Начало работы с Windows Server

Статья • 28.01.2023 • Чтение занимает 2 мин

Windows Server является платформой для создания инфраструктуры подключенных приложений, сетей и веб-служб: от рабочей группы до центра обработки данных. Она связывает локальные окружения с Azure, добавляя дополнительные уровни безопасности, а также помогает вам модернизировать приложения и инфраструктуру.

В этой коллекции статей приведены подробные сведения, которые помогут вам разобраться с платформой Windows Server и максимально эффективно ее использовать, а также определить, готовы ли вы перейти к использованию последней версии. Ознакомившись с системными требованиями, параметрами обновления и другими сведениями о Windows Server, вы можете приступить к установке того выпуска и варианта установки, который оптимально соответствует вашим потребностям.

Совет

Чтобы скачать Windows Server, ознакомьтесь со статьей **Ознакомительные версии Windows Server** в Центре оценки.

Примечание

Сведения о более ранних версиях, которые больше не поддерживаются, см. в **документации по предыдущим версиям Windows**.

Поддержка и обратная связь

Последние новости о Windows Server см. в этом блоге. Здесь можно просматривать последние объявления, функции, события и другие сведения от команды инженеров Windows Server. Вы также можете присоединиться к сообществу Windows Server, чтобы поделиться рекомендациями, ознакомиться с последними новостями и перенять опыт экспертов о Windows Server.

Learn

Ознакомьтесь с несколькими схемами обучения по работе с Windows Server, чтобы получить новые навыки и ускорить развертывание с помощью пошагового руководства. Вы можете узнать, как развертывать, настраивать и администрировать Windows Server, а также сетевую инфраструктуру, файловые серверы, службу управления хранилищем, Hyper-V, виртуализацию и многое другое.

Программа предварительной оценки Windows

Программа предварительной оценки Windows для Windows Server предоставляет предварительные сборки Windows Server. Благодаря этим сборкам вы сможете получить ранний доступ к изучению и проверке Windows Server, а также сможете определить будущее развития. Чтобы получить дополнительные сведения, вы можете приступить к работе с Программой предварительной оценки Windows для Windows Server и присоединиться к сообществу участников программы предварительной оценки Windows Server.

Дальнейшие действия

Чтобы приступить к работе, ознакомьтесь со сведениями из этих ресурсов.

- В статье Новые возможности Windows Server 2022 приведены общие сведения о новых функциях Windows Server.
- Узнайте о различных каналах обслуживания, для чего каждый из них используется, а также о том, какое значение они имеют для ваших рабочих нагрузок и поддержки.
- Сравните различия в выпусках Windows Server 2022.
- Выберите правильный вариант установки в зависимости от того, хотите ли вы использовать возможности рабочего стола или минимального базового интерфейса.
- Ознакомьтесь с требованиями к оборудованию для запуска Windows Server.
- Следуйте инструкциям из схемы обучения по развертыванию, настройке и администрированию Windows Server.
- Если вам по-прежнему нужно использовать Windows Server 2008, Windows Server 2008 R2 (а в будущем Windows Server 2012 или Windows Server 2012 R2), воспользуйтесь дополнительными обновлениями для системы безопасности. Они содержат обновления для системы безопасности и бюллетени с оценкой "критические" и "важные".

Новые возможности Windows Server 2022

Статья • 28.01.2023 • Чтение занимает 15 мин

> Область применения: Windows Server 2022

В этой статье описаны некоторые новые функции Windows Server 2022. В основе операционной системы Windows Server 2022 лежит надежная платформа Windows Server 2019. Она предоставляет множество инновационных возможностей для работы с тремя основными областями: безопасность, гибридная интеграция и управление Azure, а также платформа приложений.

Выпуск Azure

Windows Server 2022 Datacenter: Выпуск Azure помогает использовать преимущества облака, чтобы поддерживать виртуальные машины в актуальном состоянии и свести к минимуму время простоя. В этом разделе описываются некоторые новые возможности Windows Server 2022 Datacenter: Выпуск Azure. Дополнительные сведения о том, как автоматическое управление Azure для Windows Server предоставляет эти новые возможности в выпуске Windows Server Azure, см. в статье Автоматическое управление Azure для служб Windows Server .

Windows Server 2022 Datacenter. Выпуск Azure основан на datacenter Edition, чтобы предоставить операционную систему только для виртуальных машин, которая помогает использовать преимущества облака с расширенными функциями, такими как SMB через QUIC, Hotpatch и расширенная сеть Azure. В этом разделе описываются некоторые из этих новых функций.

Сравните различия в выпусках Windows Server 2022. Дополнительные сведения о том, как служба автоматического управления Azure для Windows Server предоставляет эти новые возможности в выпуске Windows Server Azure, см. в статье Автоматическое управление Azure для служб Windows Server .

Сентябрь 2022 г.

В этом разделе перечислены функции и улучшения, которые теперь доступны в Windows Server Datacenter: Выпуск Azure, начиная с накопительного пакета обновления 2022-09 для серверной операционной системы Майкрософт версии

21H2 для 64-разрядных систем (KB5017381). После установки накопительного обновления номер сборки ОС будет 20348.1070 или выше.

Сжатие реплики хранилища для передачи данных

Это обновление включает сжатие реплики хранилища для данных, передаваемых между исходным и целевым серверами. Эта новая функция сжимает данные репликации в исходной системе, отправляемые по сети и распакованные и сохраненные в назначении. Сжатие приводит к меньшему количеству сетевых пакетов для передачи того же объема данных, что обеспечивает большую пропускную способность и меньшее использование сети. Более высокая пропускная способность данных также должна привести к снижению времени синхронизации, когда она вам нужна больше всего, например в сценарии аварийного восстановления.

Новые параметры PowerShell реплики хранилища доступны для существующих команд. Дополнительные сведения см. в справочнике по Windows PowerShell StorageReplica. Дополнительные сведения о реплике хранилища см. в статье Общие сведения о реплике хранилища.

Поддержка Azure Stack HCI

В этом выпуске вы можете запустить Windows Server 2022 Datacenter: Azure Edition в качестве поддерживаемой гостевой виртуальной машины в Azure Stack HCI версии 22H2. В Выпуске Azure, работающем в Azure Stack HCI, вы сможете использовать все существующие функции, включая Hotpatch for Server Core и SMB over QUIC , в центре обработки данных и пограничных расположениях.

Начните развертывание Windows Server 2022 Datacenter: Azure Edition с помощью Azure Marketplace в Azure Stack HCI с поддержкой Arc или iso. Iso-файл можно скачать здесь:

- Windows Server 2022 Datacenter: ISO выпуска Azure (EN-US)
- Windows Server 2022 Datacenter: Azure Edition (ZH-CN) ISO

Подписка Azure позволяет использовать Windows Server Datacenter: Azure Edition на любых экземплярах виртуальных машин, работающих в Azure Stack HCI. Дополнительные сведения см. в разделе Условия продукта .

Дополнительные сведения о последних функциях Azure Stack HCI см. в статье Новые возможности Azure Stack HCI версии 22H2 .

Развертывание из Azure Marketplace в Azure Stack HCI с поддержкой Arc (предварительная версия)

Windows Server 2022 Datacenter: образы выпуска Azure будут доступны в Azure Marketplace для Azure Stack HCI с поддержкой Arc, что упрощает попытку, покупку и развертывание с помощью сертифицированных образов Azure.

Дополнительные сведения об интеграции Azure Marketplace для функций Azure Stack HCI с поддержкой Azure Arc см. в статье Новые возможности Azure Stack HCI версии 22H2.

Выпуск Azure (первоначальный выпуск)

В этом разделе перечислены функции и улучшения, доступные в Windows Server Datacenter: Выпуск Azure с выпуском в сентябре 2021 г.

Автоматическое управление Azure — горячее исправление

Горячее исправление, которое входит в состав службы "Автоматическое управление Azure", — это новый способ установки обновлений на новых виртуальных машинах Windows Server Azure Edition, который не требует перезагрузки после установки. Дополнительные сведения см. в документации по службе автоматического управления.

SMB по QUIC

SMB через QUIC обновляет протокол SMB 3.1.1, чтобы использовать протокол QUIC вместо TCP в Windows Server 2022 Datacenter: Azure Edition, Windows 11 и более поздних версиях, а также сторонние клиенты, если они его поддерживают. Используя протокол SMB по QUIC вместе с TLS 1.3, пользователи и приложения могут безопасно и надежно получать доступ к данным из пограничных файловых серверов, работающих в Azure. Пользователям мобильных устройств и удаленным сотрудникам больше не нужен VPN для доступа к своим файловым серверам по протоколу SMB при использовании Windows. Дополнительные сведения см. в документации по SMB по QUIC и в рекомендациях по управлению SMB через QUIC с помощью автоматического управления компьютерами.

Дополнительные сведения о QUIC см. в статье RFC 9000.

Расширенная сеть для Azure

Расширенная сеть Azure позволяет расширить локальную подсеть в Azure, чтобы локальные виртуальные машины после миграции в Azure сохранили исходные частные IP-адреса из локальной среды. Дополнительные сведения об этом см. в статье Расширенная сеть Azure.

Все выпуски

В этом разделе описываются некоторые новые функции Windows Server 2022 во всех выпусках. Дополнительные сведения о различных выпусках см. в статье Сравнение выпусков Standard, Datacenter и Datacenter: Azure Editions of Windows Server 2022 .

Безопасность

Новые возможности обеспечения безопасности в Windows Server 2022 сочетают в себе другие возможности обеспечения безопасности Windows Server в разных областях. Это обеспечивает надежную защиту от дополнительных угроз. Расширенная многоуровневая защита в Windows Server 2022 предоставляет комплексную защиту, которая в настоящее время необходима серверам.

Сервер с защищенным ядром

Сертифицированное защищенное основное серверное оборудование от oem-партнера обеспечивает дополнительные средства защиты, которые полезны для защиты от сложных атак. Сертифицированное серверное оборудование с защищенными ядрами может обеспечить повышенную уверенность при обработке критически важных данных в некоторых наиболее чувствительных к данным отраслях. Сервер с защищенным ядром использует возможности оборудования, встроенного ПО и драйверов для включения расширенных функций безопасности Windows Server. Многие из этих функций доступны на компьютерах Windows с защищенным ядром, а теперь также доступны при использовании серверного оборудования с защищенным ядром и Windows Server 2022. Дополнительные сведения о сервере с защищенным ядром см. в этой статье.

Корень доверия оборудования

Используемые такими функциями, как шифрование диска BitLocker, защищенные микросхемы криптопроцессоров доверенного платформенного модуля 2.0 (TPM 2.0) обеспечивают безопасное аппаратное хранилище для конфиденциальных криптографических ключей и данных, включая измерения целостности систем. TPM

2.0 может убедиться, что сервер запущен с допустимым кодом и может быть доверенным путем последующего выполнения кода, известного как аппаратный корень доверия.

Защита встроенного ПО

Встроенное ПО работает с высокими привилегиями и часто невидимо для традиционных антивирусных решений, что привело к увеличению количества атак с соответствующим направлением. Серверы с защищенными ядрами измеряют и проверяют процессы загрузки с помощью технологии динамического корня доверия для измерения (DRTM). Серверы с защищенными ядрами также могут изолировать доступ драйверов к памяти с помощью защиты прямого доступа к памяти (DMA).

Безопасная загрузка UEFI

Безопасная загрузка UEFI — это стандарт безопасности, защищающий серверы от вредоносных программ rootkit. Безопасная загрузка гарантирует, что сервер загружает только встроенное ПО и программное обеспечение, доверенное для производителя оборудования. При запуске сервера встроенное ПО проверяет подпись каждого компонента загрузки, включая драйверы встроенного ПО и ОС. Если подписи действительны, сервер загружается, а встроенное ПО предоставляет управление операционной системе.

Безопасность на базе виртуализации (VBS)

Серверы с защищенным ядром поддерживают технологии защиты на основе виртуализации (VBS) и обеспечения целостности кода на основе гипервизора (HVCI). VBS использует функции аппаратной виртуализации для создания и изоляции безопасной области памяти от обычной операционной системы, защищая от целого класса уязвимостей, используемых в атаках майнинга криптовалюты. VBS также позволяет использовать Credential Guard, где учетные данные пользователя и секреты хранятся в виртуальном контейнере, к которому операционная система не может получить прямой доступ.

HVCI использует VBS для значительного усиления политики целостности кода. Целостность режима ядра предотвращает загрузку неподписанных драйверов или системных файлов в системную память.

Защита данных ядра (KDP) обеспечивает защиту памяти ядра только для чтения с неисполняемыми данными, где страницы памяти защищены гипервизором. KDP

защищает ключевые структуры среды выполнения System Guard в Защитнике Windows от несанкционированного изменения.

Безопасное подключение

Транспортировка: протоколы HTTPS и TLS 1.3 по умолчанию включены в Windows Server 2022

Безопасные подключения являются основой современных взаимосвязанных систем. Transport Layer Security (TLS) 1.3 — это последняя версия наиболее распространенного протокола безопасности в Интернете, который шифрует данные для обеспечения безопасного канала связи между двумя конечными точками. Протоколы HTTPS и TLS 1.3 теперь включены по умолчанию в Windows Server 2022. Они защищают данные клиентов, подключающихся к серверу. Это позволяет отказаться от устаревших алгоритмов шифрования и повысить уровень безопасности по сравнению с более старыми версиями. Кроме того, эти протоколы предоставляют возможность шифровать максимально возможное количество подтверждений. Дополнительные сведения о поддерживаемых версиях TLS и наборах шифров.

Хотя TLS 1.3 на уровне протоколов теперь включен по умолчанию, приложения и службы также должны его активно поддерживать. Более подробные сведения можно найти в записи блога Майкрософт по безопасности: Вывод протокола Transport Layer Security (TLS) на новый уровень с версией TLS 1.3.

Безопасный клиент DNS: шифрование запросов разрешения DNS-имени с помощью клиента DNS по протоколу HTTPS

Клиент DNS в Windows Server 2022 теперь поддерживает использование клиента DNS по протоколу HTTPS (DoH), который шифрует запросы DNS по протоколу HTTPS. DoH помогает сохранить трафик как можно более закрытым, предотвращая прослушивание и управление данными DNS. Дополнительные сведения о настройке DNS-клиента для использования DoH.

Протокол SMB: шифрование SMB AES-256 для обеспечения максимальной безопасности

Windows Server теперь поддерживает наборы шифрования AES-256-GCM и AES-256-CCM для шифрования SMB. Windows будет автоматически согласовывать более сложный метод шифра при подключении к другому компьютеру, который также поддерживает его, и он также может быть санкционирован через групповая

политика. Windows Server по-прежнему поддерживает шифрование AES-128 для обеспечения совместимости нижнего уровня. Процесс AES-128-GMAC теперь также повышает производительность подписывания.

Протокол SMB: элементы управления шифрованием SMB в направлении с востока на запад для обмена данными между внутренними кластерами

Отказоустойчивые кластеры Windows Server теперь поддерживают гибкий контроль над шифрованием и подписыванием обмена данными внутри узлов для общих томов кластера (CSV) и уровня шины хранилища (SBL). При использовании Локальные дисковые пространства теперь можно зашифровать или подписать обмен данными между востоком и западом в самом кластере для повышения безопасности.

Шифрование SMB Direct и RDMA

SMB Direct и RDMA предоставляют высокую пропускную способность, сетевую структуру с низкой задержкой для рабочих нагрузок, таких как Локальные дисковые пространства, реплика хранилища, Hyper-V, масштабируемый файловый сервер и SQL Server. Функция SMB Direct в Windows Server 2022 теперь поддерживает шифрование. Раньше при включении шифрования SMB функция прямого размещения данных отключалась. Это было сделано намеренно. Однако это серьезно влияло на производительность. Теперь шифрование данных выполняется до их размещения, благодаря чему происходит относительно небольшое снижение производительности при обеспечении конфиденциальности пакетов, защищаемых с помощью AES-128 и AES-256.

Дополнительные сведения о шифровании SMB, ускорении подписывания, защите RDMA и поддержке кластеров см. в статье Улучшения безопасности SMB.

Гибридные возможности Azure

Вы можете повысить эффективность и гибкость благодаря встроенным гибридным возможностям в Windows Server 2022, которые позволяют расширять центры обработки данных в Azure гораздо удобнее.

Серверы Windows с поддержкой Azure Arc

Серверы с поддержкой Azure Arc с Windows Server 2022 позволяют использовать локальные и многооблачные серверы Windows в Azure с помощью Azure Arc. Этот

интерфейс управления должен соответствовать способу управления собственными виртуальными машинами Azure. Если компьютер с гибридной рабочей ролью, не относящийся к Azure, подключен к Azure, он становится подключенным компьютером и рассматривается как ресурс в Azure. Дополнительные сведения см. в документации по серверам с поддержкой Azure Arc.

Windows Admin Center;

К улучшениям Windows Admin Center для управления Windows Server 2022 относятся возможности составлять отчет о текущем состоянии функций защищенного ядра, упомянутых выше, а также предоставление возможности клиентам включать эти функции. Дополнительные сведения об этих и многих других улучшениях в Windows Admin Center см. в этой документации.

Платформа приложений

Для контейнеров Windows выполнено несколько улучшений платформы. Улучшена совместимость приложений и работа с контейнерами Windows с помощью Kubernetes.

Ниже перечислены некоторые новые функции.

- Уменьшенный размер образа контейнера Windows до 40 %, что на 30 % сокращает время запуска и улучшает производительность.
- Теперь приложения могут использовать Azure Active Directory с групповыми управляемыми учетными записями служб (gMSA) без присоединения домена к узлу контейнера. Контейнеры Windows теперь также поддерживают управление распределенными транзакциями Майкрософт (MSDTC) и очередь сообщений Майкрософт (MSMQ).
- Простые шины теперь можно назначать изолированным от процесса контейнерам Windows Server. Приложения, работающие в контейнерах, которым необходимо взаимодействовать по SPI, I2C, GPIO и UART/COM, теперь могут делать это.
- Мы включили поддержку аппаратного ускорения API DirectX в контейнерах Windows для поддержки таких сценариев, как вывод машинного обучения с использованием оборудования локальной графической обработки (GPU). Дополнительные сведения см. в записи блога Обеспечение ускорения с помощью графического процессора для контейнеров Windows.

- Есть несколько других улучшений, упрощающих работу контейнеров Windows с помощью Kubernetes. Эти улучшения включают поддержку контейнеров хост-процессов для конфигурации узла, IPv6 и постоянную реализацию политики сети с помощью Calico.
- Windows Admin Center обновлена, чтобы упростить контейнеризацию приложений .NET. После того как приложение окажется в контейнере, его можно разместить в Реестре контейнеров Azure, чтобы затем развернуть в других службах Azure, включая службу Azure Kubernetes.
- Благодаря поддержке процессоров Intel Ice Lake Windows Server 2022 поддерживает критически важные для бизнеса и крупномасштабные приложения, которым требуется до 48 ТБ памяти и 2048 логических ядер, работающих в 64 физических сокетах. Конфиденциальные вычисления с помощью технологии Intel Secured Guard Extension (SGX) в Intel Ice Lake повышают безопасность приложений за счет изоляции приложений друг от друга в защищенной области памяти.

Дополнительные сведения о новых функциях см. в статье Новые возможности контейнеров Windows в Windows Server 2022.

Другие ключевые особенности

Планировщик задач и диспетчер Hyper-V для установки основных серверных компонентов

Мы добавили два средства управления в пакет функций совместимости приложений по запросу в этой версии: планировщик задач (taskschd.msc) и диспетчер Hyper-V (virtmgmt.msc). Дополнительные сведения см. в статье Функция обеспечения совместимости приложений основных серверных компонентов по запросу (FOD).

Вложенная виртуализация для процессоров AMD

Вложенная виртуализация — это компонент, который позволяет запускать Hyper-V в виртуальной машине (ВМ) Hyper-V. Windows Server 2022 поддерживает вложенную виртуализацию с помощью процессоров AMD, предоставляя больший выбор оборудования для вашего окружения. Дополнительные сведения см. в документации по вложенной виртуализации.

Браузер Microsoft Edge

Браузер Microsoft Edge включен в состав Windows Server 2022, заменив Internet Explorer. Он основан на Chromium открытый код и поддерживается безопасностью и инновациями Майкрософт. Его можно использовать с вариантами установки основных сервера с возможностями рабочего стола. Дополнительные сведения можно найти в документации по корпоративной версии Microsoft Edge. Microsoft Edge, в отличие от остальной части Windows Server, следует современному жизненному циклу для своего жизненного цикла поддержки. Дополнительные сведения см. в документации по жизненному циклу Microsoft Edge.

Производительность сети

Повышение производительности UDP

UDP становится популярным протоколом с большим объемом сетевого трафика из-за растущей популярности RTP и пользовательских протоколов потоковой передачи и игровых протоколов. Протокол QUIC, созданный на основе протокола UDP, повышает производительность UDP до уровня возможностей TCP. Важно отметить, что Windows Server 2022 реализует разгрузку сегментации UDP (USO). USO переносит большую часть работы, необходимой для отправки пакетов UDP, с ЦП на специализированное оборудование сетевого адаптера. Хваленый метод USO включает функцию объединения на стороне приема UDP (UDP RSC), которая объединяет пакеты и снижает использование ЦП для обработки UDP. Кроме того, мы внесли сотни улучшений в путь передачи данных UDP, как для передачи, так и для приема. Windows Server 2022 и Windows 11 уже включают эту новую возможность.

Повышенная производительность TCP

Windows Server 2022 использует TCP HyStart++ для уменьшения потери пакетов при запуске соединения (особенно в высокоскоростных сетях) и RACK для уменьшения времени ожидания повторной передачи (RTO). Эти функции включены в транспортном стеке по умолчанию и обеспечивают более плавный сетевой поток данных с лучшей производительностью на высоких скоростях. Windows Server 2022 и Windows 11 уже включают эту новую возможность.

Улучшение виртуального коммутатора Hyper-V

Виртуальные коммутаторы в Hyper-V дополнены обновленной функцией объединения полученных сегментов (RSC). RSC позволяет сети низкоуровневой оболочки объединять пакеты и обрабатывать их как один более крупный сегмент.

