемых кластеров без снижения отказоустойчивости.



Последовательное обновление ОС кластера —

дает администраторам возможность постепенно обновлять операционные системы узлов в отказоустойчивом кластере с Windows Server 2012 R2 и Windows Server 2016 до Windows Server 2019.



Работа кластеров в режиме смешанных ОС —

позволяет узлам кластера Windows Server 2012 R2 работать с узлами Windows Server 2016.



Отказоустойчивые кластеры с отслеживанием местонахождения —

позволяют группировать узлы в растянутых кластерах на основе их физического расположения, улучшая основные операции жизненного цикла кластеров, такие как аварийное восстановление, политики размещения, периодические сигналы между узлами и поведение кворума.



Горячая перезагрузка ядра — ускоряет время перезагрузки WSSD-проверенного оборудования, сокращая время простоя приложений.



Постоянная память — поддержка технологии постоянной памяти обеспечивает побайтовый доступ к энергонезависимым носителям, одновременно значительно сокращая задержки при хранении и извлечении данных.



Рабочие нагрузки Linux и FreeBSD — открывают гостевым ОС Linux и FreeBSD на Hyper-V доступ к большинству возможностей Windows Server для программно-определяемого ЦОД, что помогает повысить функциональность, производительность и управляемость систем.



Горячее добавление и удаление виртуальных дисков, памяти и сетевых адаптеров —

позволяет добавлять или удалять сетевой адаптер и регулировать объем назначаемой памяти, не прерывая работу ВМ. Функция регулировки объема памяти работает даже при включенной динамической памяти на хосте Hyper-V.



Сетевой контроллер — предоставляет централизованную программируемую точку автоматизации для управления, настройки, мониторинга и устранения неполадок виртуальной сетевой инфраструктуры в вашем ЦОД.



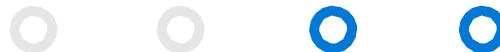
Виртуальная сеть — позволяет создать сетевые наложения на базе общей мультитенантной физической архитектуры.	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Программный балансировщик нагрузки — оптимизированный для облака балансировщик нагрузки 3- и 4-го уровней, обеспечивающий балансировку в направлениях «север-юг» и «восток-запад».	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Прямое соединение виртуальных сетей — поддержка высокоскоростного подключения между двумя виртуальными сетями. Трафик между виртуальными сетями проходит через нижестоящую сетевую структуру, минуя шлюз. Обе виртуальные сети должны относиться к одному ЦОД.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Распределенный брандмауэр и микросегментация — проводят динамическую сегментацию сети с учетом растущих требований к безопасности или к приложениям на основе брандмауэра с отслеживанием состояния и групп безопасности сети.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Гибридные шлюзы SDN — мультитенантные шлюзы высокой доступности, соединяющие клиентские виртуальные сети с Azure, другими облаками на базе Windows Server, высокоскоростными глобальными сетями и локальными неvirtualизированными ресурсами.	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Улучшенный шлюз SDN — практически трехкратное повышение эффективности GRE-туннелей и IPSec VPN типа «сеть-сеть».	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Конвергентный трафик RDMA — сводит трафик хранилища RDMA и тенантный трафик Ethernet на базе единого сетевого адаптера, способствуя значительной экономии без ущерба для пропускной способности и качества обслуживания.	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Протокол точного времени (PTP) — протокол PTP позволяет сетевым устройствам учесть задержку, добавляемую каждым сетевым устройством в измерения времени, обеспечивая намного более точные временные метки, чем протокол сетевого времени (NTP).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Секунда координации — поддержка секунд координации (периодические добавления одной секунды ко времени UTC для компенсации замедления вращения Земли) положительно сказывается на точности, соответствии требованиям и отслеживаемости.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
HTTP/2 — поддержка протокола HTTP/2 (RFC 7540) встроенным HTTP-сервером. Теперь Windows Server 2019 предлагает повышенную производительность и безопасность при развертывании веб-сайтов с применением HTTP/2.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Фоновая передача с оптимизацией задержки (компонент LEDBAT) — в Windows Server 2019 представлен компонент Low Extra Delay Background Transfer (LEDBAT), который регулирует передачу данных по сети с оптимизацией задержки. LEDBAT автоматически выделяет пропускную способность пользователям и приложениям и полностью задействует доступную скорость, когда сеть не используется.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Управление IP-адресами (IPAM) и DNS —

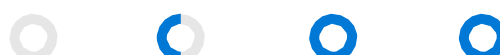
теперь IPAM поддерживает комплексное управление DNS и DHCP с возможностью контроля доступа на основе ролей в различных лесах AD. DNS обеспечивает управление трафиком, балансировку нагрузки и развертывания с разделением, а также предотвращает атаки на DNS типа «усиление».