Это значительно сокращает количество циклов процессора. Сегменты остаются объединенными во всем пути данных до тех пор, пока они не будут обработаны предполагаемым приложением. RSC повышает производительность сетевого трафика от внешнего узла, полученного виртуальным сетевым адаптером, и от виртуального сетевого адаптера к другому виртуальному сетевому адаптеру на том же узле.

Обнаружение аномалий диска с помощью функции системной аналитики

System Insights имеет еще одну возможность с помощью Windows Admin Center обнаружения аномалий диска.

Обнаружение аномалий диска — это новая возможность, которая определяет, когда диски ведут себя *иначе*, чем обычно. Хотя отличия не обязательно указывают на проблемы, просмотр этих аномальных моментов может быть полезен при устранении неполадок в ваших системах. Эта возможность также доступна для серверов под управлением Windows Server 2019.

Улучшения отката обновлений Windows

Серверы теперь могут автоматически восстанавливаться после сбоев при запуске, удаляя обновления, если сбой при запуске возник после установки последних драйверов или исправлений Windows. Если после недавней установки исправлений драйверов устройство не может загрузиться должным образом, Windows автоматически удалит обновления, чтобы устройство снова заработало в нормальном режиме.

Эта функция требует, чтобы сервер использовал вариант установки основных серверных компонентов с разделом среды восстановления Windows.

Служба хранилища

Служба миграции хранилища

Улучшения службы миграции хранилища в Windows Server 2022 упрощают перенос хранилища в Windows Server или в Azure из большего числа расположений источников. Ниже приведены функции, доступные при запуске оркестратора сервера миграции хранилищ в Windows Server 2022.

- Перенос локальных пользователей и групп на новый сервер.

- Перенос хранилища из отказоустойчивых кластеров, перенос в отказоустойчивые кластеры и перенос между автономными серверами и отказоустойчивыми кластерами.
- Перенос хранилища с сервера Linux, использующего Samba.
- Более простая синхронизация перенесенных общих ресурсов в Azure с помощью компонента "Синхронизация файлов Azure".
- Перенос в новые сети, такие как Azure.
- Перенос серверов NetApp CIFS из массивов NetApp на серверы и кластеры Windows.

Регулируемая скорость восстановления хранилища

Настраиваемая пользователем скорость восстановления хранилища — это новая функция в Локальные дисковые пространства, которая обеспечивает больший контроль над процессом повторной синхронизации данных. Регулируемая скорость восстановления хранилища позволяет выделять ресурсы для восстановления копий данных (устойчивость) или для выполнения активных рабочих нагрузок (производительность). Управление скоростью восстановления помогает повысить доступность и позволяет более гибко и эффективно обслуживать кластеры.

Более быстрое восстановление и повторная синхронизация

Восстановление хранилища и повторная синхронизация после таких событий, как перезагрузка узла и сбой диска, стали в два раза быстрее. Для восстановления обеспечивается меньшее отклонение по времени, поэтому вы будете знать более точную длительность операций исправления, что достигается за счет увеличения детализации при отслеживании данных. Восстановление теперь перемещает только те данные, которые необходимо переместить, сокращая используемые системные ресурсы и время.

Кэш шины хранилища с использованием дисковых пространств на отдельных серверах

Кэш шины хранилища теперь доступен для отдельных серверов. Это может значительно повысить производительность чтения и записи, сохраняя эффективность хранения и обеспечивая низкие эксплуатационные затраты. Как и в случае с реализацией Локальных дисковых пространств, эта функция связывает быстрый носитель (например, NVMe или SSD) с более медленным (например, HDD) для создания уровней. Часть более быстрого уровня носителя резервируется для

кэша. Дополнительные сведения см. в статье Включение кэша шины хранилища с использованием дисковых пространств на отдельных серверах.

Моментальные снимки на уровне файлов ReFS

Система Resilient File System (ReFS) корпорации Майкрософт теперь поддерживает возможность создания моментальных снимков файлов с использованием быстрой операции с метаданными. Моментальные снимки отличаются от клонирования блоков ReFS в том, что клоны доступны для записи, а моментальные снимки доступны только для чтения. Эта функция особенно полезна в сценариях резервного копирования виртуальных машин с VHD/VHDX-файлами. Моментальные снимки ReFS уникальны в том смысле, что они занимают константное время независимо от размера файла. Поддержка моментальных снимков доступна в ReFSUtil или в виде API.

Сжатие SMB

Усовершенствование протокола SMB в Windows Server 2022 и Windows 11 позволяет пользователю или приложению сжимать файлы по мере их передачи по сети. Пользователям больше не нужно вручную сжимать ZIP-файлы для ускорения их передачи в медленных или более перегруженных сетях. Дополнительные сведения см. в документации по сжатию SMB.

Новые возможности Windows Server 2019

Статья • 28.01.2023 • Чтение занимает 11 мин

В этой статье описаны некоторые новые функции Windows Server 2019. В основе операционной системы Windows Server 2019 лежит надежная платформа Windows Server 2016. Она предоставляет множество инновационных возможностей для работы с четырьмя основными областями: гибридное облако, безопасность, платформа приложений и гиперконвергентная инфраструктура (HCI).

Общие

Windows Admin Center

Windows Admin Center представляет собой локально развертываемое браузерное приложение для управления серверами, кластерами, гиперконвергентной инфраструктурой и ПК под управлением Windows 10. Он не требует дополнительных затрат, помимо Windows, и готов к использованию в рабочей среде.

Вы можете установить Windows Admin Center в Windows Server 2019 и Windows 10 и более ранних версиях Windows и Windows Server, а также использовать его для управления серверами и кластерами под управлением Windows Server 2008 R2 и более поздних версий.

Подробные сведения см. в статье Hello, Windows Admin Center! (Привет, Windows Admin Center!).

Возможности рабочего стола

Поскольку Windows Server 2019 — это выпуск Long-Term Servicing Channel (LTSC), он включает **возможности рабочего стола**. (Выпуски Semi-Annual Channel (SAC) не включают в себя возможности рабочего стола по умолчанию; это только выпуски образов контейнеров Server Core и Nano Server.) Как и в случае с Windows Server 2016, во время настройки операционной системы вы можете выбрать установку основных серверных компонентов или установку сервера с возможностями рабочего стола.

Системная аналитика

Системная аналитика — это новая функция, доступная в Windows Server 2019, за счет которой в Windows Server реализуется встроенная поддержка локальных возможностей прогнозной аналитики. Эти возможности прогнозирования, каждая из которых поддерживается моделью машинного обучения, локально анализирует системные данные Windows Server, такие как счетчики производительности и события. System Insights позволяет понять, как работают серверы, и помогает сократить эксплуатационные расходы, связанные с реактивным управлением проблемами в развертываниях Windows Server.

Гибридное облако

Функция совместимости приложений основных серверных компонентов по требованию

Компонент совместимости основных серверных приложений по запросу (FOD) значительно повышает совместимость приложений, включив подмножество двоичных файлов и компонентов из Windows Server с возможностями рабочего стола. Основные серверные компоненты поддерживаются как можно более экономичными, не добавляя графическую среду Windows Server Desktop Experience, что повышает функциональность и совместимость.

Эта дополнительная функция по требованию доступна в отдельном ISO-файле, и ее можно добавлять только в образы и установки основных серверных компонентов Windows с помощью DISM.

Роль транспортного сервера служб развертывания Windows (WDS), добавленная в server Core

Транспортный сервер содержит только основные сетевые компоненты службы развертывания Windows. Теперь вы можете использовать основные серверные компоненты с ролью транспортного сервера для создания многоадресных пространств имен, которые передают данные (включая образы операционной системы) с изолированного сервера. Вы также можете использовать его, если требуется предоставить PXE-сервер, который позволяет клиентам выполнять PXE-загрузку и скачивать собственное приложение для установки.

Интеграция служб удаленных рабочих столов с Azure AD

Благодаря интеграции Azure AD можно использовать политики условного доступа, многофакторную проверку подлинности, встроенную проверку подлинности с другими приложениями SaaS с помощью Azure AD и многое другое. Дополнительные сведения см. в разделе Интеграция доменных служб Azure AD со средой RDS.

Сеть

Мы внесли несколько улучшений в основной сетевой стек, такие как быстрое открытие TCP (TFO), автонастройка окна получения, IPv6 и многое другое. Дополнительные сведения см. в записи об улучшении функций стека core Network Stack .

Безопасность

Advanced Threat Protection в Защитнике Windows (ATP)

Датчики глубокого анализа и ответные действия платформы ATP выявляют атаки на уровне памяти и ядра и реагируют на них путем подавления вредоносных файлов и завершения вредоносных процессов.

- Подробные сведения об ATP в Защитнике Windows см. в статье Overview of Microsoft Defender ATP capabilities (Обзор возможностей ATP в Защитнике Windows).
- Подробные сведения о подключении серверов см. в статье Onboard servers to the Microsoft Defender ATP service (Подключение серверов к службе ATP в Защитнике Windows).

Защитник Windows ATP Exploit Guard — это новый набор возможностей предотвращения вторжений в узел, позволяющий сбалансировать риски безопасности и требования к производительности. Защитник Windows Exploit Guard предназначен для блокировки устройства от широкого спектра векторов атак и блокировки поведения, обычно используемого в атаках с вредоносными программами. Ниже перечислены компоненты.

- Сокращение направлений атак (ASR) ASR — это набор элементов управления, которые предприятия могут включить, чтобы предотвратить попадание

вредоносных программ на компьютер, блокируя подозрительные вредоносные файлы. Например, файлы Office, скрипты, боковое смещение, поведение программ-шантажистов и угрозы на основе электронной почты.

- Функция Защита сети защищает конечные точки от веб-угроз, блокируя любые процессы на устройстве, идущие к недоверенным узлам и IP-адресам, с помощью фильтра SmartScreen Защитника Windows.

- Функция Контролируемый доступ к файлам защищает конфиденциальные данные от программ-шантажистов, блокируя доступ недоверенных процессов к защищенным папкам.

- Защита от эксплойтов — это набор мер защиты от уязвимостей (замена EMET), которые можно легко настроить для обеспечения безопасности системы и приложений.

- Функция Управление приложениями в Защитнике Windows (также известна как политика целостности кода (CI) была представлена в Windows Server 2016. Мы упростили развертывание, включив политики CI по умолчанию. Политика по умолчанию разрешает все встроенные файлы Windows и приложения Майкрософт, такие как SQL Server, и блокирует известные исполняемые файлы, которые могут обходить CI.

Безопасность программно-конфигурируемых сетей (SDN)

Функция Безопасность для SDN предоставляет множество возможностей для безопасного выполнения рабочих нагрузок клиентами как в локальной среде, так и в качестве поставщика услуг в облаке.

Эти усовершенствования безопасности интегрированы в многофункциональную платформу SDN, появившуюся в Windows Server 2016.

Полный список новых возможностей SDN доступен в статье Что нового в программно-конфигурируемой сети (SDN) для Windows Server 2019?

Улучшения экранированных виртуальных машин

- **Улучшения для филиалов**

  Теперь экранированные виртуальные машины можно запускать на компьютерах с периодическими разрывами подключения к службе защиты узла, используя новый резервный сервер HGS и автономный режим.

Резервный сервер HGS позволяет настроить второй набор URL-адресов для Hyper-V, который будет использоваться в случае невозможности установить подключение к основному серверу HGS.

Даже если не удается получить доступ к HGS, автономный режим позволит вам продолжать запускать экранированные виртуальные машины. Автономный режим позволяет запускать виртуальные машины, если виртуальная машина успешно запущена один раз, а конфигурация безопасности узла не изменилась.

- **Дополнительные возможности устранения неполадок**

  Мы также упростили процесс устранения неполадок в работе экранированных виртуальных машин за счет добавления поддержки режима расширенного сеанса VMConnect и PowerShell Direct. Эти средства полезны, если вы потеряли сетевое подключение к виртуальной машине и вам нужно обновить ее конфигурацию для восстановления доступа.

  Эти функции не нужно настраивать, и они становятся доступными автоматически при размещении экранированных виртуальных машин на узле Hyper-V под управлением Windows Server 1803 или более поздней версии.

- **Поддержка Linux**

  Теперь Windows Server 2019 поддерживает выполнение систем Ubuntu, Red Hat Enterprise Linux и SUSE Linux Enterprise Server внутри экранированных виртуальных машина при работе в средах со смешанными ОС.

HTTP/2 для более быстрого и безопасного просмотра веб-страниц

- Улучшенное объединение подключений исключает сбои при работе в Интернете, а также обеспечивает правильное шифрование веб-сеансов.
- Обновленный процесс согласования наборов шифров на стороне сервера в HTTP/2 обеспечивает автоматическое устранение сбоев подключений и удобство развертывания.
- Мы сделали CUBIC поставщиком контроля перегрузки протокола TCP по умолчанию, чтобы еще больше повысить пропускную способность!

Хранение

Вот некоторые изменения, которые мы внесли в хранилище в Windows Server 2019. Подробные сведения см. в статье What's new in Storage in Windows Server (Новые возможности хранилища в Windows Server).

дедупликация данных;

- **Дедупликация данных теперь поддерживает ReFS** Теперь вы можете включить дедупликацию данных везде, где можно включить ReFS, что повышает эффективность хранилища до 95 % с помощью ReFS.
- **API DataPort для оптимизированного входящего и исходящего трафика в дедуплицированные тома** Теперь разработчики могут воспользоваться знаниями дедупликации данных о том, как эффективно хранить данные для эффективного перемещения данных между томами, серверами и кластерами.

File Server Resource Manager

Теперь можно запретить службе файлового сервера Resource Manager создавать журнал изменений (также известный как журнал USN) на всех томах при запуске службы. Предотвращение создания пути изменения может сэкономить место на каждом томе, но приведет к отключению классификации файлов в режиме реального времени. Подробные сведения см. в статье File Server Resource Manager (FSRM) overview (Обзор диспетчера ресурсов файлового сервера (FSRM)).

SMB

- **Удаление SMB1 и гостевой проверки подлинности** Windows Server больше не устанавливает клиент и сервер SMB1 по умолчанию. Кроме того, возможность проверки подлинности гостя в SMB2 и более поздних версиях отключена по умолчанию. Дополнительные сведения см. в статье SmBv1 не устанавливается по умолчанию в Windows 10 версии 1709 и Windows Server версии 1709 .
- **Безопасность и совместимость SMB2/SMB3** Теперь у вас есть возможность отключить блокировки операций в SMB2+ для устаревших приложений и требовать подписывания или шифрования для каждого подключения от клиента. Дополнительные сведения см. в справке по модулю SMBShare PowerShell.

Служба миграции хранилища

Служба миграции хранилища — это новая технология, которая упрощает перенос серверов в более новую версию Windows Server. Мы предоставили графическое средство, которое выполняет инвентаризацию данных на серверах, а затем передает данные и конфигурацию на более новые серверы. Служба миграции хранилища также при необходимости переместит удостоверения старых серверов на новые, чтобы приложениям и пользователям не нужно было ничего изменять. Подробные сведения см. в разделе Storage Migration Service overview (Обзор службы миграции хранилища).

Дисковые пространства прямого подключения

Ниже приведен список новых возможностей в Локальных дисковых пространствах. Подробные сведения см. в разделе Storage Spaces Direct (Windows Server 2019 only) (Локальные дисковые пространства (только для Windows Server 2019). Информацию о приобретении проверенных систем с Локальными дисковыми пространствами см. в статье Общие сведения об Azure Stack HCI.

- Дедупликация и сжатие томов ReFS
- Встроенная поддержка энергонезависимой памяти
- Программно вложенная устойчивость гиперконвергентной инфраструктуры с двумя узлами на границе
- Кластеры из двух серверов, использующие USB-устройство флэш-памяти в качестве свидетеля
- Поддержка Windows Admin Center
- Журнал производительности
- Масштабирование до 4 ПБ на кластер
- Контроль четности с зеркальным ускорением вдвое быстрее
- Обнаружение выброса задержки диска
- Ручное разграничение выделения томов для повышения отказоустойчивости

Реплика хранилища

Новые возможности в реплике хранилища. Подробные сведения см. в разделе Storage Replica (Реплика хранилища).

- Реплика хранилища теперь доступна в Windows Server 2019 Standard Edition.
- Тестовая отработка отказа — это новая функция, которая позволяет подключать целевое хранилище для проверки репликации или резервного копирования данных. Подробные сведения см. в статье с часто задаваемыми вопросами о реплике хранилища.
- Улучшения производительности журнала реплики хранилища

- Поддержка Windows Admin Center

Отказоустойчивая кластеризация

Ниже приведен список новых возможностей отказоустойчивой кластеризации. Подробные сведения см. в статье What's new in Failover Clustering (Новые возможности отказоустойчивой кластеризации).

- Наборы кластеров
- Кластеры с поддержкой Azure
- Миграция кластеров между доменами
- Свидетель USB
- Улучшения инфраструктуры кластера
- Кластерное обновление поддерживает локальные дисковые пространства
- Улучшения файлового ресурса-свидетеля
- Усиление защиты кластера
- Отказоустойчивый кластер больше не использует аутентификацию NTLM

Платформы приложений

Контейнеры Linux в Windows

Теперь можно запускать контейнеры Windows и Linux на одном узле контейнеров с помощью одной и той же управляющей программы Docker. Теперь у вас есть разнородная среда узла контейнера, обеспечивающая гибкость для разработчиков приложений.

Встроенная поддержка Kubernetes

В Windows Server 2019 улучшены функции вычислений, сети и хранилища выпусков Semi-Annual Channel, необходимых для реализации поддержки платформы Kubernetes в Windows. Дополнительная информация будет доступна в следующих выпусках Kubernetes.

- Сеть контейнеров в Windows Server 2019 значительно повышает удобство использования Kubernetes в Windows. Мы улучшили устойчивость платформы к сети и поддержку подключаемых модулей сети контейнеров.

- Развернутые в Kubernetes рабочие нагрузки могут использовать средства сетевой безопасности для защиты служб Linux и Windows с помощью

встроенных механизмов безопасности.

Улучшения контейнеров

- **Улучшенные интегрированные удостоверения**

  Мы упростили процесс встроенной проверки подлинности Windows в контейнерах и повысили ее надежность, устранив некоторые ограничения предыдущих выпусков Windows Server.

- **Улучшенная совместимость приложений**

  Упрощено создание контейнеров приложений Windows: улучшена совместимость приложений для имеющегося образа **windowsservercore**. Для приложений с большими зависимостями API теперь существует третий базовый образ: **windows**.

- **Уменьшение размера и повышение производительности**

  Размеры загрузки базового образа контейнера, размер на диске и время запуска были улучшены для ускорения рабочих процессов контейнеров.

- **Интерфейс администрирования в Windows Admin Center (предварительная версия)**

  Мы значительно упростили мониторинг контейнеров, запущенных на вашем компьютере, а также управление отдельными контейнерами с помощью нового расширения для Windows Admin Center. Найдите расширение "Контейнеры" в общедоступном веб-канале Windows Admin Center.

Улучшения вычислений

- **Упорядочение на виртуальной машине** Порядок запуска виртуальной машины также улучшен благодаря повышению осведомленности об ОС и приложениях, в результате чего добавлены улучшенные триггеры, когда виртуальная машина считается запущенной перед запуском следующей.

- **Поддержка памяти класса хранилища для виртуальных машин** позволяет создавать тома с прямым доступом и форматированием с файловой системой NTFS на энергонезависимых модулях DIMM и предоставлять их виртуальным машинам Hyper-V. Виртуальные машины Hyper-V теперь могут использовать преимущества производительности с низкой задержкой, предоставляемые устройствами памяти класса хранения.

- **Поддержка постоянной памяти для виртуальных машин Hyper-V** Чтобы использовать высокую пропускную способность и низкую задержку постоянной памяти (также известной как память класса хранения) на виртуальных машинах, теперь ее можно проецировать непосредственно на виртуальные машины. Постоянная память может помочь значительно сократить задержку транзакций базы данных или сократить время восстановления для баз данных с низкой задержкой в памяти при сбое.

- **Хранилище контейнеров — постоянные тома данных** Контейнеры приложений теперь имеют постоянный доступ к томам. Дополнительные сведения см. в разделе поддержка контейнера хранилища с общими томами кластера (CSV), локальными дисковыми пространствами (S2D) и глобальным сопоставлением SMB.

- **Формат файла конфигурации виртуальной машины (обновлен)** Файл гостевого состояния виртуальной машины (`.vmgs`) добавлен для виртуальных машин с конфигурацией версии 8.2 и выше. Файл гостевого состояния виртуальной машины содержит сведения о состоянии устройства, которые ранее были частью файла состояния среды выполнения виртуальной машины.

Зашифрованные сети

Зашифрованные сети — функция шифрования виртуальных сетей, позволяющая шифровать трафик виртуальной сети между виртуальными машинами, которые обмениваются данными между собой в подсетях с пометкой **Включено шифрование**. Для шифрования пакетов с помощью этой возможности также используется протокол DTLS в виртуальной подсети. Протокол DTLS обеспечивает защиту от перехвата, несанкционированных изменений и подделки со стороны любых лиц, имеющих доступ к физической сети.

Повышение производительности сети для виртуальных рабочих нагрузок

Повышение производительности сети для виртуальных рабочих нагрузок обеспечивает максимальную пропускную способность сети для виртуальных машин без необходимости постоянной настройки или избыточного предоставления ресурсов узла. Повышение производительности снижает затраты на операции и обслуживание, одновременно увеличивая плотность доступных узлов. Новые функции:

- динамическое управление несколькими очередями виртуальных машин (d.VMMQ).
- объединение полученных сегментов в виртуальном коммутаторе;

Передача данных с помощью алгоритма Low Extra Delay Background Transport

Фоновый транспорт с низкой дополнительной задержкой (LEDBAT) — это оптимизированный для задержки поставщик управления перегрузкой сети, предназначенный для автоматического обеспечения пропускной способности для пользователей и приложений. LEDBAT потребляет доступную пропускную способность, пока сеть не используется. Эта технология предназначена для использования при развертывании крупных критически важных обновлений в ИТ-среде без влияния на службы, связанные с клиентами, и связанную с ними пропускную способность.

служба времени Windows

В службе времени Windows реализована полноценная поддержка UTC-совместимой корректировочной секунды, новый протокол времени под названием "Протокол точного времени" (Precision Time Protocol), а также трассировка в сквозном режиме.

Высокопроизводительные шлюзы SDN

Высокопроизводительные шлюзы SDN в Windows Server 2019 значительно повышают производительность подключений IPsec и GRE, обеспечивая сверхвысокую пропускную способность при гораздо меньшей нагрузке на ЦП.

Новый пользовательский интерфейс развертывания и расширение Windows Admin Center для SDN

Теперь в Windows Server 2019 можно легко выполнять развертывание и управление с помощью нового пользовательского интерфейса для развертывания, а также расширения Windows Admin Center, которое предоставляет возможности SDN всем пользователям.

Подсистема Windows для Linux (WSL)

WSL позволяет администраторам сервера использовать имеющиеся средства и сценарии с Linux в Windows Server. Множество усовершенствований, о которых рассказывалось в блоге command line, теперь входят в состав Windows Server, включая фоновые задачи, DriveFS, WSLPath и многое другое.

Новые возможности Windows Server 2016

Статья • 28.01.2023 • Чтение занимает 10 мин

В этой статье описаны некоторые новые функции Windows Server 2016, которые, скорее всего, окажут наибольшее влияние во время работы с этим выпуском.

Вычисления

Область виртуализации охватывает продукты для виртуализации и средства разработки, развертывания и поддержки Windows Server для ИТ-специалистов.

Общие

Преимущества для физических и виртуальных машин — повышена точность времени благодаря усовершенствованию служб синхронизации Win32 Time и Hyper-V Time. В Windows Server теперь можно разместить службы, которые будут соответствовать растущим стандартам точности времени (1 мс относительно времени UTC).

Hyper-V

- Новые возможности Hyper-V в Windows Server 2016. В этом разделе рассматриваются новые и измененные функции роли Hyper-V в Windows Server 2016, клиента Hyper-V в Windows 10 и Microsoft Hyper-V Server 2016.
- Контейнеры Windows: поддержка контейнеров в Windows Server 2016 обеспечивает повышение производительности, упрощенное управления сетями и использование контейнеров Windows в Windows 10. Дополнительные сведения о контейнерах см. в записи блога Containers: Docker, Windows and Trends (Контейнеры: Docker, Windows и тенденции).

Сервер Nano Server

Новые возможности сервера Nano Server. В Nano Server обновлен модуль для создания образов Nano Server. Это обновление включает дополнительное разграничение функций физического узла и гостевой виртуальной машины, а также поддержку разных выпусков Windows Server.

Кроме того, усовершенствован агент восстановления: разграничены правила брандмауэра для входящего и исходящего трафика, а также добавлена возможность восстановить настройки службы WinRM.

Экранированные виртуальные машины

Windows Server 2016 предоставляет новые экранированные виртуальные машины на основе Hyper-V для защиты любой виртуальной машины поколения 2 от скомпрометированной структуры. В число функций, реализованных в Windows Server 2016, входят следующие:

- Новый режим **Поддержка шифрования** обеспечивает более надежную защиту, чем для обычной виртуальной машины, но менее надежную, чем режим **Экранирование**. При этом он поддерживает vTPM, шифрование дисков, шифрование трафика динамической миграции и другие компоненты, в том числе такие преимущества непосредственного администрирования структуры, как подключение консоли виртуальной машины и Powershell Direct.

- Полная поддержка для преобразования существующих неэкранированных виртуальных машин второго поколения в экранированные виртуальные машины, в том числе автоматическое шифрование дисков.

- Диспетчер виртуальных машин Hyper-V теперь отображает структуры, в которых авторизованы для выполнения экранированные виртуальные машины. Это позволяет администратору структуры открыть предохранитель ключа (KP) экранированной виртуальной машины и просмотреть структуры, в которых ей разрешено выполнение.

- Вы можете переключать режимы аттестации на выполняющиеся службы защиты узла. Теперь вы можете немедленно переключаться между менее безопасной, но более простой аттестацией для Active Directory и аттестацией для доверенного платформенного модуля.

- Комплексные средства диагностики на основе Windows PowerShell, которые позволяют обнаружить неверные настройки или ошибки в защищенных узлах Hyper-V и службе защиты узла.

- Среда восстановления, которая обеспечивает средства безопасного устранения неполадок и восстановления экранированных виртуальных машин в обычной структуре их выполнения. Она предоставляет тот же уровень защиты, что и собственно экранированная виртуальная машина.

- Поддержка службы защиты узла для существующего безопасного Active Directory — вы можете указать службе защиты узла использовать существующий лес Active Directory вместо создания собственного экземпляра Active Directory.

Дополнительные сведения и инструкции по работе с экранированными виртуальными машинами см. в статье Защищенная структура и экранированные виртуальные машины.

Удостоверение и доступ

Новые компоненты удостоверения повышают уровень защиты окружений Active Directory для организаций, а также помогают перейти к развертываниям только для облачной среды и гибридным развертываниям, в которых некоторые приложения и службы размещены в облаке, а другие — на локальном компьютере.

Службы сертификатов Active Directory

Для служб сертификатов Active Directory (AD CS) в Windows Server 2016 увеличена поддержка аттестации ключей доверенного платформенного модуля. Теперь можно использовать KSP смарт-карты для аттестации ключей. Для устройств, не присоединенных к домену, теперь можно использовать регистрацию NDES, чтобы получить сертификат, который можно аттестовать для ключей в доверенном платформенном модуле.

Доменные службы Active Directory

Доменные службы Active Directory содержат усовершенствования, которые помогут организациям обеспечить безопасность сред Active Directory и повысить эффективность выполнения задач по управлению удостоверениями для корпоративных и персональных устройств. Дополнительные сведения см. в статье Новые возможности доменных служб Active Directory (AD DS) в Windows Server 2016.

Службы федерации Active Directory (AD FS)

Новые возможности служб федерации Active Directory. В состав служб федерации Active Directory (AD FS) в Windows Server 2016 включены новые возможности, которые позволяют настраивать AD FS для проверки подлинности пользователей,

хранящихся в каталогах LDAP. Дополнительные сведения см. в статье Новые возможности служб федерации Active Directory.

Прокси-сервер веб-приложения

Последняя версия прокси-службы веб-приложения обеспечивает новые возможности для публикации и предварительной проверки подлинности дополнительных приложений, а также удобство работы пользователей. Ознакомьтесь с полным списком новых возможностей, включающих предварительную проверку подлинности многофункциональных клиентских приложений, таких как Exchange ActiveSync, и домены с подстановочными знаками для упрощения публикации приложений SharePoint. Дополнительные сведения см. в статье Прокси-служба веб-приложения в Windows Server 2016.

Администрирование

Область управления и автоматизации содержит средства и справочную информацию, которые необходимы ИТ-специалистам для запуска выпуска Windows Server 2016 и управления им, в том числе Windows PowerShell.

Windows PowerShell 5.1 содержит важные новые компоненты, в том числе поддержку разработки с использованием классов и новые средства безопасности, которые расширяют возможности использования, повышают удобство использования и упрощают комплексное управление средами для Windows. Подробные сведения см. в статье Заметки о выпуске Windows Management Framework (WMF) 5.x.

Новые функции в Windows Server 2016: возможность запускать PowerShell.exe локально на сервере Nano Server (теперь доступ не только удаленный), новые командлеты для локальных пользователей и групп для замены графического интерфейса пользователя, реализована поддержка отладки PowerShell, а также поддержка ведения и расшифровки журнала безопасности и JEA в Nano Server.

Ниже приведены некоторые другие новые функции администрирования.

Настройка требуемого состояния (DSC) PowerShell в Windows Management Framework (WMF) 5

Windows Management Framework 5 включает в себя обновления для настройки требуемого состояния (DSC) Windows PowerShell, службы удаленного управления Windows (WinRM) и инструментария управления Windows (WMI).

Дополнительные сведения о тестировании возможностей DSC в Windows Management Framework 5 см. в серии записей блога Validate features of PowerShell DSC (Проверка компонентов PowerShell DSC). Чтобы скачать Windows Management Framework 5.1, перейдите в этот раздел.

Унифицированное управление пакетами PackageManagement для обнаружения программного обеспечения, установки и инвентаризации

Windows Server 2016 и Windows 10 включает новую функцию PackageManagement (раньше она называлась OneGet). С ее помощью ИТ-специалисты и разработчики могут автоматизировать удаленные или локальные операции обнаружения, установки и инвентаризации ПО. При этом не важно, какая технология установщика используется и где это ПО расположено.

Подробнее см. по адресу https://github.com/OneGet/oneget/wiki.

Усовершенствования PowerShell для облегчения цифровых расследований и снижения угроз безопасности

Чтобы помочь группе, расследующей нарушения безопасности (ее иногда называют "blue team"), мы добавили функции ведения журналов PowerShell и другие функциональные возможности цифровых расследований, а также возможности для сокращения числа уязвимостей в скриптах, например ограниченный режим в PowerShell и безопасные API CodeGeneration.

Дополнительные сведения см. в статье, посвященной PowerShell на стороне синих.

Сеть

Эта область сети охватывает сетевые продукты и компоненты, позволяющие ИТ-специалистам проектировать, развертывать и обслуживать Windows Server 2016.

Программно-определяемая сеть

Теперь доступны зеркалирование и маршрутизация трафика для новых или существующих виртуальных модулей. Вместе с распределением брандмауэра и групп безопасности сети вы получаете возможность динамически сегментировать

и защищать рабочие нагрузки так же, как в Azure. Кроме того, вы можете развертывать целый стек программно конфигурируемой сети (SDN) и управлять ими с помощью System Center Virtual Machine Manager. И, наконец, с помощью Docker вы можете управлять сетью контейнеров Windows Server и связывать политики SDN не только с виртуальными машинами, но и с контейнерами. Дополнительные сведения см. в статье, посвященной планированию инфраструктуры программно-конфигурируемой сети.

Повышенная производительность TCP

Начальный период перегрузки (ICW) по умолчанию был увеличен с 4 до 10, а также была реализована функция TCP Fast Open (TFO). TFO сокращает время, необходимое для установки TCP-соединения, а увеличенный период ICW позволяет передавать более крупные объекты в рамках начальной отправки. Такое сочетание может значительно снизить время, необходимое для передачи интернет-объекта между клиентом и облаком.

Чтобы улучшить поведение TCP при восстановлении после потери пакетов, мы реализовали функции Tail Loss Probe (TLP) и Recent Acknowledgement (RACK). TLP позволяет преобразовать время ожидания повторной передачи в быстрое восстановление, а RACK сокращает время, необходимое быстрому восстановлению для повторной передачи потерянного пакета.

Безопасность и контроль

Область безопасности и контроля включает решения и компоненты в области безопасности, которые ИТ-специалисты могут развертывать в центре обработки данных и облачном окружении. Общие сведения о безопасности в Windows Server 2016 см. в статье Безопасность и контроль.

Just Enough Administration

Just Enough Administration в Windows Server 2016 — это технология безопасности, позволяющая делегировать администрирование всех компонентов, которыми можно управлять через Windows PowerShell. Возможности включают в себя поддержку выполнения с сетевым удостоверением, подключения через PowerShell Direct, безопасное копирование файлов из конечных точек JEA или в них, а также настройку консоли PowerShell для запуска в контексте JEA по умолчанию. Дополнительные сведения см. в статье о JEA на GitHub.

Credential Guard

Для защиты секретов Credential Guard использует безопасность на основе виртуализации, чтобы только привилегированное системное ПО могло получать доступ к этим данным. См. статью Защита извлеченных учетных данных домена с помощью Credential Guard.

Удаленный Credential Guard

Credential Guard поддерживает сеансы RDP, чтобы учетные данные пользователя оставались на стороне клиента и не предоставлялись на стороне сервера. Это также обеспечивает единый вход для удаленного рабочего стола. См. сведения в статье Защита извлеченных учетных данных домена с помощью Credential Guard.

Device Guard (целостность кода)

Device Guard обеспечивает целостность кода режима ядра (KMCI) и целостность кода пользовательского режима (UMCI) путем создания политик, которые указывают, какой код может выполняться на сервере. См. сведения в статье Windows Defender Application Control and virtualization-based protection of code integrity (Управление приложениями в Защитнике Windows и безопасность целостности кода на основе виртуализации).

Защитник Windows

Обзор Защитника Windows для Windows Server 2016. В Windows Server 2016 установлено и включено по умолчанию ПО защиты от вредоносных программ Windows Server Antimalware, однако пользовательский интерфейс для этого ПО не установлен. Тем не менее, Windows Server Antimalware будет обновлять определения для антивредоносного ПО и защищать компьютер без пользовательского интерфейса. Если вам требуется пользовательский интерфейс для Windows Server Antimalware, его можно установить после установки операционной системы, воспользовавшись мастером добавления ролей и компонентов.

Защита потока управления

Защита потока управления (CFG) — это компонент безопасности платформы, предназначенный для борьбы с уязвимостями на базе повреждения памяти. Дополнительные сведения см. в статье Защита потока управления.

Служба хранилища

Хранилище в Windows Server 2016 включает новые возможности и усовершенствования для программно-определяемого хранилища, а также для традиционных файловых серверов. Ниже представлено лишь несколько новых функций, дополнительные сведения см. в статье Новые возможности хранилища в Windows Server 2016.

Дисковые пространства прямого подключения

Локальные дисковые пространства позволяют создавать масштабируемые хранилища с высоким уровнем доступности с помощью серверов с локальным хранилищем. Они упрощают развертывание и администрирование программно-определяемых систем хранения данных и открывают возможность использования дисковых устройств новых классов, например SATA SSD и NVMe. Ранее для кластерных дисковых пространств с общими дисками это было невозможно.

Дополнительные сведения см. в статье Локальные дисковые пространства.

Реплика хранилища

Реплика хранилища реализует независимую от хранилища синхронную репликацию между серверами или кластерами на уровне блоков для аварийного восстановления, а также растягивание отказоустойчивого кластера между сайтами. Синхронная репликация позволяет зеркально отображать данные в физических расположениях с отказоустойчивыми томами, что полностью предотвращает потерю данных на уровне файловой системы. Асинхронная репликация позволяет использовать физические расположения за пределами города, но при этом вероятна потеря данных.

Дополнительные сведения см. в статье Реплика хранилища.

Качество обслуживания хранилища

Функцию качества обслуживания хранилища (QoS) теперь можно использовать для централизованного отслеживания общей производительности хранилища, а также для создания политик управления с помощью Hyper-V и кластеров CSV в Windows Server 2016.

Дополнительные сведения см. в статье Качество обслуживания хранилища.

Отказоустойчивая кластеризация

Windows Server 2016 включает ряд новых возможностей и усовершенствований для нескольких серверов, которые группируются в один отказоустойчивый кластер с помощью функции отказоустойчивой кластеризации. Дополнения приведены ниже; более полный список см. в статье Новые возможности отказоустойчивой кластеризации в Windows Server 2016.

Последовательное обновление ОС кластера

Последовательное обновление ОС кластера позволяет администратору обновлять ОС узлов кластера с Windows Server 2012 R2 до Windows Server 2016, не останавливая рабочие нагрузки Hyper-V или масштабируемого файлового сервера. Благодаря этой функции можно избежать штрафов за простои, которые полагаются согласно соглашениям об уровне обслуживания.

Дополнительные сведения см. в статье Последовательное обновление ОС кластера.

Облако-свидетель

Облако-свидетель — это новый тип свидетеля кворума отказоустойчивого кластера в Windows Server 2016, который использует Microsoft Azure в качестве точки арбитража. Облако-свидетель, как любой другой свидетель кворума, получает голос и может участвовать в подсчете кворума. Вы можете настроить облако-свидетель в качестве свидетеля кворума с помощью мастера настройки кворума кластера.

Дополнительные сведения см. в статье Развертывание облака-свидетеля.

Служба работоспособности

Служба работоспособности улучшает повседневные операции, мониторинг и обслуживание ресурсов кластера в локальных дисковых пространствах.

Дополнительные сведения см. в статье Служба работоспособности.

Разработка приложений

Службы IIS 10.0

Новые возможности веб-сервера IIS 10.0 в Windows Server 2016:

- Поддержка протокола HTTP/2 в стеке сети и интеграция с IIS 10.0, благодаря которой веб-сайты IIS 10.0 могут автоматически обрабатывать запросы HTTP/2 для поддерживаемых конфигураций. Если сравнивать с результатами использования HTTP/1.1, увеличена эффективность повторного использования подключений, уменьшена задержка, улучшено время загрузки веб-страниц.
- Возможность запускать службы IIS 10.0 и управлять ими в Nano Server. Сведения об IIS на сервере Nano Server.
- Поддержка заголовков узла с подстановочными знаками, благодаря которой администраторы могут настроить веб-сервер для домена так, чтобы этот веб-сервер обрабатывал запросы и для поддоменов.
- Новый модуль PowerShell (IISAdministration) для управления IIS.

Дополнительные сведения см. в статье об IIS.

Координатор распределенных транзакций (MSDTC)

В Microsoft Windows 10 и Windows Server 2016 добавлены три новые возможности:

- Диспетчер ресурсов может использовать новый интерфейс для метода Rejoin, чтобы определить результат сомнительной транзакции после перезагрузки базы данных из-за ошибки. Дополнительные сведения см. в статье о IResourceManagerRejoinable::Rejoin.

- Максимальный размер DSN-имени увеличен с 256 до 3072 байтов. Дополнительные сведения см. в статьях об IDtcToXaHelperFactory::Create, IDtcToXaHelperSinglePipe::XARMCreate и IDtcToXaMapper::RequestNewResourceManager.

- Теперь можно настроить раздел реестра так, чтобы включить путь к файлу образа в имя файла журнала трассировки, упростив таким образом поиск нужного файла журнала трассировки. Дополнительные сведения о настройке диагностической трассировки для MSDTC на компьютере под управлением Windows см. в этой статье.

Каналы обслуживания Windows Server

Статья • 28.01.2023 • Чтение занимает 9 мин

Ранее в Windows Server 2016 и Windows Server 2019 было доступно два основных канала выпуска: Long-Term Servicing Channel и Semi-Annual Channel. Long-Term Servicing Channel (LTSC) предоставляет более долгосрочный вариант с акцентом на стабильность, тогда как Semi-Annual Channel (SAC) обеспечивает более частые выпуски, позволяя клиентам быстрее использовать преимущества инноваций.

Начиная с версии Windows Server 2022, будет доступен один основной канал выпуска — Long-Term Servicing Channel. Основное внимание в Semi-Annual Channel в предыдущих версиях Windows Server уделялось контейнерам и микрослужбам, и эти инновации будут и дальше реализовываться в Azure Stack HCI.

Long-Term Servicing Channel (LTSC)

При использовании Long-Term Servicing Channel новая основная версия Windows Server выпускается каждые 2–3 года. Пользователи имеют право на 5 лет основной поддержки и 5 лет расширенной поддержки. Этот канал обеспечивает системам возможность длительного обслуживания и функциональную стабильность и может быть установлен в рамках вариантов установки основных серверных компонентов или сервера с возможностями рабочего стола. На развертывания LTSC Windows Server не влияют выпуски Semi-Annual Channel. Канал Long-Term Servicing Channel продолжит получать обновления системы безопасности и не связанные с безопасностью обновления, но не получит новые функции и возможности.

Semi-Annual Channel

Канал Semi-Annual Channel позволяет клиентам, быстро внедряющим инновации, скорее начать использовать возможности новой операционной системы с поддержкой контейнеров и микрослужб. Для каждого выпуска в этом канале предоставляется поддержка в течение 18 месяцев начиная с даты начального выпуска.

> **Примечание**
>
> Дальнейшие выпуски Semi-Annual Channel Windows Server не планируются. Клиентам, использующим SAC, необходимо перейти на **Azure Stack HCI** с такой

же периодичностью выпусков и быстрыми инновациями с такими функциями, как **Служба Azure Kubernetes в Azure Stack HCI** . В качестве альтернативы можно использовать канал Long-Term Servicing Channel Windows Server.

Большая часть функций, реализованных в канале Semi-Annual Channel, содержится в следующем выпуске канала Long-Term Servicing для Windows Server. Канал Semi-Annual Channel доступен корпоративным клиентам, участвующим в программе Software Assurance, а также через Azure Marketplace или другого поставщика облачных услуг / услуг хостинга, а также в рамках программ лояльности, таких как подписки на Visual Studio.

> ⓘ **Примечание**
>
> **Текущий выпуск канала Semi-Annual Channel — Windows Server версии 20H2**. Чтобы присоединиться к этому каналу, требуется ОС Windows Server версии 20H2, которую можно установить в режиме основных серверных компонентов или в виде Nano Server с выполнением в контейнере. Обновления на месте выпуска Long-Term Servicing Channel не поддерживаются, так как они находятся в **разных каналах выпуска**. Справедливо и обратное. Вы не сможете выполнить обновление с Semi-Annual Channel до Long-Term Servicing Channel или перейти на эту версию, не выполнив чистую установку.
>
> Выпуск Semi-Annual Channel не является обновлением. Это следующий выпуск Windows Server в канале Semi-Annual Channel. Обновления на месте с одного выпуска Semi-Annual Channel до выпуска Semi-Annual Channel с более высокой версией поддерживаются. Это упрощает использование выпусков (с учетом их частоты).

В этой модели выпуски Windows Server идентифицированы по году и месяцу выпуска, например выпуск от 9-го месяца (сентября) 2017 года будет обозначаться как **версия 1709**. Новые выпуски Windows Server в канале Semi-Annual Channel появлялись два раза в год. Срок поддержки для каждого выпуска составляет 18 месяцев. Начиная с выпусков, реализованных осенью 2020 г. (20H2), мы меняем обозначения. Вместо месяца для именования выпуска использован цикл выпуска. Например: **версия 20H2** для выпуска во второй половине 2020 г.