Роль служб MultiPoint — понижение стоимости рабочего места за счет того, что несколько пользователей могут выполнять собственные сеансы с подключением к одному компьютеру.



Режим высокой доступности посредника подключений RDS — помогает создать отказоустойчивый посредник подключений для сценариев удаленных рабочих столов (RDS).



SDN через IPv4/IPv6 — программно-определяемые сети (SDN) предоставляют способ центрального конфигурирования физических и виртуальных сетевых устройств и управления ими. Кроме того, отныне Windows Server 2019 поддерживает протокол IPv6 и двойную адресацию IPv4/IPv6.



Расширенные возможности защиты

Укрепление защиты центра обработки данных начинается с операционной системы — выведите безопасность своей инфраструктуры на новый уровень.

Безопасность остается одним из главных приоритетов для организаций. Количество инцидентов кибербезопасности продолжает расти, и последствия этих инцидентов становятся все более серьезными. Майкрософт продолжает помогать клиентам укреплять безопасность ИТ-сред. Система безопасности Windows Server основывается на трех столпах — защита, обнаружение и реагирование. Windows Server 2019 предоставляет новые возможности, чтобы предотвратить атаки и обнаружить подозрительную активность, управляя доступом с расширенными правами, защищая виртуальные машины и укрепляя платформу для противодействия возникающим угрозам.

Функция и описание	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019
Улучшенная служба Advanced Threat Protection (ATP) в Защитнике Windows — ATP Exploit Guard в Защитнике Windows представляет собой новый комплекс средств для предотвращения вторжений на хосте, в том числе профилактическую защиту, обнаружение атак и отражение эксплойтов нулевого дня.				
Экранированные виртуальные машины для Windows — возможность шифровать диски и состояние ВМ на основе Windows с помощью BitLocker.				
Экранированные виртуальные машины для Linux — Windows Server 2019 поддерживает экранированные ВМ на основе Linux, обеспечивающие защиту таких ВМ от атак и скомпрометированных администраторов в остальной структуре сети, а также				
Автономный режим HGS для экранированных ВМ — автономный режим позволяет экранированным ВМ включаться при отсутствии связи с сервером HGS, если конфигурация безопасности хоста Hyper-V осталась неизменной.				

VMConnect для экранированных ВМ — возможность безопасного подключения к ВМ на основе Windows и Linux из консоли для более удобного проведения интерактивных сеансов.				
Усиление защиты кластеров — новые кластеры под управлением Windows Server 2019 не нуждаются в NTLM, а значит, не обязательно использовать Active Directory для кластеров Windows Server.				
Зашифрованные подсети SDN — обеспечение шифрования трафика виртуальных сетей при взаимодействии ВМ друг с другом в пределах подсетей.				
Администрирование с минимальными привилегиями — технология, позволяющая ограничить административные привилегии минимальным набором необходимых действий (с пространственным ограничением).				
Администрирование точно в нужный момент — позволяет обеспечить привилегированный доступ через аудируемый и ограниченный по времени рабочий процесс.				
Credential Guard — защита на основе виртуализации, которая обеспечивает безопасность учетных данных в свете сложных продолжительных угроз и исключает их кражу скомпрометированным администратором или вредоносными программами.				
Защита потока управления — передовая защита от классов атак с повреждением памяти.				
Удаленный Credential Guard — работает совместно с Credential Guard для сеансов протокола RDP, обеспечивает единый вход и позволяет обойтись без передачи учетных данных хосту RDP.				
Device Guard (целостность кода) — позволяет запускать на сервере только разрешенные исполняемые файлы.				
Динамический контроль доступа — позволяет администраторам применять разрешения и ограничения управления доступом на основе четко заданных правил.				
AppLocker — обеспечивает управление доступом к приложениям на основе политик.				
BitLocker — обеспечивает шифрование диска (тома данных и системные тома) с помощью аппаратного или виртуального доверенного платформенного модуля (TPM).				