Основные отличия

В следующей таблице приведены основные различия между каналами.

Описание	Long-Term Servicing Channel (Windows Server 2019)	Semi-Annual Channel (Windows Server)
Рекомендуемые сценарии	Файловые серверы общего назначения, рабочие нагрузки Майкрософт и других производителей, традиционные приложения, инфраструктурные роли, программно-определяемые центры обработки данных и гиперконвергентная инфраструктура.	Контейнерные приложения, узлы контейнеров и сценарии с приложениями, где ускоренные инновации приносят пользу
Новые выпуски	Каждые 2–3 года	Каждые 6 месяцев
Поддержка	5 лет основной поддержки, а также 5 лет расширенной поддержки	18 месяцев
Выпуски	Все доступные выпуски Windows Server	Выпуски Standard и Datacenter
Возможные пользователи	Все клиенты во всех каналах	Только клиенты облака и клиенты Software Assurance
Параметры установки	Основные серверные компоненты и сервер с возможностями рабочего стола	Основные серверные компоненты для узла контейнеров, образа контейнера и образа контейнера Nano Server

ⓘ Важно!

Учитывайте, что набор ролей и функций в Windows Server SAC (доступный только при установке в качестве основных серверных компонентов) отличается от набора Windows Server LTSC при установке в качестве основных серверных компонентов. Например, вы не сможете использовать Windows Server SAC в качестве платформы для таких служб, как Локальные дисковые пространства.

Совместимость устройств

Если не будет указано иное, минимальные требования к оборудованию для запуска выпусков Semi-Annual Channel аналогичны минимальным требованиям,

предъявляемым к последнему выпуску Long-Term Servicing Channel для Windows Server. Большинство драйверов оборудования продолжат работать в этих выпусках.

Обслуживание

Для обоих выпусков — Long-Term Servicing Channel и Semi-Annual Channel — будут доступны обновления системы безопасности, а также не связанные с безопасностью обновления до дат, указанных на страницах о жизненном цикле Майкрософт. Выпуски будут отличаться лишь длительностью предоставления поддержки, как описано выше.

Средства обслуживания

Существует множество средств, с помощью которых ИТ-специалисты могут обслуживать Windows Server. Каждый вариант имеет свои преимущества и недостатки с точки зрения возможностей, контроля, простоты и низких административных требований. Ниже приведены примеры средств обслуживания для управления обслуживающими обновлениями.

- **Центр обновления Windows (автономный)** . Этот вариант доступен только для серверов, которые подключены к Интернету и для которых активирован Центр обновления Windows.
- **Windows Server Update Services (WSUS)** обеспечивают расширенный контроль над обновлениями Windows Server и клиента Windows и доступны в операционной системе Windows Server на уровне кода. Помимо возможности откладывать обновления организации могут также добавить уровень утверждения обновлений и развертывать их на конкретных компьютерах или в группах компьютеров по мере готовности.
- **Microsoft Endpoint Configuration Manager** обеспечивает максимальный контроль над обслуживанием. ИТ-специалисты могут откладывать обновления, утверждать их и использовать различные возможности для целевых развертываний и контроля над использованием пропускной способности и временем развертывания.

Скорее всего, вы уже используете хотя бы один из этих вариантов, выбрав его с учетом имеющихся ресурсов, персонала и знаний. Вы можете продолжать использовать тот же процесс для выпусков Semi-Annual Channel: например, если вы уже используете Configuration Manager для управления обновлениями, можно и дальше применять это решение. Аналогичным образом, если вы используете WSUS, можно продолжать это делать.

Где можно получить выпуски Semi-Annual Channel

Для выпусков Semi-Annual Channel следует применять чистую установку. Но можно выполнить обновление на месте с помощью ISO с одной версии SAC до более поздней.

- Volume Licensing Service Center (VLSC). Корпоративным клиентам, участвующим в программе Software Assurance, для получения этого выпуска следует перейти на веб-сайт Volume Licensing Service Center и нажать кнопку **Вход**. Затем необходимо щелкнуть **Загрузки и ключи** и найти этот выпуск.
- Выпуски каналов Semi-Annual Channel также доступны в Microsoft Azure.
- Подписки Visual Studio. Подписчики Visual Studio могут получить выпуски Semi-Annual Channel, скачав их на странице загрузки для подписчиков Visual Studio. Если вы еще не являетесь подписчиком, перейдите на страницу Подписки на Visual Studio, зарегистрируйтесь, а затем перейдите на страницу скачивания для подписчиков Visual Studio, как указано выше. Выпуски, полученные с помощью подписок на Visual Studio, используются только для разработки и тестирования.

Активация выпусков Semi-Annual Channel

- При использовании Microsoft Azure выпуски Semi-Annual Channel должны активироваться автоматически.
- Если вы получили этот выпуск через центр Volume Licensing Service Center или подписки Visual Studio, для активации воспользуйтесь клиентским ключом корпоративного лицензирования Windows Server (CSVLK, также называемым ключом узла KMS) с помощью среды системы управления ключами (KMS). Дополнительные сведения см. на странице Ключи установки клиента KMS.

> **Примечание**
>
> Чтобы упростить обслуживание и управление активацией, вы можете использовать ADBA (активация на основе Active Directory) для Windows Server 2012 и более поздних версий, в том числе Windows Server SAC. Кроме того, вы можете управлять лицензиями с помощью инструмента VAMT 3.x (Volume Activation Management Tool), который входит в состав последней версии ADK.

Выпуски Semi-Annual Channel, выпущенные вместе с Windows Server 2019 или позже, используют CSVLK для Windows Server 2019. Выпуски Semi-Annual Channel, выпущенные до Windows Server 2019, используют CSVLK для Windows Server 2016.

Почему выпуски Semi-Annual Channel предлагают только вариант установки основных компонентов?

Одним из важнейших наших шагов при планировании каждого выпуска Windows Server является учет отзывов клиентов о том, как они используют Windows Server. Какие новые возможности окажут наибольшее влияние на среды Windows Server и, следовательно, на текущую деятельность компании? Согласно вашим отзывам, приоритетной задачей является максимально быстрое и эффективное внедрение инноваций. В то же время клиенты, внедряющие инновации наиболее быстро, сообщили нам, что они в основном используют сценарии командной строки в PowerShell для управления центрами обработки данных. Поэтому при установке Windows Server с возможностями рабочего стола им едва ли потребуется графический пользовательский интерфейс рабочего стола, особенно теперь, когда для удаленного управления вашими серверами доступен Windows Admin Center.

Отдавая предпочтение варианту установки основных серверных компонентов, мы получаем возможность направить больше ресурсов на нововведения, сохраняя при этом присущие платформе Windows Server возможности и широкий спектр поддерживаемых приложений.

Начиная с Windows Server версии 1809 и Windows Server 2019, функция совместимости приложений основных серверных компонентов по требованию (FOD) является дополнительным пакетом компонентов, который значительно улучшает совместимость приложений для установки основных серверных компонентов Windows за счет включения подмножества двоичных файлов и пакетов из Windows Server с возможностями рабочего стола без добавления графической среды возможностей рабочего стола Windows Server.

Как насчет Nano Server?

Сервер Nano Server доступен только в качестве операционной системы контейнера. См. дополнительные сведения о базовом образе ОС контейнера.

Как определить, работает ли на сервере выпуск LTSC или SAC

Раньше выпуски канала Long-Term Servicing Channel, такие как Windows Server 2019, выпускались одновременно с новой версией канала Semi-Annual Channel, например Windows Server версии 1809 был выпущен одновременно с Windows Server 2019. Из-за этого сложнее определить, работает ли на сервере выпуск канала Semi-Annual Channel. Вместо того, чтобы смотреть на номер сборки, следует посмотреть на название продукта. Выпуски канала Semi-Annual Channel используют имя продукта Windows Server Standard или Windows Server Datacenter без номера версии, в то время как выпуски канала Long-Term Servicing Channel содержат номер версии, например Windows Server 2019 Datacenter.

> **Примечание**
>
> Приведенные ниже инструкции помогут идентифицировать LTSC и SAC и выявить различия между ними в целях управления жизненным циклом и общей инвентаризации. Они не предназначены для определения совместимости приложений или представления поверхности определенного API. Для обеспечения совместимости разработчикам приложений следует использовать другие инструкции, так как в течение срока эксплуатации системы могут добавляться компоненты, API и функции, либо они могут быть еще недоступны. **Версия операционной системы** — оптимальная отправная точка для разработчиков приложений.

Откройте PowerShell и используйте командлет `Get-ItemProperty` или командлет `Get-ComputerInfo`, чтобы проверить соответствующие свойства в реестре. Вместе с номером сборки вы сможете найти информацию о наличии или отсутствии LTSC или SAC по году выпуска, например 2019 — LTSC имеется, в то время как SAC — нет. Вы также узнаете время выпуска по идентификатору ReleaseId или WindowsVersion, например 1809, а также тип установки: основные серверные компоненты или сервер с возможностями рабочего стола.

Пример выпуска Windows Server 2019 Datacenter Edition (LTSC) с возможностями рабочего стола:

PowerShell

```
Get-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\CurrentVersion"
| Select ProductName, ReleaseId, InstallationType,
CurrentMajorVersionNumber,CurrentMinorVersionNumber,CurrentBuild
```

```
ProductName               : Windows Server 2019 Datacenter
ReleaseId                 : 1809
InstallationType          : Server
CurrentMajorVersionNumber : 10
CurrentMinorVersionNumber : 0
CurrentBuild              : 17763
```

Пример основных серверных компонентов Windows Server, версия 1809 (SAC), Standard Edition:

PowerShell

```
Get-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\CurrentVersion"
| Select ProductName, ReleaseId, InstallationType,
CurrentMajorVersionNumber,CurrentMinorVersionNumber,CurrentBuild
```

```
ProductName               : Windows Server Standard
ReleaseId                 : 1809
InstallationType          : Server Core
CurrentMajorVersionNumber : 10
CurrentMinorVersionNumber : 0
CurrentBuild              : 17763
```

Пример основных серверных компонентов Windows Server 2019 Standard Edition (LTSC):

PowerShell

```
Get-ComputerInfo | Select WindowsProductName, WindowsVersion,
WindowsInstallationType, OsServerLevel, OsVersion,
OsHardwareAbstractionLayer
```

```
WindowsProductName            : Windows Server 2019 Standard
WindowsVersion                : 1809
WindowsInstallationType       : Server Core
OsServerLevel                 : ServerCore
OsVersion                     : 10.0.17763
OsHardwareAbstractionLayer    : 10.0.17763.107
```

Чтобы уточнить наличие на сервере новой функции совместимости приложений основных серверных компонентов по требованию, воспользуйтесь командлетом

Get-WindowsCapability и найдите следующее:

```
Name    :     ServerCore.AppCompatibility~~~~0.0.1.0
State   :     Installed
```

Сравнение выпусков Windows Server 2022 Standard, Datacenter и Datacenter: Azure Edition

Статья • 28.01.2023 • Чтение занимает 7 мин

С помощью приведенных в этой статье сведений сравните выпуски Windows Server 2022 Standard, Datacenter и Datacenter: Azure Edition, чтобы выбрать для себя наиболее подходящий.

Общедоступные возможности

Полное сравнение

Общедоступные компоненты	**Windows Server 2022 Standard**	**Windows Server 2022 Datacenter**	**Windows Server 2022 Datacenter: Azure Edition**
Расширенная сеть Azure	Нет	Нет	**Да**
Анализатор соответствия рекомендациям	Да	Да	Да
Контейнеры	Да	Да	Да
Прямой доступ	Да	Да	Да
Динамическая память (в виртуализации)	Да	Да	Да
Горячее добавление и удаление оперативной памяти	Да	Да	Да
возникла в результате горячего исправления;	Нет	Нет	**Да**
Microsoft Management Console (MMC)	Да	Да	Да

Общедоступные компоненты	**Windows Server 2022 Standard**	**Windows Server 2022 Datacenter**	**Windows Server 2022 Datacenter: Azure Edition**
Минимальный интерфейс сервера	Да	Да	Да
Network Load Balancing	Да	Да	Да
Windows PowerShell	Да	Да	Да
Установка основных серверных компонентов	Да	Да	Да
Диспетчер серверов	Да	Да	Да
SMB Direct и SMB через RDMA	Да	Да	Да (не поддерживается в Azure)
Сжатие SMB	Да	Да	Да
SMB по QUIC	Нет	Нет	**Да**
Программно-определяемая сеть	Нет	**Да**	**Да**
Служба миграции хранилища	Да	Да	Да
Реплика хранилища	Да, (1 партнерство и 1 группа ресурсов с одним томом в 2 ТБ)	Да, **без ограничений**	Да, **без ограничений**
Сжатие реплики хранилища	Нет	Нет	**Да**
Дисковые пространства	Да	Да	Да
Дисковые пространства прямого подключения	Нет	**Да**	**Да**
Службы активации корпоративных лицензий	Да	Да	Да

Общедоступные компоненты	Windows Server 2022 Standard	Windows Server 2022 Datacenter	Windows Server 2022 Datacenter: Azure Edition
Интеграция со службами теневого копирования (VSS)	Да	Да	Да
Службы Windows Server Update Services	Да	Да	Да
Учет серверных лицензий	Да	Да	Да
Наследование активаций	Как гость, если служба размещена на выпуске Datacenter	**Узел или гость**	**Узел или гость**
рабочие папки	Да	Да	Да

Блокировки и ограничения

Полное сравнение

Блокировки и ограничения	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Максимальное число пользователей	По числу клиентских лицензий	По числу клиентских лицензий
Максимальное число подключений SMB	16 777 216	16 777 216
Максимальное число подключений RRAS	Неограниченно	Неограниченно
Максимальное число подключений IAS	2 147 483 647	2 147 483 647
Максимальное число подключений RDS	65 535	65 535
Максимальное число сокетов в 64-разрядной версии	64	64

Блокировки и ограничения	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Максимальное число ядер	Неограниченно	Неограниченно
Максимальный объем ОЗУ	48 ТБ	48 ТБ
Можно использовать как гостевую службу виртуализации	Да; 2 виртуальные машины и один узел Hyper-V на лицензию	Да; **неограниченное количество виртуальных машин** и один узел Hyper-V на лицензию.
Контейнеры Windows Server	Неограниченно	Неограниченно
Виртуальные изолированные контейнеры OSE/Hyper-V	2	Неограниченно
Сервер может присоединиться к домену	Да	Да
Защита периметра сети или брандмауэр	Нет	Нет
DirectAccess	Да	Да
DLNA-кодеки и потоковая передача мультимедиа в Интернете	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола

Роли сервера

Полное сравнение

Доступны роли Windows Server	Службы ролей	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Службы сертификатов Active Directory		Да	Да

Доступны роли Windows Server	Службы ролей	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Доменные службы Active Directory		Да	Да
Службы федерации Active Directory (AD FS)		Да	Да
Службы Active Directory облегченного доступа к каталогам (AD LDS)		Да	Да
Службы управления правами Active Directory (AD RMS)		Да	Да
Подтверждение работоспособности устройств		Да	Да
DHCP-сервер		Да	Да
DNS-сервер		Да	Да
Факс-сервер		Да	Да
Файловые службы и службы хранилища	Файловый сервер	Да	Да
Файловые службы и службы хранилища	Служба BranchCache для сетевых файлов	Да	Да
Файловые службы и службы хранилища	дедупликация данных;	Да	Да
Файловые службы и службы хранилища	Пространства имен DFS	Да	Да
Файловые службы и службы хранилища	Репликация DFS	Да	Да
Файловые службы и службы хранилища	File Server Resource Manager	Да	Да

Доступны роли Windows Server	Службы ролей	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Файловые службы и службы хранилища	Служба агента VSS файлового сервера	Да	Да
Файловые службы и службы хранилища	Целевой сервер iSCSI	Да	Да
Файловые службы и службы хранилища	Поставщик хранилища цели iSCSI	Да	Да
Файловые службы и службы хранилища	Сервер для NFS	Да	Да
Файловые службы и службы хранилища	рабочие папки	Да	Да
Файловые службы и службы хранилища	Службы хранения	Да	Да
Служба защиты узла		Да	Да
Hyper-V		Да	Да; в том числе экранированные виртуальные машины
Сетевой контроллер		Нет	**Да**
Network Policy and Access Services		Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Службы печати и документов		Да	Да
Удаленный доступ		Да	Да
Службы удаленных рабочих столов		Да	Да
Службы активации корпоративных лицензий		Да	Да
Веб-службы (IIS)		Да	Да

Доступны роли Windows Server	Службы ролей	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Windows Deployment Services		Да	Да
Службы Windows Server Update Services		Да	Да

Функции

Полное сравнение

Доступные компоненты Windows Server	Windows Server 2022 Standard	Windows Server 2022 Datacenter
.NET Framework 3.5	Да	Да
.NET Framework 4.8	Да	Да
Фоновая интеллектуальная служба передачи (BITS)	Да	Да
Шифрование диска BitLocker	Да	Да
Сетевая разблокировка BitLocker	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
BranchCache	Да	Да
Клиент для NFS	Да	Да
Контейнеры	Да	Да
Data Center Bridging	Да	Да
Direct Play	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Enhanced Storage;	Да	Да

Доступные компоненты Windows Server	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Отказоустойчивая кластеризация	Да	Да
Управление групповой политикой	Да	Да
Поддержка защиты узла Hyper-V	Нет	**Да**
Качество обслуживания ввода-вывода	Да	Да
Внедряемое веб-ядро служб IIS	Да	Да
Клиент печати через Интернет	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Сервер управления IP-адресами (IPAM)	Да	Да
Монитор порта LPR	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Расширение IIS OData для управления	Да	Да
Media Foundation	Да	Да
Очередь сообщений	Да	Да
Антивирусная программа Microsoft Defender	Да	Да
Multipath I/O;	Да	Да
Соединитель MultiPoint	Да	Да
Network Load Balancing	Да	Да
Виртуализация сети	Да	Да
протокол PNRP;	Да	Да
qWave;	Да	Да

Доступные компоненты Windows Server	Windows Server 2022 Standard	Windows Server 2022 Datacenter
пакет администрирования диспетчера RAS-подключений (CMAK);	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Удаленная помощь	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
удаленное разностное сжатие;	Да	Да
Средства удаленного администрирования сервера (RSAT)	Да	Да
RPC через HTTP-прокси;	Да	Да
Коллекция событий установки и загрузки	Да	Да
простые службы TCP/IP;	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Поддержка протоколов общего доступа к файлам SMB 1.0 и CIFS	Да	Да
Ограничение пропускной способности SMB	Да	Да
SMTP-сервер	Да	Да
служба SNMP;	Да	Да
Подсистема балансировки нагрузки программного обеспечения	Да	Да
Служба миграции хранилища	Да	Да
Прокси-сервер службы миграции хранилища	Да	Да

Доступные компоненты Windows Server	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Реплика хранилища	Да	Да
Архиватор системных данных	Да	Да
Системная аналитика	Да	Да
Клиент Telnet	Да	Да
TFTP-клиент	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Средства экранирования виртуальных машин для управления структурой	Да	Да
Перенаправитель WebDAV	Да	Да
Биометрическая платформа Windows	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Windows Identity Foundation 3.5	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Внутренняя база данных Windows	Да	Да
Windows PowerShell	Да	Да
Служба активации процессов Windows	Да	Да
Служба Windows Search	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Система архивации данных Windows Server	Да	Да

Доступные компоненты Windows Server	Windows Server 2022 Standard	Windows Server 2022 Datacenter
Средства миграции Windows Server	Да	Да
Стандартизированное управление хранилищами Windows	Да	Да
Подсистема Windows для Linux	Да	Да
Фильтры Windows TIFF IFilter	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Расширение IIS WinRM	Да	Да
WINS-сервер	Да	Да
Служба беспроводной локальной сети	Да	Да
поддержка WoW64.	Да	Да
Средство просмотра XPS	Да, установлено в рамках варианта "Сервер с возможностями рабочего стола"	Да, установлено в рамках варианта "Сервер с возможностями рабочего стола"

Сравнение выпусков Windows Server 2019 Standard и Datacenter

Статья • 28.01.2023 • Чтение занимает 6 мин

С помощью приведенных в этой статье сведений сравните выпуски Windows Server 2019 Standard и Datacenter, чтобы выбрать для себя наиболее подходящий.

Общедоступные возможности

Полное сравнение

Общедоступные компоненты	**Windows Server 2019 Standard**	**Windows Server 2019 Datacenter**
Анализатор соответствия рекомендациям	Да	Да
Прямой доступ	Да	Да
Динамическая память (в виртуализации)	Да	Да
Горячее добавление и удаление оперативной памяти	Да	Да
Microsoft Management Console (MMC)	Да	Да
Минимальный интерфейс сервера	Да	Да
Network Load Balancing	Да	Да
Windows PowerShell	Да	Да
Установка основных серверных компонентов	Да	Да
Диспетчер серверов	Да	Да
SMB Direct и SMB через RDMA	Да	Да

Общедоступные компоненты	**Windows Server 2019 Standard**	**Windows Server 2019 Datacenter**
Программно-определяемая сеть	Нет	**Да**
Служба миграции хранилища	Да	Да
Реплика хранилища	Да, (1 партнерство и 1 группа ресурсов с одним томом в 2 ТБ)	Да, **без ограничений**
Дисковые пространства	Да	Да
Дисковые пространства прямого подключения	Нет	**Да**
Службы активации корпоративных лицензий	Да	Да
Интеграция со службами теневого копирования (VSS)	Да	Да
Службы Windows Server Update Services	Да	Да
Учет серверных лицензий	Да	Да
Наследование активаций	Как гость, если служба размещена на выпуске Datacenter	**Узел или гость**
рабочие папки	Да	Да

Блокировки и ограничения

Полное сравнение

Блокировки и ограничения	**Windows Server 2019 Standard**	**Windows Server 2019 Datacenter**
Максимальное число пользователей	По числу клиентских лицензий	По числу клиентских лицензий
Максимальное число подключений SMB	16 777 216	16 777 216

Блокировки и ограничения	Windows Server 2019 Standard	Windows Server 2019 Datacenter
Максимальное число подключений RRAS	без ограничений	без ограничений
Максимальное число подключений IAS	2 147 483 647	2 147 483 647
Максимальное число подключений RDS	65 535	65 535
Максимальное число сокетов в 64-разрядной версии	64	64
Максимальное число ядер	без ограничений	без ограничений
Максимальный объем ОЗУ	24 ТБ	24 ТБ
Можно использовать как гостевую службу виртуализации	Да; 2 виртуальные машины и один узел Hyper-V на лицензию	Да; **неограниченное количество виртуальных машин** и один узел Hyper-V на лицензию.
Сервер может присоединиться к домену	да	да
Защита периметра сети или брандмауэр	нет	нет
DirectAccess	да	да
DLNA-кодеки и потоковая передача мультимедиа в Интернете	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола

Роли сервера

Полное сравнение

Доступны роли Windows Server	Службы ролей	Windows Server 2019 Standard	Windows Server 2019 Datacenter

Доступны роли Windows Server	Службы ролей	Windows Server 2019 Standard	Windows Server 2019 Datacenter
Службы сертификатов Active Directory		Да	Да
Доменные службы Active Directory		Да	Да
Службы федерации Active Directory (AD FS)		Да	Да
Службы Active Directory облегченного доступа к каталогам (AD LDS)		Да	Да
Службы управления правами Active Directory (AD RMS)		Да	Да
Подтверждение работоспособности устройств		Да	Да
DHCP-сервер		Да	Да
DNS-сервер		Да	Да
Факс-сервер		Да	Да
Файловые службы и службы хранилища	Файловый сервер	Да	Да
Файловые службы и службы хранилища	Служба BranchCache для сетевых файлов	Да	Да
Файловые службы и службы хранилища	дедупликация данных;	Да	Да
Файловые службы и службы хранилища	Пространства имен DFS	Да	Да
Файловые службы и службы хранилища	Репликация DFS	Да	Да

Доступны роли Windows Server	Службы ролей	Windows Server 2019 Standard	Windows Server 2019 Datacenter
Файловые службы и службы хранилища	File Server Resource Manager	Да	Да
Файловые службы и службы хранилища	Служба агента VSS файлового сервера	Да	Да
Файловые службы и службы хранилища	Целевой сервер iSCSI	Да	Да
Файловые службы и службы хранилища	Поставщик хранилища цели iSCSI	Да	Да
Файловые службы и службы хранилища	Сервер для NFS	Да	Да
Файловые службы и службы хранилища	рабочие папки	Да	Да
Файловые службы и службы хранилища	Службы хранения	Да	Да
Служба защиты узла		Да	Да
Hyper-V		Да	Да; в том числе экранированные виртуальные машины
Сетевой контроллер		Нет	**Да**
Network Policy and Access Services		Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Службы печати и документов		Да	Да
Удаленный доступ		Да	Да
Службы удаленных рабочих столов		Да	Да

Доступны роли Windows Server	Службы ролей	Windows Server 2019 Standard	Windows Server 2019 Datacenter
Службы активации корпоративных лицензий		Да	Да
Веб-службы (IIS)		Да	Да
Windows Deployment Services		Да*	Да*
Службы Windows Server Update Services		Да	Да

> **Примечание**
>
> WDS Transport Server — новая возможность в установках основных серверных компонентов Windows Server 2019, которая также включена в Semi-Annual Channel, начиная с Windows Server версии 1803.

Функции

Полное сравнение

Доступные компоненты Windows Server	Windows Server 2019 Standard	Windows Server 2019 Datacenter
.NET Framework 3.5	Да	Да
.NET Framework 4.7	Да	Да
Фоновая интеллектуальная служба передачи (BITS)	Да	Да
Шифрование диска BitLocker	Да	Да
Сетевая разблокировка BitLocker	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола

Доступные компоненты Windows Server	**Windows Server 2019 Standard**	**Windows Server 2019 Datacenter**
BranchCache	Да	Да
Клиент для NFS	Да	Да
Контейнеры	Да (контейнеры Windows — без ограничений; контейнеры Hyper-V — до двух)	Да (**контейнеры Windows и контейнеры Hyper-V — без ограничений**)
Data Center Bridging	Да	Да
Direct Play	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Enhanced Storage;	Да	Да
Отказоустойчивая кластеризация	Да	Да
Управление групповой политикой	Да	Да
Поддержка защиты узла Hyper-V	Нет	**Да**
Качество обслуживания ввода-вывода	Да	Да
Внедряемое веб-ядро служб IIS	Да	Да
Клиент печати через Интернет	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Сервер управления IP-адресами (IPAM)	Да	Да
Службы iSNS-сервера	Да	Да
Монитор порта LPR	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола

Доступные компоненты Windows Server	Windows Server 2019 Standard	Windows Server 2019 Datacenter
Расширение IIS OData для управления	Да	Да
Media Foundation	Да	Да
Очередь сообщений	Да	Да
Multipath I/O;	Да	Да
Соединитель MultiPoint	Да	Да
Network Load Balancing	Да	Да
протокол PNRP;	Да	Да
qWave;	Да	Да
пакет администрирования диспетчера RAS-подключений (CMAK);	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Удаленная помощь	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
удаленное разностное сжатие;	Да	Да
Средства удаленного администрирования сервера (RSAT)	Да	Да
RPC через HTTP-прокси;	Да	Да
Коллекция событий установки и загрузки	Да	Да
простые службы TCP/IP;	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Поддержка протоколов общего доступа к файлам SMB 1.0 и CIFS	Да	Да

Доступные компоненты Windows Server	Windows Server 2019 Standard	Windows Server 2019 Datacenter
Ограничение пропускной способности SMB	Да	Да
SMTP-сервер	Да	Да
служба SNMP;	Да	Да
Подсистема балансировки нагрузки программного обеспечения	Да	Да
Служба миграции хранилища	Да	Да
Прокси-сервер службы миграции хранилища	Да	Да
Реплика хранилища	Да	Да
Архиватор системных данных	Да	Да
Системная аналитика	Да	Да
Клиент Telnet	Да	Да
TFTP-клиент	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Средства экранирования виртуальных машин для управления структурой	Да	Да
Перенаправитель WebDAV	Да	Да
Биометрическая платформа Windows	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Антивирусная программа "Защитник Windows"	Да	Да
Windows Identity Foundation 3.5	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола

Доступные компоненты Windows Server	Windows Server 2019 Standard	Windows Server 2019 Datacenter
Внутренняя база данных Windows	Да	Да
Windows PowerShell	Да	Да
Служба активации процессов Windows	Да	Да
Служба Windows Search	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Система архивации данных Windows Server	Да	Да
Средства миграции Windows Server	Да	Да
Стандартизированное управление хранилищами Windows	Да	Да
Подсистема Windows для Linux	Да	Да
Фильтры Windows TIFF IFilter	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Расширение IIS WinRM	Да	Да
WINS-сервер	Да	Да
Служба беспроводной локальной сети	Да	Да
Поддержка WoW64	Да	Да
Средство просмотра XPS	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола

Сравнение выпусков Windows Server 2016 Standard и Datacenter

Статья • 28.01.2023 • Чтение занимает 6 мин

С помощью приведенных в этой статье сведений сравните выпуски Windows Server 2016 Standard и Datacenter, чтобы выбрать для себя наиболее подходящий.

Общедоступные возможности

Полное сравнение

Общедоступные компоненты	**Windows Server 2016 Standard**	**Windows Server 2016 Datacenter**
Анализатор соответствия рекомендациям	Да	Да
Прямой доступ	Да	Да
Динамическая память (в виртуализации)	Да	Да
Горячее добавление и удаление оперативной памяти	Да	Да
Microsoft Management Console (MMC)	Да	Да
Минимальный интерфейс сервера	Да	Да
Network Load Balancing	Да	Да
Windows PowerShell	Да	Да
Установка основных серверных компонентов	Да	Да
Вариант установки Nano Server	Да	Да
Диспетчер серверов	Да	Да
SMB Direct и SMB через RDMA	Да	Да

Общедоступные компоненты	**Windows Server 2016 Standard**	**Windows Server 2016 Datacenter**
Программно-определяемая сеть	Нет	**Да**
Реплика хранилища	Нет	**Да**
Дисковые пространства	Да	Да
Дисковые пространства прямого подключения	Нет	**Да**
Службы активации корпоративных лицензий	Да	Да
Интеграция со службами теневого копирования (VSS)	Да	Да
Службы Windows Server Update Services	Да	Да
Учет серверных лицензий	Да	Да
Наследование активаций	Как гость, если служба размещена на выпуске Datacenter	**Узел или гость**
рабочие папки	Да	Да

Блокировки и ограничения

Полное сравнение

Блокировки и ограничения	**Windows Server 2016 Standard**	**Windows Server 2016 Datacenter**
Максимальное число пользователей	По числу клиентских лицензий	По числу клиентских лицензий
Максимальное число подключений SMB	16 777 216	16 777 216
Максимальное число подключений RRAS	без ограничений	без ограничений

Блокировки и ограничения	Windows Server 2016 Standard	Windows Server 2016 Datacenter
Максимальное число подключений IAS	2 147 483 647	2 147 483 647
Максимальное число подключений RDS	65535	65535
Максимальное число сокетов в 64-разрядной версии	64	64
Максимальное число ядер	без ограничений	без ограничений
Максимальный объем ОЗУ	24 ТБ	24 ТБ
Можно использовать как гостевую службу виртуализации	Да; 2 виртуальные машины и один узел Hyper-V на лицензию	Да; **неограниченное количество виртуальных машин** и один узел Hyper-V на лицензию.
Сервер может присоединиться к домену	да	да
Защита периметра сети или брандмауэр	нет	нет
DirectAccess	да	да
DLNA-кодеки и потоковая передача мультимедиа в Интернете	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола

Роли сервера

Полное сравнение

Доступны роли Windows Server	Службы ролей	Windows Server 2016 Standard	Windows Server 2016 Datacenter
Службы сертификатов Active Directory		Да	Да

Доступны роли Windows Server	Службы ролей	Windows Server 2016 Standard	Windows Server 2016 Datacenter
Доменные службы Active Directory		Да	Да
Службы федерации Active Directory (AD FS)		Да	Да
Службы Active Directory облегченного доступа к каталогам (AD LDS)		Да	Да
Службы управления правами Active Directory (AD RMS)		Да	Да
Подтверждение работоспособности устройств		Да	Да
DHCP-сервер		Да	Да
DNS-сервер		Да	Да
Факс-сервер		Да	Да
Файловые службы и службы хранилища	Файловый сервер	Да	Да
Файловые службы и службы хранилища	Служба BranchCache для сетевых файлов	Да	Да
Файловые службы и службы хранилища	дедупликация данных;	Да	Да
Файловые службы и службы хранилища	Пространства имен DFS	Да	Да
Файловые службы и службы хранилища	Репликация DFS	Да	Да
Файловые службы и службы хранилища	File Server Resource Manager	Да	Да

Доступны роли Windows Server	**Службы ролей**	**Windows Server 2016 Standard**	**Windows Server 2016 Datacenter**
Файловые службы и службы хранилища	Служба агента VSS файлового сервера	Да	Да
Файловые службы и службы хранилища	Целевой сервер iSCSI	Да	Да
Файловые службы и службы хранилища	Поставщик хранилища цели iSCSI	Да	Да
Файловые службы и службы хранилища	Сервер для NFS	Да	Да
Файловые службы и службы хранилища	рабочие папки	Да	Да
Файловые службы и службы хранилища	Службы хранения	Да	Да
Служба защиты узла		Да	Да
Hyper-V		Да	Да; **в том числе экранированные виртуальные машины**.
Службы MultiPoint		Да	Да
Сетевой контроллер		Нет	**Да**
Network Policy and Access Services		Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Службы печати и документов		Да	Да
Удаленный доступ		Да	Да
Службы удаленных рабочих столов		Да	Да
Службы активации корпоративных лицензий		Да	Да

Доступны роли Windows Server	Службы ролей	Windows Server 2016 Standard	Windows Server 2016 Datacenter
Веб-службы (IIS)		Да	Да
Windows Deployment Services		Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Режим Windows Server Essentials		Да	Да
Службы Windows Server Update Services		Да	Да

Функции

Полное сравнение

Доступные компоненты Windows Server	Windows Server 2016 Standard	Windows Server 2016 Datacenter
.NET Framework 3.5	Да	Да
.NET Framework 4.6	Да	Да
Фоновая интеллектуальная служба передачи (BITS)	Да	Да
Шифрование диска BitLocker	Да	Да
Сетевая разблокировка BitLocker	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
BranchCache	Да	Да
Клиент для NFS	Да	Да
Контейнеры	Да (контейнеры Windows — без ограничений; контейнеры Hyper-V — до двух)	Да (все типы контейнеров — без ограничений)

Доступные компоненты Windows Server	Windows Server 2016 Standard	Windows Server 2016 Datacenter
Data Center Bridging	Да	Да
Direct Play	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Enhanced Storage;	Да	Да
Отказоустойчивая кластеризация	Да	Да
Управление групповой политикой	Да	Да
Поддержка защиты узла Hyper-V	Нет	**Да**
Качество обслуживания ввода-вывода	Да	Да
Внедряемое веб-ядро служб IIS	Да	Да
Клиент печати через Интернет	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
IPAM-сервер	Да	Да
Службы iSNS-сервера	Да	Да
Монитор порта LPR	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Расширение IIS OData для управления	Да	Да
Media Foundation	Да	Да
Очередь сообщений	Да	Да
Multipath I/O;	Да	Да
Соединитель MultiPoint	Да	Да

Доступные компоненты Windows Server	Windows Server 2016 Standard	Windows Server 2016 Datacenter
Network Load Balancing	Да	Да
протокол PNRP;	Да	Да
qWave;	Да	Да
Пакет администрирования диспетчера подключений RAS	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Удаленная помощь	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
удаленное разностное сжатие;	Да	Да
RSAT	Да	Да
RPC через HTTP-прокси;	Да	Да
Коллекция событий установки и загрузки	Да	Да
простые службы TCP/IP;	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Поддержка протоколов общего доступа к файлам SMB 1.0 и CIFS	Да	Да
Ограничение пропускной способности SMB	Да	Да
SMTP-сервер	Да	Да
служба SNMP;	Да	Да
Подсистема балансировки нагрузки программного обеспечения	Нет	**Да**
Реплика хранилища	Нет	Да
Клиент Telnet	Да	Да

Доступные компоненты Windows Server	Windows Server 2016 Standard	Windows Server 2016 Datacenter
TFTP-клиент	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Средства экранирования виртуальных машин для управления структурой	Да	Да
Перенаправитель WebDAV	Да	Да
Биометрическая платформа Windows	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Компоненты Защитника Windows	Да	Да
Windows Identity Foundation 3.5	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Внутренняя база данных Windows	Да	Да
Windows PowerShell	Да	Да
Служба активации процессов Windows	Да	Да
Служба Windows Search	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Система архивации данных Windows Server	Да	Да
Средства миграции Windows Server	Да	Да
Стандартизированное управление хранилищами Windows	Да	Да

Доступные компоненты Windows Server	Windows Server 2016 Standard	Windows Server 2016 Datacenter
Фильтры Windows TIFF IFilter	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола
Расширение IIS WinRM	Да	Да
WINS-сервер	Да	Да
Служба беспроводной локальной сети	Да	Да
поддержка WoW64.	Да	Да
Средство просмотра XPS	Да, если продукт установлен как сервер с возможностями рабочего стола	Да, если продукт установлен как сервер с возможностями рабочего стола

Требования к оборудованию для Windows Server

Статья • 28.01.2023 • Чтение занимает 3 мин

В этой статье приведены минимальные требования к оборудованию для запуска Windows Server. Если компьютер не удовлетворяет минимальным требованиям, вы не сможете правильно установить этот продукт. Фактические требования зависят от конфигурации системы и устанавливаемых приложений и компонентов.

Если не указано иное, эти минимальные требования к оборудованию применяются ко всем вариантам установки (основные серверные компоненты и сервер с рабочим столом), а также к выпускам Standard и Datacenter.

> ⓘ **Важно!**
>
> Возможные варианты развертывания столь разнообразны, что невозможно дать универсальные рекомендации по требованиям к оборудованию. Чтобы подробнее узнать о ресурсах, необходимых для каждой развертываемой роли сервера, обратитесь к документации по этой роли. Выполните тестовое развертывание, чтобы определить подходящие требования к оборудованию в конкретном сценарии. Это позволит добиться оптимального результата.

Процессор

Производительность процессора зависит не только от тактовой частоты, но также от количества его ядер и размера кэша. Ниже указаны требования к процессору для данного продукта.

Минимальные требования

- 64-разрядный процессор с тактовой частотой 1,4 ГГц
- Совместимый с набором инструкций для архитектуры x64
- Поддержка технологий NX и DEP
- Поддержка CMPXCHG16b, LAHF/SAHF и PrefetchW
- Поддержка преобразования адресов второго уровня (EPT или NPT)

Coreinfo, часть Windows Sysinternals, — это инструмент, который можно использовать, чтобы проверить, какой из этих возможностей обладает ваш ЦП.

ОЗУ

Ниже указаны примерные требования к ОЗУ для данного продукта.

Минимальные требования

- 512 МБ (2 ГБ для варианта установки "Сервер с рабочим столом")
- Тип ECC (код исправления ошибок) или аналогичная технология для развертывания на физических узлах

> **ⓘ Важно!**
>
> Если вы создадите виртуальную машину с минимальными поддерживаемыми параметрами оборудования (1 ядро процессора и ОЗУ объемом 512 МБ) и затем попытаетесь установить этот выпуск на виртуальной машине, установка завершится ошибкой.
>
> Чтобы этого не случилось, выполните одно из указанных ниже действий.
>
> - Выделите виртуальной машине, на которой планируется установить данный выпуск, более 800 МБ ОЗУ. По завершении установки можно уменьшить этот объем до 512 МБ в зависимости от реальной конфигурации сервера. Если вы изменили загрузочный образ, чтобы выполнить установку с дополнительными языками и обновлениями, то для выполнения установки может потребоваться выделить более 800 МБ ОЗУ.
> - Прервите процесс загрузки данного выпуска на виртуальной машине, нажав сочетание клавиш `SHIFT+F10`. Используйте программу `diskpart.exe` в открывшейся командной строке, чтобы создать и отформатировать раздел для установки. Запустите `wpeutil createpagefile /path=C:\pf.sys` (предполагается, что созданный вами раздел для установки — C:\). Затем закройте окно командной строки и продолжите установку.

Требования к контроллеру запоминающего устройства и пространству на диске

Компьютеры под управлением Windows Server должны иметь адаптер хранения, соответствующий спецификации архитектуры PCI Express. Устройства постоянного хранения на серверах, классифицируемые как жесткие диски, не должны быть

устройствами PATA. В Windows Server устройства ATA, PATA, IDE и EIDE нельзя использовать в качестве загрузочных дисков, дисков с файлом подкачки или дисков с данными.

Ниже указаны примерные **минимальные** требования к свободному месту на диске для системного раздела.

Минимальные требования 32 ГБ

> ⓘ **Примечание**
>
> Обратите ванимание, что 32 ГБ — это *абсолютный минимум* для успешной установки. Этот минимум должен позволять установить Windows Server 2022 с помощью варианта установки основных серверных компонентов с ролью сервера веб-служб (IIS). Сервер в режиме установки основных серверных компонентов примерно на 4 ГБ меньше, чем тот же сервер с вариантом установки возможности рабочего стола.
>
> В любом из следующих случаев потребуется дополнительное место для системного раздела.
>
> - Система устанавливается по сети.
> - Для компьютеров с объемом ОЗУ более 16 ГБ потребуется больше места на диске для файлов подкачки, гибернации и дампа.

Требования к сетевому адаптеру

Сетевые адаптеры, используемые в этом выпуске, должны включать следующие компоненты.

Минимальные требования

- Адаптер Ethernet с пропускной способностью не менее 1 гигабит в секунду.
- Совместимость со спецификацией архитектуры PCI Express.

Сетевой адаптер с поддержкой сетевой отладки (KDNet) может пригодиться, но не входит в минимальные требования.

Сетевой адаптер с поддержкой среды предзагрузочного выполнения (PXE) может пригодиться, но не входит в минимальные требования.

Другие требования

Компьютеры под управлением этого выпуска также должны содержать следующие компоненты.

- Дисковод DVD-дисков (если операционная система будет устанавливаться с DVD-диска)

Указанные ниже элементы требуются лишь для определенных компонентов:

- Система UEFI на основании версии 2.3.1c и встроенное ПО с поддержкой безопасной загрузки.
- Доверенный платформенный модуль
- Графическое устройство и монитор Super VGA (1024 x 768) или с более высоким разрешением.
- Клавиатура и мышь Microsoft (или другое совместимое указывающее устройство).
- Доступ к Интернету (может потребоваться дополнительная оплата)

> ⓘ **Примечание**
>
> Для использования определенных компонентов, таких как шифрование диска BitLocker, требуется микросхема доверенного платформенного модуля (TPM). Если компьютер использует доверенный платформенный модуль, он должен соответствовать следующим требованиям.
>
> - Аппаратный доверенный платформенный модуль должен иметь спецификации доверенного платформенного модуля версии 2.0.
> - Доверенный платформенный модуль, реализующий версию 2.0, должен иметь сертификат EK, который либо заранее подготовлен для доверенного платформенного модуля поставщиком оборудования, либо может быть получен устройством при первой загрузке.
> - Доверенный платформенный модуль, реализующий версию 2.0, должен поставляться в комплекте с банками памяти SHA-256 PCR и реализовать PCR от 0 до 23 для алгоритма SHA-256. Допускается поставка доверенных платформенных модулей с одним банком PCR, который можно использовать для расчета алгоритмов SHA-1 и SHA-256.
>
> Параметр UEFI, запрашивающий выключение доверенного платформенного модуля, не является обязательным требованием.