Ускоренная модернизация приложений

Разработчики и ИТ-специалисты смогут создавать собственные облачные приложения и улучшать существующие с помощью контейнеров и микрослужб.

Предприятия осуществляют цифровую трансформацию, чтобы привлечь конечных пользователей, предложить клиентам конкурентоспособные продукты, расширить возможности персонала и повысить эффективность работы. Чтобы стимулировать эту трансформацию, разработчикам нужна современная платформа, которая поможет им предоставлять инновационные решения с учетом меняющихся требований бизнеса. Windows Server 2019 поможет модернизировать приложения и быстрее внедрять инновации. Windows Server 2019 дает

разработчикам и эксплуатационным службам возможность разрабатывать приложения на основе традиционной и контейнерной модели, опираясь на заготовленные решения и доступные артефакты, которые отражают передовой опыт в области разработки и эксплуатации.

Функция и описание	Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019
Контейнеры Linux — облегчают задачу администраторов приложений, позволяя управлять из одной среды приложениями Windows и Linux.				
Контейнеры Windows Server — создают изолированную программную среду, где можно выполнять приложение, не боясь изменений в основной среде из-за приложений или конфигураций.				
Базовый образ контейнера Server Core — уменьшенный базовый образ контейнера Server Core быстрее загружается, а также ускоряет и оптимизирует процесс разработки.				
Базовый образ контейнера Nano Server — уменьшенный базовый образ контейнера Nano Server быстрее загружается, а также ускоряет и оптимизирует процесс разработки. Для Windows Server 2016 оптимизация базового образа контейнера Nano Server предоставляется в рамках обновлений Semi-Annual Channel. Эта возможность доступна для Windows Server 2019 изначально.				
Компоненты Server Core по запросу — установка компонентов по запросу (Features on Demand, FoD) значительно повышает совместимость приложений на Windows Server Core благодаря добавлению набора двоичных файлов и пакетов от Windows Server с возможностями рабочего стола без каких-либо элементов графического интерфейса пользователя Windows Server или Windows 10.				
Поддержка платформы Kubernetes — поддержка кластеров Kubernetes с заметными улучшениями вычислительных ресурсов, хранилища и сетевых компонентов.				
Групповые управляемые учетные записи (gMSA) — единое удостоверение для служб, выполняющихся на ферме серверов или на системах с балансировкой сетевой нагрузки. Благодаря gMSA службам и их администраторам не нужно управлять синхронизацией паролей между экземплярами служб. В Windows Server 2019 технология gMSA улучшает масштабируемость и надежность контейнеров при доступе к сетевым ресурсам.				
Подсистема Windows для Linux (WSL) — дает возможность разработчикам и администраторам приложений пользоваться инструментами в средах Linux наряду с командной строкой и PowerShell.				

<p>Контейнеры Hyper-V — создают среду с высокой степенью изоляции, где другие выполняемые контейнеры никак не влияют на ОС-хост.</p>				
<p>Azure Service Fabric для Windows Server — позволяет создать кластер структуры службы Azure с несколькими компьютерами в вашем собственном ЦОД или в других общедоступных облаках.</p>				
<p>PowerShell 5.1 — предоставляет улучшенные функции сценариев для конфигурации, управления и развертывания компонентов программно-определяемого ЦОД.</p>				
<p>Платформа PowerShell Desired State Configuration (DSC) — предоставляет набор расширений и командлетов языка PowerShell, позволяя декларативно задать конфигурацию программной среды.</p>				
<p>Visual Studio Code — поддерживает операции разработки, такие как отладка, выполнение задач и управление версиями, предоставляя только те средства, которые требуются специалисту (или быстрый цикл создания и отладки кода).</p>				
<p>.NET Core — позволяет создать современные веб-приложения, микрослужбы, библиотеки и консольные приложения, которые выполняются в Windows, Mac и Linux.</p>				

Начните работу

Сделайте следующий шаг. Узнайте больше.

- Постройте свое будущее с Windows Server www.microsoft.com/windowsserver