Удаленные или больше не разрабатываемые компоненты в Windows Server версии 2022

Статья • 28.01.2023 • Чтение занимает 4 мин

В каждом выпуске Windows Server добавляются новые компоненты и возможности. Иногда мы также удаляем компоненты и функциональные возможности. Как правило, это происходит, когда мы добавляем улучшенную функцию. Ниже приведены подробные сведения о компонентах и возможностях, которые были удалены в Windows Server версии 2022.

> **Совет**
>
> - Ранний доступ к сборкам Windows Server можно получить, вступив в **Программу предварительной оценки Windows для бизнеса**, — это отличный способ для проверки изменений в функциональных возможностях.

Этот список не является исчерпывающим и может быть изменен.

Semi-Annual Channel

В рамках нашего подхода, ориентированного на клиентов, мы перейдем на использование Long-Term Servicing Channel (LTSC) в качестве основного канала выпуска. Текущие выпуски Semi-Annual Channel (SAC) будут работать до дат завершения базовой поддержки, а именно до 10 мая 2022 г. для Windows Server версии 20H2 и 14 декабря 2021 г. для Windows Server версии 2004.

Помимо работы с инновациями в контейнерах и микрослужбах, ранее выпущенных в Semi-Annual Channel, мы также продолжим реализовывать улучшения для Службы Azure Kubernetes (AKS), AKS в Azure Stack HCI и другие улучшения платформы, выполненные в сотрудничестве с сообществом Kubernetes. Благодаря Long-Term Servicing Channel новая основная версия Windows Server будет выходить каждые 2–3 года. Поэтому клиенты могут рассчитывать, что частота выпусков узлов и образов контейнера будет соответствовать этой тенденции.

Компоненты, которые мы удалили в этом выпуске

Мы удаляем следующие компоненты и функциональные возможности из установленного образа продукта в Windows Server версии 2022. Приложения или код, которые зависят от этих компонентов, не будут работать в этом выпуске, если вы не используете какой-либо альтернативный метод.

Функция	Объяснение
Служба "Сервер службы имен хранилищ Интернета (iSNS)"	Служба "Сервера iSNS" теперь удалена из Windows Server версии 2022 после того, как ее было отмечено в Windows Server версии 1709 как подлежащую удалению. Вы по-прежнему можете подключаться к серверам iSNS или добавлять цели iSCSI по отдельности.

Компоненты, которые мы больше не разрабатываем

Мы прекращаем активную разработку этих компонентов и, возможно, удалим их из будущих обновлений. Некоторые компоненты заменены на другие компоненты или функции, в то время как другие компоненты теперь доступны в иных источниках.

Признак	Объяснение
Служба WINS	WINS — это устаревшая служба регистрации и разрешения имен компьютеров. Вместо WINS нужно использовать службу доменных имен (DNS). Дополнительные сведения см. в статье Служба WINS.
Защищенная структура и экранированные виртуальные машины	Windows Server и Azure Stack HCI согласовываются с Azure для предоставления преимуществ постоянных улучшений в конфиденциальных вычислениях Azure и Центре безопасности Azure. Такое согласование приводит к распространению большего количества предложений по облачной безопасности на центры обработки данных клиентов (локально). Корпорация Майкрософт продолжит предоставление поддержки этих функций, но дальнейшего их развитие не планируется. В клиентских версиях Windows функция средства удаленного администрирования сервера (RSAT): средства экранированных виртуальных машин будет удалена.

Признак	Объяснение
Запуск SConfig из окна командной строки (CMD) с помощью командлета `sconfig.cmd`	Начиная с Windows Server версии 2022, SConfig запускается **по умолчанию** при входе на сервер, на котором запущен вариант установки основных серверных компонентов. Более того, PowerShell теперь является оболочкой по умолчанию для основных серверных компонентов. Выйдя из SConfig, вы попадете в обычное интерактивное окно PowerShell. Точно так же вы можете отказаться от автозапуска SConfig. В этом случае вы получите окно PowerShell при входе. В любом сценарии можно запустить SConfig из PowerShell, запустив `SConfig`. При необходимости вы также можете запустить устаревшую командную строку (CMD) из PowerShell. Но для упрощения вариантов перехода мы планируем удалить `sconfig.cmd` из следующей версии операционной системы. Если вам нужно запустить SConfig из окна CMD, сначала необходимо запустить PowerShell.
Развертывание образа boot.wim в службе развертывания Windows (WDS)	Функция развертывания операционной системы WDS частично устарела. В рабочих процессах, использующих boot.wim с установочного носителя Windows Server 2022, будет отображаться неблокирующее уведомление о прекращении использовании. Это никак не повлияет на рабочие процессы. Рабочие процессы Windows 11 и будущих версий Windows Server, которые используют образы boot.wim с установочного носителя, будут заблокированы. Альтернативы WDS, такие как Microsoft Endpoint Configuration Manager или Microsoft Deployment Toolkit (MDT), предоставляют лучшие, более гибкие и многофункциональные возможности для развертывания образов Windows. Вместо этого рекомендуется перейти на одно из этих решений. Загрузка PXE WDS не затрагивается. Вы все еще можете использовать загрузочные устройства PXE службы WDS для пользовательских образов загрузки. Вы также можете запустить программу установки из общей сетевой папки. Это изменение не повлияет на рабочие процессы, использующие пользовательские образы boot.wim, например с Configuration Manager или MDT.
Интерфейс LSARPC	Именованный канал **\PIPE\lsarpc** для доступа к зашифрованным файлам EFS по сети будет отключен и в конечном итоге удален из будущих версий Windows. Вы по-прежнему можете использовать именованный канал **\PIPE\efsrpc** для доступа к зашифрованным файлам.
Hyper-V vSwitch в LBFO	В будущем выпуске Hyper-V vSwitch больше невозможно будет привязать группе LBFO. Вместо этого для привязки можно будет использовать технологию Switch Embedded Teaming (SET).

Признак	Объяснение
Драйвер удаленного отображения на основе XDDM	Начиная с этого выпуска, службы удаленных рабочих столов используют драйвер непрямого отображения (IDD) на основе модели драйвера дисплея Windows (WDDM) для подключений к удаленному рабочему столу в одном сеансе. Поддержка драйверов удаленного отображения на основе модели драйвера дисплея Windows 2000 (XDDM) будет удалена в следующем выпуске. Независимые поставщики программного обеспечения, использующие драйвер удаленного отображения на основе XDDM, должны планировать переход на модель драйвера WDDM. Дополнительные сведения о реализации драйвера непрямого отображения удаленного отображения см. в разделе Обновления для IddCx версии 1.4 и более поздних версий.
Средство сбора журналов UCS	Средство сбора журналов UCS, хотя явно не предназначено для использования с Windows Server, тем не менее заменяется Центром отзывов в Windows 10.

Удаленные или больше не разрабатываемые компоненты в Windows Server версии 2019

Статья • 28.01.2023 • Чтение занимает 6 мин

В каждом выпуске Windows Server добавляются новые компоненты и возможности. Иногда мы также удаляем компоненты и функциональные возможности. Как правило, это происходит, когда мы добавляем улучшенную функцию. Ниже приведены подробные сведения о компонентах и возможностях, которые были удалены в Windows Server версии 2019.

> **Совет**
>
> - Ранний доступ к сборкам Windows Server можно получить, вступив в **Программу предварительной оценки Windows**, — это отличный способ для проверки изменений в функциональных возможностях.

Этот список не является исчерпывающим и может быть изменен.

Компоненты, которые мы удалили в этом выпуске

Мы удаляем следующие компоненты и функциональные возможности из установленного образа продукта в Windows Server версии 2019. Приложения или код, которые зависят от этих компонентов, не будут работать в этом выпуске, если вы не используете какой-либо альтернативный метод.

Функция	Объяснение
Бизнес-сканирование, также известное как распределенное управление сканированием (DSM)	Мы удаляем это безопасное сканирование и возможность управления сканером — устройств, поддерживающих эту функцию, нет.

Функция	Объяснение
Компоненты печати — теперь это дополнительные компоненты для варианта установки основных серверных компонентов.	В предыдущих выпусках Windows Server компоненты печати были **отключены** по умолчанию в варианте установки основных серверных компонентов. Мы внесли изменения в Windows Server 2016, сделав эти компоненты включенными по умолчанию. В Windows Server 2019 эти компоненты печати опять отключены по умолчанию для основных серверных компонентов. Чтобы включить компоненты печати, выполните командлет `Install-WindowsFeature Print-Server`.
Брокер подключений к удаленному рабочему столу и узел виртуализации удаленных рабочих столов в установке основных серверных компонентов	Большинство развертываний служб удаленных рабочих столов имеют эти роли совместно с узлом сеансов удаленных рабочих столов (RDSH), для которого требуется сервер с возможностями рабочего стола. Чтобы обеспечить согласованность с RDSH, мы меняем эти роли, чтобы также требовать сервер с возможностями рабочего стола. Эти роли RDS больше не доступны для использования в установке основных серверных компонентов. Если вам необходимо развернуть эти роли как часть инфраструктуры удаленного рабочего стола, можно установить их в Windows Server с возможностями рабочего стола. Эти роли также включаются в вариант установки с возможностями рабочего стола в Windows Server 2019.
3D-видеоадаптер RemoteFX (vGPU)	Мы разрабатываем новые параметры ускорения графики для виртуализованных сред. В качестве альтернативы также можно использовать Дискретное назначение устройств (DDA).
Вариант установки Nano Server	Сервер Nano Server недоступен в качестве операционной системы устанавливаемого узла. Вместо этого Nano Server доступен в качестве операционной системы контейнера. Дополнительные сведения о Nano Server в качестве контейнера см. в статье Базовые образы контейнеров Windows.
Server Message Block (SMB) версии 1	Начиная с этого выпуска, Server Message Block (SMB) версии 1 больше не устанавливается по умолчанию. Дополнительные сведения см. в статье SMBv1 не устанавливается по умолчанию в Windows 10 версии 1709, Windows Server версии 1709 и более поздних.
Служба репликации файлов	Службы репликации файлов, представленные в Windows Server 2003 R2, замещаются функцией репликации DFS. Необходимо перенести все контроллеры домена, использующие FRS для папки sysvol, в репликацию DFS.
Виртуализация сети Hyper-V (HNV)	Виртуализация сети теперь включена в Windows Server как часть решения программно-конфигурируемой сети (SDN). Решение SDN также включает сетевой контроллер, программную балансировку нагрузки, маршрутизацию User-Defined и списки контроль доступа.

Компоненты, которые мы больше не разрабатываем

Мы прекращаем активную разработку этих компонентов и, возможно, удалим их из будущих обновлений. Некоторые компоненты заменены на другие компоненты или функции, в то время как другие компоненты теперь доступны в иных источниках.

Признак	Объяснение
Диск для хранилища ключей в Hyper-V	Мы прекращаем работу над компонентом диска для хранилища ключей в Hyper-V. Если вы используете виртуальные машины 1-го поколения, обратитесь к статье Параметры безопасности для виртуальных машин 1-го поколения. При создании виртуальных машин используйте виртуальные машины 2-го поколения и устройства с доверенными платформенными модулями, чтобы получить более безопасное решение.
Консоль управления доверенным платформенным модулем (TPM)	Сведения, ранее доступные в консоли управления доверенным платформенным модулем, теперь доступны на странице **Device security** (Безопасность устройств) в Центре безопасности Защитника Windows.
Режим аттестации на основе Active Directory для службы защиты узла	Мы больше не разрабатываем режим аттестации Active Directory службы защиты узла. Вместо этого мы добавили новый режим аттестации — аттестацию ключа узла. Аттестация ключа узла проще и в равной степени совместима с аттестацией на основе Active Directory. Этот новый режим обеспечивает аналогичные функции, а также оптимизацию установки, более простое управление и меньшее число зависимостей инфраструктуры, чем аттестация на основе Active Directory. Аттестация ключа узла не предъявляет дополнительных требований к оборудованию, помимо требований аттестации Active Directory, поэтому все существующие системы останутся совместимыми с новым режимом. Дополнительные сведения о параметрах аттестации см. в статье Развертывание защищенных узлов .
Служба OneSync	Служба OneSync синхронизирует данные приложений "Почта", "Календарь" и "Люди". В приложение Outlook был добавлен механизм синхронизации, который обеспечивает аналогичный процесс синхронизации.
Поддержка API-интерфейса удаленного разностного сжатия	Поддержка API-интерфейса удаленного разностного сжатия позволила синхронизировать данные с удаленным источником с использованием технологий сжатия, что дает возможность уменьшить объем данных, передаваемых по сети.

Признак	Объяснение
Расширение для коммутатора упрощенной фильтрации WFP	Расширение для коммутатора упрощенной фильтрации WFP позволяет разработчикам создавать расширения для упрощенной фильтрации сетевых пакетов виртуального коммутатора Hyper-V. Вы сможете получить те же функциональные возможности, создав расширение для комплексной фильтрации. Таким образом, в будущем это расширение будет удалено.
Совместимость управления IIS 6.	Ниже приведены конкретные возможности, рассматриваемые к замене: • совместимость метабазы IIS 6 (Web-Metabase); • консоль управления IIS 6 (Web-Lgcy-Mgmt-Console); • средства создания сценариев IIS 6 (Web-Lgcy-Scripting); • совместимость WMI IIS 6 (Web-WMI). Совместимость метабазы IIS 6 выступает в качестве уровня эмуляции между скриптами метабазы на основе IIS 6 и файловой конфигурацией, используемой СЛУЖБАми IIS 7 или более поздних версий. Вы должны начать перенос скриптов управления для настройки на основе файлов IIS напрямую с помощью таких средств, как пространство имен Microsoft.Web.Administration. Также следует начать перенос с IIS 6.0 или более ранних версий и перейти на последнюю версию IIS, которая всегда доступна в самой последней версии Windows Server.
Дайджест-проверка подлинности IIS	Этот способ проверки подлинности планируется заменить. Вместо него следует начать использовать другие способы проверки подлинности, такие как сопоставление сертификата клиента (см. раздел Настройка сопоставлений клиентских сертификатов «один-к-одному») или проверка подлинности Windows (см. раздел Настройки приложения).
iSNS	Функция SMB предлагает практически те же функции с дополнительными функциями. Для получения дополнительных сведений об этой возможности см. раздел Общие сведения о протоколе SMB.
Шифрование RSA/AES для IIS	Этот метод шифрования будет заменен на более совершенный способ на основе API-интерфейса: Метод шифрования нового поколения (CNG) уже доступен. Дополнительные сведения о шифровании CNG см. в разделе Описание CNG.
Windows PowerShell 2.0	Эта ранняя версия Windows PowerShell заменена несколькими более поздними версиями. Для обеспечения наилучших возможностей и производительности перейдите на Windows PowerShell 5.0 или более позднюю версию. Подробные сведения см. в разделе Документация по PowerShell.

Признак	Объяснение
Технологии туннелирования IPv4/6 (6to4, ISATAP и прямое туннелирование)	Функция 6to4 отключена по умолчанию начиная с Windows 10 версии 1607 (юбилейное обновление), ISATAP отключена по умолчанию начиная с Windows 10 версии 1703 (Creators Update), а прямое туннелирование всегда было отключено по умолчанию. Вместо этого используйте встроенную поддержку IPv6.
Службы MultiPoint	Мы больше не разрабатываем роль служб MultiPoint в составе Windows Server. Службы соединителя MultiPoint доступны в функции Компонент по требованию для Windows Server и Windows 10. Можно использовать Службы удаленных рабочих столов, в частности, Узел сеансов служб удаленных рабочих столов для обеспечения связи RDP.
Автономные пакеты символов (MSI-файлы символов для отладки)	Мы больше не предлагаем пакеты символов в виде загружаемых MSI-файлов. Вместо этого сервер символов (Майкрософт) станет хранилищем символов на основе Azure. Если вам требуются символы Windows, подключитесь к серверу символов (Майкрософт), чтобы закэшировать символы в локальном режиме, или используйте файл манифеста с SymChk.exe на компьютере с доступом в Интернет.
Политика программных ограничений в групповой политике	Вместо использования политик ограниченного использования программного обеспечения через групповая политика можно использовать AppLocker или Защитник Windows управление приложениями. Вы можете использовать AppLocker и Защитник Windows Управление приложениями, чтобы управлять приложениями, к которым пользователи могут получать доступ и какой код может выполняться в ядре.
Дисковые пространства в общей конфигурации с использованием структуры SAS	Вместо этого разворачивайте локальные дисковые пространства. Локальные дисковые пространства поддерживают использование сертифицированных HLK корпусов SAS, но в конфигурации без общего доступа, как описано в требованиях к оборудованию локальных дисковых пространств.
Режим Windows Server Essentials	Мы больше не разрабатываем роль режима Essentials для Windows Server Standard и SKU Windows Server Datacenter. Если вам требуется простое серверное решение для предприятий малого и среднего бизнеса, проверьте наше новое решение Microsoft 365 для бизнеса или используйте Windows Server 2016 Essentials.

Компоненты, удаленные или не рекомендуемые к использованию в Windows Server 2016

Статья • 28.01.2023 • Чтение занимает 2 мин

В каждом выпуске Windows Server добавляются новые компоненты и возможности. Иногда мы также удаляем компоненты и функциональные возможности. Как правило, это происходит, когда мы добавляем улучшенную функцию. Ниже приведены подробные сведения о компонентах и возможностях, которые были удалены в Windows Server 2016.

> **Совет**
>
> - Ранний доступ к сборкам Windows Server можно получить, вступив в **Программу предварительной оценки Windows для бизнеса**, — это отличный способ для проверки изменений в функциональных возможностях.

Этот список не является исчерпывающим и может быть изменен.

Компоненты, которые мы удалили в этом выпуске

Мы удаляем следующие компоненты и функциональные возможности из установленного образа продукта в Windows Server 2016. Приложения или код, которые зависят от этих компонентов, не будут работать в этом выпуске, если вы не используете какой-либо альтернативный метод.

> **Примечание**
>
> При переходе на Windows Server 2016 с более раннего выпуска, чем Windows Server 2012 R2 или Windows Server 2012, рекомендуется также ознакомиться со статьями **Компоненты, удаленные или не рекомендуемые к использованию в Windows Server 2012 R2** и **Компоненты, удаленные или не рекомендуемые к использованию в Windows Server 2012**.

Признак	Объяснение
Оснастка "Управление общими ресурсами и хранилищами" для консоли управления	Если на компьютере, которым вы хотите управлять, запущена более ранняя ОС, чем Windows Server 2016, подключитесь к нему с помощью удаленного рабочего стола и используйте локальную версию оснастки "Управление общими ресурсами и хранилищами". На компьютере под управлением Windows 8.1 или более ранней версии используйте оснастку "Управление общими ресурсами и хранилищами" из средства удаленного администрирования сервера для просмотра компьютера, которым вы хотите управлять. Используйте Hyper-V на клиентском компьютере, чтобы запустить виртуальную машину под управлением Windows 7, Windows 8 или Windows 8.1 с оснасткой "Управление общими ресурсами и хранилищами" в средстве удаленного администрирования сервера.
Journal.dll	Файл `Journal.dll` был удален из Windows Server 2016. Замены нет.
Мастер настройки безопасности	Мастер настройки безопасности удален. Вместо этого функции являются защищенными по умолчанию. Если вам необходимо управлять определенными параметрами безопасности, можно использовать групповую политику или Microsoft Security Compliance Manager.
SQM	Были удалены компоненты участия, управляющие участием в программе улучшения качества ПО.

Центр обновления Windows	Команда **wuauclt.exe /detectnow** была удалена и больше не поддерживается. Чтобы запустить сканирование обновлений, выполните следующие команды PowerShell:
	
	`$AutoUpdates = New-Object -ComObject "Microsoft.Update.AutoUpdate"`
	`$AutoUpdates.DetectNow()`

Компоненты, которые мы больше не разрабатываем

Мы прекращаем активную разработку этих компонентов и, возможно, удалим их из будущих обновлений. Некоторые компоненты заменены на другие компоненты или функции, в то время как другие компоненты теперь доступны в иных источниках.

Признак	Объяснение
Средства настройки	Параметр `scregedit.exe` использовать не рекомендуется. Если у вас есть сценарии, зависящие от scregedit.exe, измените их для использования методов reg.exe или PowerShell.
Sconfig.exe	Вместо этого используйте Sconfig.cmd.

Признак	Объяснение
Настраиваемые API-интерфейсы NetCfg	Установка PrintProvider, NetClient и ISDN с помощью настраиваемых API-интерфейсов NetCfg не рекомендуется.
Удаленное управление	WinRM.vbs не рекомендуется к использованию. Вместо этого используйте функции в поставщике WinRM PowerShell.
SMB 2+ через NetBT	SMB 2+ через NetBT не рекомендуется к использованию. Вместо этого внедрите SMB через TCP или RDMA.

Информация о выпуске Windows Server

Статья • 28.01.2023 • Чтение занимает 2 мин

Windows Server переходит на этап Long-Term Servicing Channel (LTSC), наш основной канал выпуска. Поддержка Windows Server Semi-Annual Channel (SAC) прекращена 9 августа 2022 года. Дальнейшие выпуски SAC для Windows Server не планируются.

Помимо работы с инновациями в контейнерах и микрослужбах, ранее выпущенных в Semi-Annual Channel, мы также продолжим реализовывать улучшения для Службы Azure Kubernetes (AKS), AKS в Azure Stack HCI и другие улучшения платформы, выполненные в сотрудничестве с сообществом Kubernetes. Новая основная версия Windows Server будет по-прежнему выходить каждые 2–3 года. Поэтому вы можете рассчитывать, что частота выпусков узлов и образов контейнера будет соответствовать этой тенденции.

Центр работоспособности выпуска Windows постоянно развивается. **Примите участие в нашем коротком опросе** и сообщите нам, что мы можем улучшить.

Текущие версии Windows Server по варианту обслуживания

(Все даты указаны в формате ISO 8601: ГГГГ-ММ-ДД)

Выпуск Windows Server	Тип обслуживания	Выпуски	Доступность	Создание	Дата окончания основной фазы поддержки	Дата окончания дополнительной фазы поддержки
Windows Server 2022	Long-Term Servicing Channel (LTSC)	Datacenter, Standard	18.08.2021	20348.169	2026-10-13	2031-10-14
Windows Server 2019 (версия 1809)	Long-Term Servicing Channel (LTSC)	Datacenter, Essentials, Standard	2018-11-13	17763.107	2024-01-09	2029-01-09
Windows Server 2016 (версия 1607)	Long-Term Servicing Channel (LTSC)	Datacenter, Essentials, Standard	2016-10-15	14393.0	Окончание обслуживания	2027-01-11

Примечание

Windows Server управляется **современной политикой жизненного цикла** или **фиксированной политикой жизненного цикла** в зависимости от версии или выпуска. Подробные сведения о требованиях к обслуживанию и другую важную информацию см. в статье **с вопросами и ответами о жизненном цикле продуктов Windows** и статье **со сравнением каналов обслуживания**. Дополнительные сведения о том, какие версии Windows Server применяются к современной политике жизненного цикла, см. в статье **Выпуски Windows Server**.

Общие сведения о дополнительных обновлениях для системы безопасности Windows Server

Статья • 17.01.2023 • Чтение занимает 4 мин

Программа "Дополнительные обновления для системы безопасности" (ESU) — это крайняя мера для клиентов, которым необходимо использовать определенные устаревшие продукты Microsoft после окончания срока поддержки. По каналу Windows Server Long Term Servicing Channel (LTSC) предусмотрено не менее десяти лет поддержки — пять лет для основной поддержки и пять лет для расширенной поддержки, в которую входят регулярные обновления системы безопасности.

Однако прекращение поддержки продуктов также означает прекращение выхода обновлений для системы безопасности и бюллетеней. Этот сценарий может вызвать проблемы с безопасностью или соответствием и подвергнуть бизнес-приложения риску. Корпорация Майкрософт для обеспечения максимальной безопасности, производительности и инноваций рекомендует обновить Windows Server до текущей версии.

> **Совет**
>
> Сведения о сроках поддержки можно найти на странице о **жизненном цикле Майкрософт**.

Ниже приведены версии Windows Server, которые уже достигли или скоро достигнут окончания расширенной поддержки:

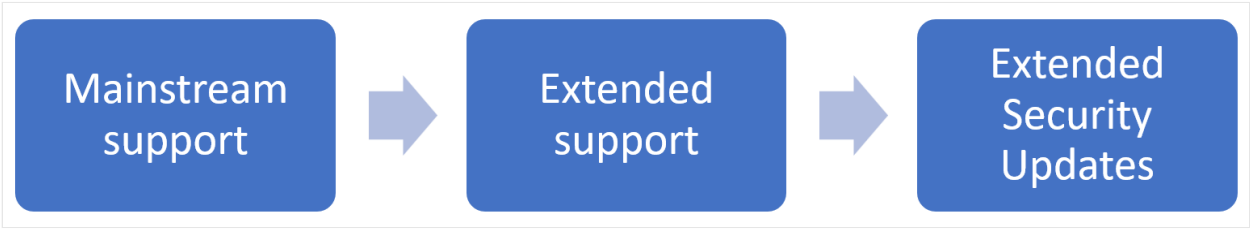
- Расширенная поддержка для Windows Server 2008 и Windows Server 2008 R2 прекращена 14 января 2020 г.
- Расширенная поддержка для Windows Server 2012 и Windows Server 2012 R2 будет прекращена 10 октября 2023 г.

Что такое дополнительные обновления системы безопасности?

Дополнительные обновления для системы безопасности Windows Server содержат обновления для системы безопасности и бюллетени с оценкой *критические* и *важные* в течение максимального периода времени с даты окончания

предоставления расширенной поддержки в зависимости от версии (см. ниже). Они предоставляются бесплатно для серверов, размещенных в Azure, а также доступны для покупки для серверов, не размещенных в Azure. Дополнительные обновления для системы безопасности не содержат новые возможности, запрошенные клиентом исправления, не относящиеся к системе безопасности, а также запросы на изменение архитектуры. Дополнительные сведения см. в статье Часто задаваемые вопросы о жизненном цикле — расширенные обновления безопасности.

При использовании расширенной Обновления безопасности для этих версий Windows Server выполняются следующие этапы.



Если вы еще не обновили серверы, следующие параметры помогут защитить приложения и данные во время перехода:

- **Перенос затронутых существующих рабочих нагрузок Windows Server на виртуальные машины Azure в исходном состоянии**. Этот тип миграции в Azure автоматически предоставляет дополнительные обновления для системы безопасности на указанный период. Дополнительная плата за дополнительные обновления для системы безопасности вдобавок к стоимости виртуальной машины Azure не взимается, а дополнительная настройка не требуется.
- **Приобретение подписки на дополнительные обновления для системы безопасности для своих серверов и сохранение средств защиты, пока не будете готовы к обновлению до новой версии Windows Server**. Такие обновления предоставляются на определенный период. После приобретения подписки вам понадобится получить ключ продукта и установить его на каждом соответствующем сервере. Дополнительные сведения см. в статье Сведения о том, как получить дополнительные обновления для системы безопасности.

Период предоставления дополнительных обновлений для системы безопасности зависит от версии Windows Server и от расположения размещения:

Версия продукта	Размещенные*	Длительность ESU	Дата окончания ESU

Версия продукта	Размещенные*	Длительность ESU	Дата окончания ESU
Windows Server 2008 Windows Server 2008 R2	Azure*	Четыре года	9 января 2024 г.
Windows Server 2008 Windows Server 2008 R2	Вне Azure	Три года	10 января 2023 г.
Windows Server 2012 Windows Server 2012 R2	Azure*	Три года	13 октября 2026 г.
Windows Server 2012 Windows Server 2012 R2	Вне Azure	Три года	13 октября 2026 г.

* Содержит портфель продуктов Azure Stack, расширяющий возможности и доступные услуги для выбранного окружения.

> ⚠ **Предупреждение**
>
> По истечении периода предоставления дополнительных обновлений для системы безопасности обновления не будут выпускаться. Рекомендуется поскорее обновить Windows Server до более новой версии.

Перенос в Azure

Вы можете перенести в Azure локальные серверы, которые работают, используя версию Windows Server, для которой завершен или будет завершен период предоставления расширенной поддержки, и впредь запускать их как виртуальные машины. В Azure вы обеспечите соответствие нормативным требованиям, повысите уровень защиты и сможете использовать в своей работе преимущества облачных технологий. Преимущества переноса в Azure:

- Обновления системы безопасности в Azure.
- Получайте важные обновления системы безопасности для Windows Server на определенный срок без дополнительной платы.
- Бесплатные обновления в Azure.
- Внедрение дополнительных облачных служб по мере готовности.
- При переносе SQL Server на виртуальные машины Azure в течение трех дополнительных лет вы будете получать важные обновления для системы безопасности для Windows Server без дополнительной платы. Вы также можете обновить SQL Server до Управляемого экземпляра Azure SQL.
- Только в Azure вы сможете использовать имеющиеся лицензии на SQL Server и Windows Server для экономии на облачных ресурсах благодаря

Преимуществу гибридного использования Azure.

Чтобы приступить к миграции, ознакомьтесь со сведениями о загрузке универсального виртуального жесткого диска и использовании его для создания новых виртуальных машин в Azure или воспользуйтесь общими коллекциями образов в Azure.

Сведения о том, как анализировать имеющиеся ИТ-ресурсы, оценить то, что у вас уже есть, определить преимущества переноса конкретных служб и приложений в облако по сравнению с сохранением рабочих нагрузок в локальной среде, а также понять, какую выгоду вы получите от обновления до последней версии Windows Server, см. в руководстве по переносу для Windows Server.

Миграция или обновление в локальной среде

Если вам необходимо поддерживать работоспособность локальных серверов, нужно либо создать новые серверы с поддерживаемой версией Windows Server, либо перенести приложения и данные, либо выполнить обновление на месте до поддерживаемой версии Windows Server. При обновлении Windows Server обычно можно пропустить одну, а иногда даже две версии. Например, Windows Server 2012 R2 можно обновить на месте до Windows Server 2019. Однако для Windows Server 2008 или Windows Server 2008 R2 не предусмотрен прямой путь обновления до Windows Server 2016 или более поздней версии. Вместо этого сначала обновите их до Windows Server 2012 R2, а затем — до Windows Server 2016 или Windows Server 2019. В ходе обновления у вас останется возможность выполнить перенос в Azure, как описано ниже. Подробные сведения о вариантах локального обновления см. в статье о поддерживаемых путях обновления для Windows Server.

Обновление SQL Server параллельно с серверами Windows Server

Если вы используете версию SQL Server, для которой завершен или будет завершен период предоставления расширенной поддержки, можно также воспользоваться преимуществами дополнительных обновлений для системы безопасности для SQL Server. Дополнительные сведения см. на странице, посвященной теме дополнительных обновлений для системы безопасности для SQL Server и Windows Server.

Дальнейшие действия

- Узнайте больше о том, как получить дополнительные обновления для системы безопасности (ESU) для Windows Server

Общие сведения об обновлениях Windows Server

Статья • 29.09.2022 • Чтение занимает 2 мин

Процесс обновления до новой версии Windows Server может отличаться в зависимости от используемой операционной системы и выбранного пути. Чтобы определить действия, выполняемые в новом развертывании Windows Server, мы будем использовать следующие термины.

- **Обновление.** Также именуется "обновление на месте". Вы переходите с более старой версии операционной системы на более новую, сохраняя неизменным физическое оборудование. **Именно этот метод мы рассмотрим в этой статье**.

  > **ⓘ Важно!**
  >
  > Обновления на месте можно дополнить поддержкой общедоступного или частного облачного поставщика, но соответствующие возможности и процедуры нужно уточнять отдельно у каждого из них. Кроме того, вы не сможете выполнить обновление на месте для Windows Server, если настроена **загрузка с VHD**. Обновление на месте с выпусков Windows Storage Server не поддерживается. Вместо этого можно выполнить **миграцию** или **установку**.

- **Установка.** Также именуется "чистая установка". Вы переходите с более старой версии операционной системы на более новую, полностью удалив старую установку.

- **Миграция.** Вы переходите с более старой версии операционной системы на более новую путем ее переноса на другой набор оборудования или другую виртуальную машину.

- **Последовательное обновление операционной системы кластера.** Вы обновляете ОС узлов кластера, не останавливая рабочие нагрузки Hyper-V и (или) масштабируемого файлового сервера. Эта функция позволяет избежать простоя, который может нарушать соглашения об уровне обслуживания. Дополнительные сведения см. в статье Последовательное обновление ОС кластера.

- **Преобразование лицензии.** Вы преобразуете определенный выпуск версии в другой выпуск той же версии за один шаг, выполнив простую команду и предоставив соответствующий лицензионный ключ. Это называется

преобразованием лицензии. Например, если ваш сервер работает под управлением выпуска Standard, вы можете преобразовать его в Datacenter.

До какой версии Windows Server лучше всего обновляться?

Мы рекомендуем всегда обновлять ОС до последней версии Windows Server. Использование последней версии Windows Server предоставит вам все современные функции, в том числе повышающие безопасность и производительность.

> **Совет**
>
> Вы можете одновременно обновить до двух версий до более новой версии Windows Server. Например, Windows Server 2016 можно обновить до Windows Server 2019 или Windows Server 2022. Если вы применяете **функцию последовательного обновления ОС кластера**, вы можете использовать только одну версию за раз.

В этой таблице приведены поддерживаемые пути обновления на основе текущей версии.

Обновление с / до	**Windows Server 2008 R2**	**Windows Server 2012**	**Windows Server 2012 R2**	**Windows Server 2016**	**Windows Server 2019**	**Windows Server 2022**
Windows Server 2008	Да	Да	-	-	-	-
Windows Server 2008 R2	-	Да	Да	-	-	-
Windows Server 2012	-	-	Да	Да	-	-
Windows Server 2012 R2	-	-	-	Да	Да	-
Windows Server 2016	-	-	-	-	Да	Да
Windows Server 2019	-	-	-	-	-	Да

Вы также можете провести обновление с ознакомительной версии операционной системы на розничную, с более старой розничной версии на более новую или, в некоторых случаях, с корпоративного выпуска ОС на обычный. Дополнительные сведения о поддерживаемых способах, отличных от обновления на месте, см. в этой статье.

> ⓘ **Примечание**
>
> Поддержка для **Windows Server 2008** и **Windows Server 2008 R2** прекращена. Рекомендуется поскорее обновить Windows Server до более новой версии. Узнайте больше о **дополнительных обновлениях для системы безопасности (ESU)**, которые следует использовать только в крайних случаях.

Дальнейшие действия

Теперь, когда все готово к обновлению Windows Server, ознакомьтесь со следующими статьями, которые могут помочь вам приступить к работе:

- Установка, обновление или миграция в Windows Server
- Обновление и миграция ролей и компонентов в Windows Server
- Параметры обновления и преобразования для Windows Server
- Обновление Windows Server на месте

Установка, обновление или миграция в Windows Server

Статья • 28.01.2023 • Чтение занимает 2 мин

Пришло время перейти на более новую версию Windows Server? В зависимости от того, какая операционная система сейчас установлена на вашем компьютере, у вас есть несколько вариантов.

> **ⓘ Важно!**
>
> Расширенная поддержка Windows Server 2008 R2 и Windows Server 2008 закончилась в январе 2020 года. Доступны дополнительные обновления для системы безопасности (ESU) с одним вариантом миграции локальных серверов в Azure, где вы можете по-прежнему запускать их на виртуальных машинах. Дополнительные сведения см. на странице **обзора дополнительных обновлений для системы безопасности**.

> **Совет**
>
> Чтобы скачать Windows Server 2022, см. статью **Ознакомительные версии Windows Server**.

Чистая установка

Чистая установка — это самый простой способ установки Windows Server, при использовании которого выполняется установка на пустом сервере или перезаписывается существующая операционная система. Но для этого сначала нужно создать резервную копию данных и запланировать переустановку приложений. Существует несколько факторов, которые следует учитывать, например требования к оборудованию. Поэтому обязательно проверьте данные по Windows Server.

Обновление «на месте»

Обновление на месте позволяет использовать то же оборудование и сохранить все роли сервера, которые вы настроили, без очистки и переустановки операционной системы. При этом вы переходите со старой операционной системы на более

новую, а параметры, роли и функции сервера, остаются без изменений. Например, если ваш сервер работает под управлением Windows Server 2019, вы можете обновить его до Windows Server 2022. Но не со всех более ранних версий операционных систем можно перейти на более новую версию. Некоторые роли или компоненты не поддерживают эту возможность или требуют выполнения дополнительных действий. Обновление на месте лучше всего работает на виртуальных машинах, где для успешного обновления не нужны специальные драйверы оборудования OEM.

Пошаговые инструкции и дополнительные сведения об обновлении см. в статье Общие сведения об обновлениях Windows Server и Обновление и перенос ролей и функций в Windows Server.

Последовательное обновление ОС кластера

Последовательное обновление ОС кластера дает администратору возможность обновлять ОС узлов кластера, не останавливая рабочие нагрузки Hyper-V или масштабируемого файлового сервера. Например, если узлы в вашем кластере работают под управлением Windows Server 2019, вы можете установить на них Windows Server 2022, чтобы избежать простоев в работе кластера, которые в противном случае повлияли бы на соглашения об уровнях обслуживания. Подробнее эта функция рассматривается в статье Последовательное обновление ОС кластера.

Миграция

С помощью миграции Windows Server вы можете переместить одну роль или компонент за раз с исходного компьютера, работающего под управлением Windows Server, на другой целевой компьютер, работающий под управлением Windows Server такой же или более новой версии. Для этих целей миграция определяется как перемещение одной роли или компонента и его данных на другой компьютер без обновления компонентов на том же компьютере.

Преобразование лицензии

Для некоторых выпусков Windows Server преобразование лицензии позволяет перейти с определенного выпуска версии на другой выпуск той же версии в один этап с помощью простой команды и соответствующего лицензионного ключа. Например, если ваш сервер работает под управлением Windows Server 2022 Standard, вы можете преобразовать его в Windows Server 2022 Datacenter.

Учитывайте, что вы можете перейти с плана Windows Server 2022 Standard на Windows Server 2022 Datacenter, но не сможете перейти обратно с выпуска Datacenter на выпуск Standard. Кроме того, в некоторых выпусках Windows Server можно свободно выбирать между переходом на версию OEM, версию с корпоративным лицензированием и розничную версию с помощью той же команды и соответствующего ключа.

Сравнение вариантов установки "Основные серверные компоненты" и "Сервер с возможностями рабочего стола"

Статья • 29.09.2022 • Чтение занимает 2 мин

При установке Windows Server с помощью мастера установки можно выбрать один из вариантов: "Основные серверные компоненты" или "Сервер с возможностями рабочего стола". При использовании варианта "Основные серверные компоненты" стандартный графический пользовательский интерфейс (возможности рабочего стола) не устанавливается. Управление сервером осуществляется из командной строки, из средства настройки сервера (SConfig) или с помощью PowerShell. При использовании варианта "Сервер с возможностями рабочего стола" устанавливается стандартный графический пользовательский интерфейс и все средства, в том числе функции взаимодействия с клиентами.

Рекомендуем выбрать вариант установки "Основные серверные компоненты", если нет особой необходимости в дополнительных элементах пользовательского интерфейса и графических средствах управления, входящих в вариант "Сервер с возможностями рабочего стола".

Мастер установки выводит список параметров установки, показанный ниже. В этом списке выпуски без **возможностей рабочего стола** являются вариантами установки "Основные серверные компоненты":

- Windows Server Standard
- Windows Server Standard с возможностями рабочего стола;
- Windows Server Datacenter;
- Windows Server Datacenter с возможностями рабочего стола.

> ⓘ **Примечание**
>
> В отличие от предыдущих выпусков Windows Server, после установки преобразовать основные серверные компоненты в сервер с возможностями рабочего стола (и наоборот) невозможно. Если вы решите выбрать другой вариант, в дальнейшем нужно будет выполнить **чистую установку**.

Различия

Есть ряд основных различий между вариантами "Основные серверные компоненты" и "Сервер с возможностями рабочего стола":

Компонент	Основные серверные компоненты	Сервер с возможностями рабочего стола
Пользовательский интерфейс	Минимальный, управление с помощью командной строки (PowerShell, SConfig, cmd)	Стандартный графический пользовательский интерфейс Windows
Пространство на диске	Меньше требований	Больше требований
Установка, настройка и удаление ролей сервера в локальной среде	PowerShell	Диспетчер сервера или PowerShell
Роли и компоненты	Некоторые роли и функции недоступны. Дополнительные сведения см. в статье Роли, службы ролей и компоненты, не включенные в основные серверные компоненты Windows Server. Некоторые из функций варианта "Сервер с возможностями рабочего стола" для обеспечения совместимости приложений можно установить с помощью функции совместимости приложений по запросу (FOD).	Доступны все роли и функции, в том числе предназначенные для обеспечения совместимости приложений.
Удаленное управление	Да, решением можно управлять удаленно с помощью средств GUI, таких как Windows Admin Center, средства удаленного администрирования сервера (RSAT), диспетчер сервера или PowerShell.	Да, решением можно управлять удаленно с помощью средств GUI, таких как Windows Admin Center, средства удаленного администрирования сервера (RSAT), диспетчер сервера или PowerShell.
Потенциальные направления атак	Существенное сокращение направлений атак	Без сокращения

Компонент	Основные серверные компоненты	Сервер с возможностями рабочего стола
Microsoft Management Console (MMC)	Не установлено. Можно установить с функцией обеспечения совместимости приложений по запросу (FOD).	Установлено

> **Примечание**
>
> Для RSAT необходимо использовать версию, входящую в состав Windows 10 или более поздней версии.

Обновление и миграция ролей и компонентов в Windows Server

Статья • 29.09.2022 • Чтение занимает 4 мин

Вы можете обновить роли и компоненты до последних версий Windows Server, выполнив миграцию на новый сервер. Многие роли и компоненты также поддерживают обновление на месте, когда вы устанавливаете новую версию Windows Server поверх текущей. Эта статья содержит ссылки на руководства по миграции, а также таблицу со сведениями о миграции и обновлении на месте, которые помогут выбрать нужный метод.

Вы можете перенести разные роли и компоненты с помощью средств миграции Windows Server (встроенная в Windows Server функция для переноса ролей и компонентов). А файловые серверы и хранилища можно перенести с помощью Службы миграции хранилища.

Руководства по миграции охватывают перенос определенных ролей и компонентов с одного сервера на другой (не обновление на месте). Если в руководствах не указано иное, поддерживается перенос между физическими и виртуальными компьютерами, а также между установками Windows Server с возможностями рабочего стола или основными серверными компонентами.

> **ⓘ Важно!**
>
> Перед началом переноса ролей и компонентов убедитесь, что исходный и целевой серверы работают под управлением операционных систем с последними доступными для них пакетами обновления.
>
> При миграции или обновлении до любой версии Windows Server следует изучить **политику сроков поддержки** и период времени для этой версии и плана соответственно. Вы можете **найти информацию о сроках** для определенного выпуска Windows Server, который вас интересуют.

Средства миграции Windows Server

Средства миграции Windows Server позволяют вам переносить роли сервера, компоненты, настройки операционной системы и другие данные и общие папки на серверы, в том числе последние версии Windows Server. Это функция Windows Server, поэтому ее можно легко установить с помощью мастера добавления ролей

и компонентов или PowerShell. Дополнительные сведения об установке, использовании и удалении средств миграции Windows Server см. здесь.

> ⓘ **Примечание**
>
> Миграция между подсетями с помощью средств миграции Windows Server доступна в Windows Server 2012 и более поздних выпусках. Предыдущие версии средств миграции Windows Server поддерживают только миграцию в одной подсети.

Руководства по переносу

Ниже можно найти ссылки на руководства по миграции для конкретных ролей и компонентов Windows.

Active Directory

- Руководство по переносу служб сертификатов Active Directory для Windows Server 2012 R2
- Руководство по переносу служб сертификатов Active Directory для Windows Server 2008 R2
- Перенос служб ролей для служб федерации Active Directory в Windows Server 2012 R2
- Перенос служб ролей для служб федерации Active Directory в Windows Server 2012
- Руководство по обновлению и переносу служб управления правами Active Directory
- Обновление контроллеров домена до Windows Server 2012 R2 и Windows Server 2012
- Руководство по переносу служб домена Active Directory и DNS-сервера для Windows Server 2008 R2

BranchCache

- Руководство по переносу BranchCache

DHCP

- Перенос DHCP-сервера в Windows Server 2012 R2

- Руководство по переносу DHCP-сервера для Windows Server 2008 R2

Отказоустойчивая кластеризация

- Перенос кластерных ролей в Windows Server 2012 R2
- Перенос кластеризованных служб и приложений на Windows Server 2012

Файловые службы и службы хранилища

- Служба миграции хранилища
- Перенос файловых служб и служб хранилища в Windows Server 2012 R2

Hyper-V

- Перенос Hyper-V в Windows Server 2012 R2 с Windows Server 2012
- Перенос Hyper-V на Windows Server 2012 с Windows Server 2008 R2

Сервер политики сети

- Перенос сервера политики сети в Windows Server 2012
- Перенос центра регистрации работоспособности в Windows Server 2012

Службы печати и документов

- Перенос служб печати и документов в Windows Server 2012

Удаленный доступ

- Перенос удаленного доступа в Windows Server 2012

Службы удаленных рабочих столов

- Перенос служб удаленных рабочих столов
- Перенос служб удаленных рабочих столов в Windows Server 2012 R2
- Перенос служб MultiPoint

Маршрутизация и удаленный доступ

- Руководство по переносу RRAS

Веб-сервер (IIS)

- Веб-сервер (IIS)

Службы Windows Server Update Services

- Перенос служб обновления Windows Server Update Services в Windows Server 2012 R2

Другие руководства по миграции в Windows

- Руководство по переносу группы и локальных пользователей
- Руководство по переносу IP-конфигурации

Таблица по обновлению и миграции

Роль сервера	Обновляется на месте?	Поддерживается ли миграция?	Можно ли выполнить миграцию без простоя?
Службы сертификатов Active Directory	Да	Да	Нет
Доменные службы Active Directory	Да	Да	Да
Службы федерации Active Directory (AD FS)	Нет	Да	Нет (в ферму нужно добавить новые узлы)
Службы Active Directory облегченного доступа к каталогам (AD LDS)	Да	Да	Да
Службы управления правами Active Directory (AD RMS)	Да	Да	Нет

Роль сервера	Обновляется на месте?	Поддерживается ли миграция?	Можно ли выполнить миграцию без простоя?
DHCP-сервер	Да	Да	Да
DNS-сервер	Да	Да	нет
Отказоустойчивая кластеризация	Да, с помощью процесса последовательного обновления ОС кластера (Windows Server 2012 R2 и более поздних версий) или при удалении сервера в ходе обновления кластера и его последующего добавления на другой кластер.	Да	Да, для Отказоустойчивых кластеров с виртуальными машинами Hyper-V или Отказоустойчивых кластеров с ролью горизонтально масштабируемого файлового сервера. См. сведения о последовательном обновлении ОС кластера (Windows Server 2012 R2 и более поздних версий).
Файловые службы и службы хранилища	Да	Зависит от подкомпонента	Нет
Hyper-V	Да, с помощью процесса последовательного обновления ОС кластера (Windows Server 2012 R2 и более поздних версий).	Да	Да, для Отказоустойчивых кластеров с виртуальными машинами Hyper-V или Отказоустойчивых кластеров с ролью горизонтально масштабируемого файлового сервера. См. сведения о последовательном обновлении ОС кластера (Windows Server 2012 R2 и более поздних версий).

Роль сервера	Обновляется на месте?	Поддерживается ли миграция?	Можно ли выполнить миграцию без простоя?
Службы печати и факсов	Нет	Да (с помощью Printbrm.exe)	Нет
Службы удаленных рабочих столов	Да, для всех подчиненных ролей, но ферма в смешанном режиме не поддерживается	Да	Нет
Веб-сервер (IIS)	Да	Да	Нет
Режим Windows Server Essentials	Да	Да	Нет
Службы Windows Server Update Services	Да	Да	Нет
рабочие папки	Да	Да	Да, с помощью процесса последовательного обновления ОС кластера (Windows Server 2012 R2 и более поздних версий).

Параметры обновления и преобразования для Windows Server

Статья • 28.01.2023 • Чтение занимает 5 мин

Вы можете обновить или преобразовать установки Windows Server в более новые версии, различные выпуски или переключаться между вариантами лицензирования, такими как ознакомительная, розничная и корпоративная лицензия. В этой статье объясняется, какие возможности могут помочь при планировании.

Процесс обновления или преобразования установок Windows Server может сильно различаться в зависимости от того, какая версия и выпуск установлены, как они лицензированы, а также от выбранного вами пути. Мы используем разные термины для различения действий, любое из которых может использоваться при развертывании Windows Server: чистая установка, обновление на месте, последовательное обновление кластерной операционной системы (ОС), миграция и преобразование лицензий. Дополнительные сведения об этих терминах см. в статье Установка, обновление или миграция.

Обновление лицензированных версий Windows Server

Ниже приведены общие рекомендации для путей обновления на месте, где Windows Server **уже лицензирован** (то есть не является ознакомительной версией):

- Обновления с 32-разрядных до 64-разрядных архитектур не поддерживаются. Все выпуски Windows Server, начиная с Windows Server 2008 R2, являются только 64-разрядными.
- Обновления с версии на одном языке до версии на другом языке не поддерживаются.
- Если сервер является контроллером домена Active Directory, вы не можете преобразовать его в розничную версию. Дополнительные сведения см. в статье Обновление контроллеров домена до Windows Server 2012 R2 и Windows Server 2012.
- Обновления с предварительных версий Windows Server не поддерживаются. Выполните чистую установку Windows Server.
- Обновления, выполняющие переключение с установки основных серверных компонентов на установку Server с возможностями рабочего стола (или наоборот), не поддерживаются.

- Обновления предыдущей установки Windows Server на пробную версию Windows Server не поддерживаются. Для ознакомительных версий следует применять чистую установку.
- При обновлении можно изменить только выпуск Standard на выпуск Datacenter. Переход с выпуска Datacenter на выпуск Standard не поддерживается.

> **ⓘ Важно!**
>
> Если сервер использует объединение сетевых карт, отключите эту функцию перед обновлением, а после его завершения снова включите ее. Дополнительные сведения см. в статье **Обзор объединения сетевых карт**.

Преобразование ознакомительной версии в розничную версию

Вы можете перейти с ознакомительной версии Windows Server на розничную. Если вы установили ознакомительную версию выпуска Standard, вы можете преобразовать ее в розничную версию выпуска Standard или Datacenter. Аналогичным образом, если вы установили ознакомительную версию выпуска Datacenter, ее можно преобразовать только в розничную версию выпуска Datacenter.

Если вы еще не активировали Windows, в правом нижнем углу рабочего стола отображается время, оставшееся для ознакомительного периода.

> **ⓘ Важно!**
>
> Для выпусков Windows Server 2016, предшествующих 14393.0.161119-1705.RS1_REFRESH, преобразование ознакомительной версии в розничную можно выполнить только для системы Windows Server с вариантом установки "Возможности рабочего стола" (а не установки основных серверных компонентов). Начиная с выпуска 14393.0.161119-1705.RS1_REFRESH, можно преобразовывать ознакомительные выпуски в коммерческие независимо от варианта установки.

> **ⓘ Примечание**

Перед переходом с ознакомительной на розничную версию убедитесь, что на вашем сервере действительно работает ознакомительная версия. В командной строке с повышенными привилегиями введите команду `slmgr.vbs /dlv`. В ознакомительных версиях вывод будет включать строку **EVAL**.

Windows Server Standard или Datacenter

Если на сервере установлена ознакомительная версия Windows Server Standard или Windows Server Datacenter, вы можете преобразовать ее в розничную версию следующим образом:

1. В командной строке с повышенными привилегиями или в сеансе PowerShell выполните следующую команду, чтобы сохранить условия лицензионного соглашения на использование программного обеспечения корпорации Майкрософт для Windows Server, которые затем можно изучить:

   ```
   DISM /online /Set-Edition:ServerDatacenter /GetEula:C:\eula.rtf
   ```

2. Определите имя текущего выпуска, выполнив приведенную ниже команду. Выходные данные представляют собой сокращенную форму имени выпуска, например Windows Server Datacenter Edition — **ServerDatacenter**:

   ```
   DISM /online /Get-CurrentEdition
   ```

3. Проверьте, в какие выпуски можно преобразовать текущую установку, выполнив команду ниже. Ознакомительную версию выпуска Windows Server Standard можно преобразовать в розничную версию выпуска Windows Server или Datacenter, а ознакомительную версию Windows Server Datacenter можно преобразовать только в розничную версию Windows Server Datacenter:

   ```
   DISM /online /Get-TargetEditions
   ```

4. Запишите имя целевого выпуска, в который необходимо преобразовать систему, и введите ее и розничный ключ продукта в приведенной ниже команде. Для этого процесса необходимо принять условия лицензионного

соглашения на использование программного обеспечения корпорации Майкрософт для Windows Server, которые вы ранее сохранили.

> **Совет**
>
> Вы можете преобразовать ознакомительную версию Windows Server Standard в розничную версию Windows Server Datacenter за один шаг, используя соответствующий ключ продукта и идентификатор выпуска.

```
DISM /online /Set-Edition:<edition ID> /ProductKey:XXXXX-XXXXX-XXXXX-XXXXX-XXXXX /AcceptEula
```

Пример:

```
DISM /online /Set-Edition:ServerDatacenter /ProductKey:ABCDE-12345-ABCDE-12345-ABCDE /AcceptEula
```

> **Совет**
>
> Дополнительные сведения о Dism.exe см. в статье **DISM Command-Line Options** (Параметры командной строки DISM).

> **Важно!**
>
> Если сервер является контроллером домена Active Directory, вы не можете преобразовать его в розничную версию. В этом случае установите дополнительный контроллер домена на сервере с установленной розничной версией, перенесете имеющиеся роли FSMO и удалите доменные службы Active Directory (AD DS) с контроллера домена, на котором установлена ознакомительная версия. Дополнительные сведения см. в статье **Обновление контроллеров домена до Windows Server 2012 R2 и Windows Server 2012**.

Windows Server Essentials

Если сервер работает под управлением Windows Server Essentials, можно преобразовать его в полную розничную версию. Для этого нужно запустить

командную строку с повышенными привилегиями и ввести ключ розничной или корпоративной лицензии или ключ изготовителя оборудования в качестве части следующей команды:

```
slmgr.vbs /ipk XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Преобразование выпуска Windows Server Standard в выпуск Datacenter

В любое время после установки Windows Server вы можете преобразовать выпуск Windows Server Standard в выпуск Datacenter. Можно также запустить `setup.exe` с установочного носителя, чтобы обновить или восстановить установку (иногда это называется восстановлением на месте). Если вы запустите `setup.exe`, чтобы обновить или восстановить на месте любой выпуск Windows Server, результатом будет тот же выпуск, с которого вы начали.

Выпуск Windows Server Standard можно преобразовать в выпуск Datacenter следующим образом:

1. Определите, что имя текущего выпуска — Windows Server Standard. Для этого выполните команду ниже. Выходные данные представляют собой сокращенную форму имени выпуска, например Windows Server Standard Edition — **ServerStandard**:

   ```
   DISM /online /Get-CurrentEdition
   ```

2. Убедитесь, что Windows Server Datacenter является допустимым вариантом для преобразования, выполнив следующую команду:

   ```
   DISM /online /Get-TargetEditions
   ```

3. Введите **ServerDatacenter** и ключ розничного продукта в следующей команде:

   ```
   ```

```
DISM /online /Set-Edition:ServerDatacenter /ProductKey:XXXXX-XXXXX-
XXXXX-XXXXX-XXXXX /AcceptEula
```

Преобразование между розничной, корпоративной лицензией и лицензией для изготовителей оборудования

В любое время после установки Windows Server вы можете беспрепятственно перейти на розничную, корпоративную лицензию или лицензию для изготовителей оборудования. Это преобразование не меняет выпуск (Standard или Datacenter). Если вы начинаете с ознакомительной версии, сначала преобразуйте ее в розничную версию, после чего можно выполнить преобразование между версиями.

Для этого выполните следующую команду в командной строке с повышенными привилегиями, включая предоставление ключа продукта корпоративной, розничной лицензии или лицензии изготовителя оборудования:

```
slmgr.vbs /ipk XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Автоматическая активация виртуальной машины в Windows Server

Статья • 28.01.2023 • Чтение занимает 4 мин

Автоматическая активация виртуальной машины (AVMA) — это механизм подтверждения законности приобретения, помогающий удостовериться, что продукты Windows используются в соответствии с правами на использование продуктов и условиями лицензионного соглашения на использование программного обеспечения корпорации Майкрософт.

AVMA позволяет активировать виртуальные машины Windows Server на активированном надлежащим образом узле Hyper-V Windows Server даже в отключенных средах. Она привязывает активацию виртуальной машины к лицензированному узлу виртуализации и активирует виртуальную машину при запуске. Используя AVMA, вы можете получать отчеты по использованию в реальном времени и данные о состоянии лицензии виртуальной машины за прошлые периоды. Отчеты и данные отслеживания доступны на узле виртуализации.

Практическое применение

AVMA на узлах виртуализации включает несколько преимуществ.

Диспетчеры центра обработки данных сервера могут использовать AVMA для выполнения следующих действий:

- Активация виртуальных машин в удаленных расположениях
- Активация виртуальных машин с подключением к Интернету или без него
- Отслеживание данных об использовании и лицензиях виртуальных машин с узла виртуализации без прав доступа к виртуализованным системам

Партнеры с лицензионным соглашением с поставщиком услуг (SPLA) и другие поставщики услуг размещения не обязаны предоставлять ключи продукта арендаторам или активировать виртуальные машины арендаторов. С помощью AVMA клиенты могут легко активировать виртуальные машины. Поставщики услуг размещения могут использовать журналы сервера для проверки соответствия лицензии и отслеживания хронологии использования клиента.

Требования к системе

Узел виртуализации, на котором будут работать виртуальные машины, должен быть активирован. Ключи можно получить в Microsoft Volume Licensing Service Center или у поставщика OEM.

> **Примечание**
>
> В отказоустойчивом кластере необходимо активировать каждый узел виртуализации, чтобы виртуальные машины оставались активными независимо от сервера, на котором они запущены.

Для AVMA требуется выпуск Windows Server Datacenter с установленной ролью узла Hyper-V. Версия операционной системы узла Hyper-V определяет версии операционной системы для активации на виртуальной машине. Ниже представлен список гостей, которых можно активировать с помощью различных версий серверов узла.

Версия сервера узла	**Гостевая виртуальная машина Windows Server 2022**	**Гостевая виртуальная машина Windows Server 2019**	**Гостевая виртуальная машина Windows Server 2016**	**Гостевая виртуальная машина Windows Server 2012 R2**
Windows Server 2022	X	X	X	X
Windows Server 2019		X	X	X
Windows Server 2016			X	X
Windows Server 2012 R2				X

> **Примечание**
>
> В приведенной выше таблице применимы все выпуски (Datacenter, Standard или Essentials).
>
> AVMA не работает с другими технологиями виртуализации серверов.

Реализация AVMA

Чтобы активировать виртуальные машины с помощью AVMA, используйте общий ключ AVMA (см. подробные сведения в разделе Ключи AVMA), соответствующий версии Windows Server, которую необходимо активировать. Чтобы создать виртуальную машину и активировать ее с помощью ключа AVMA, выполните следующие действия:

1. На сервере, на котором будут размещены виртуальные машины, установите и настройте роль сервера Microsoft Hyper-V. Дополнительную информацию см. в статье об установке Hyper-V Server. Убедитесь, что сервер успешно активирован.

2. Создайте виртуальную машину и установите на ней поддерживаемую операционную систему Windows Server.

   > **ⓘ Важно!**
   >
   > Для использования AVMA включите **службу интеграции обмена данными** (также известную как обмен парами "ключ-значение") в настройках виртуальной машины. По умолчанию она включена для новых виртуальных машин.

3. После установки Windows Server на виртуальной машине установите в ней ключ AVMA. В PowerShell или командной строке с повышенными привилегиями введите следующую команду:

   ```
   slmgr /ipk <AVMA_key>
   ```

Виртуальная машина активируется автоматически, если активирован узел виртуализации.

> **Совет**
>
> Вы также можете добавить ключи AVMA в любом **файле автоматической установки**.

Ключи AVMA

Перечисленные ниже ключи AVMA можно использовать для Windows Server 2022.

Выпуск	Ключ AVMA
Центр обработки данных	W3GNR-8DDXR-2TFRP-H8P33-DV9BG
Standard	YDFWN-MJ9JR-3DYRK-FXXRW-78VHK

Перечисленные ниже ключи AVMA можно использовать для Windows Server 2019.

Выпуск	Ключ AVMA
Центр обработки данных	H3RNG-8C32Q-Q8FRX-6TDXV-WMBMW
Standard	TNK62-RXVTB-4P47B-2D623-4GF74
Essentials	2CTP7-NHT64-BP62M-FV6GG-HFV28

Перечисленные ниже ключи AVMA можно использовать для Windows Server версий 1909, 1903 и 1809.

Выпуск	Ключ AVMA
Центр обработки данных	H3RNG-8C32Q-Q8FRX-6TDXV-WMBMW
Standard	TNK62-RXVTB-4P47B-2D623-4GF74

Перечисленные ниже ключи AVMA можно использовать для Windows Server версии 1803 и 1709.

Выпуск	Ключ AVMA
Центр обработки данных	TMJ3Y-NTRTM-FJYXT-T22BY-CWG3J
Standard	C3RCX-M6NRP-6CXC9-TW2F2-4RHYD

Перечисленные ниже ключи AVMA можно использовать для Windows Server 2016.

Выпуск	Ключ AVMA
Центр обработки данных	TMJ3Y-NTRTM-FJYXT-T22BY-CWG3J
Standard	C3RCX-M6NRP-6CXC9-TW2F2-4RHYD
Основные компоненты	B4YNW-62DX9-W8V6M-82649-MHBKQ

Перечисленные ниже ключи AVMA можно использовать для Windows Server 2012 R2.

Выпуск	Ключ AVMA
Центр обработки данных	Y4TGP-NPTV9-HTC2H-7MGQ3-DV4TW
Standard	DBGBW-NPF86-BJVTX-K3WKJ-MTB6V
Основные компоненты	K2XGM-NMBT3-2R6Q8-WF2FK-P36R2

Отчетность и отслеживание

Обмен парами "ключ-значение" (KVP) между узлом виртуализации и виртуальной машиной предоставляет данные отслеживания в реальном времени для операционной системы на виртуальной машине, включая сведения об активации. Эти сведения об активации хранятся в реестре Windows виртуальной машины. Исторические данные о запросах AVMA регистрируются в компоненте "Просмотр событий" на узле виртуализации.

Дополнительные сведения о KVP см. на странице Использование пар "ключ-значение" для совместного использования информации на узле и в гостевой ОС Hyper-V.

> ⓘ **Примечание**
>
> Данные KVP не защищены. Они допускают модификации и не контролируются на предмет изменений.

> ⓘ **Важно!**
>
> Данные KVP следует удалить в случае замены ключа AVMA другим ключом продукта (розничным, OEM или ключом корпоративного лицензирования).

Поскольку процесс активации AVMA прозрачен, сообщения об ошибках не отображаются. Однако запросы AVMA также регистрируются на узле виртуализации в компоненте "Просмотр событий" в журнале приложений с идентификатором события 12310 и на виртуальной машине с идентификатором события 12309. Данные о перечисленных ниже событиях записываются на виртуальных машинах:

Уведомление	Описание

Уведомление	Описание
AVMA успешна	Виртуальная машина активирована.
Недопустимый узел	Узел виртуализации не отвечает. Это может произойти, когда на сервере не установлена поддерживаемая версия Windows.
Недопустимые данные	Это событие обычно возникает в результате сбоя связи между узлом виртуализации и виртуальной машиной, часто из-за повреждения, шифрования или несоответствия данных.
Отказано в активации	Узлу виртуализации не удалось активировать операционную систему на виртуальной машине из-за несоответствия идентификатора AVMA.

Планирование активации на основе службы управления ключами (KMS)

Статья • 21.09.2022 • Чтение занимает 6 мин

При первоначальном планировании активации на основе службы управления ключами (KMS) обратите внимание на следующие аспекты.

KMS использует модель "клиент — сервер" для активных клиентов. Сама служба используется для активации корпоративных лицензий. Для активации клиенты KMS подключаются к серверу KMS, который называется узлом KMS. Узел KMS должен находиться в локальной сети.

Узлы KMS не обязательно должны быть выделенными серверами, и службы KMS могут размещаться на сервере вместе с другими службами. Вы можете запустить узел KMS в любой физической или виртуальной системе, в которой работает поддерживаемая клиентская операционная система Windows Server или Windows. Узел KMS, работающий под управлением операционной системы Windows Server, может активировать компьютеры под управлением как серверной, так и клиентской операционных систем. Однако узел KMS, работающий под управлением клиентской операционной системы Windows, может активировать только компьютеры, работающие под управлением клиентских операционных систем.

Для узла KMS требуется ключ, который активирует (проверяет подлинность) узла KMS в Майкрософт. Этот ключ иногда называется ключом узла KMS, но его официальное название — клиентский ключ многократной установки Майкрософт (CSVLK). Чтобы получить ключ, перейдите в раздел "Ключи продуктов" веб-сайта Volume Licensing Service Center для следующих соглашений: Open, Open Value, Select, Enterprise и Services Provider License. Вы также можете получить помощь в местном Центре активации Майкрософт.

Требования к операционной деятельности

KMS может активировать физические и виртуальные компьютеры, но для активации на основе KMS в сети должно присутствовать минимальное количество компьютеров (порог активации). Клиенты KMS активируются только после достижения этого порогового значения. Чтобы обеспечить достижение порога активации, узел KMS подсчитывает количество компьютеров, запрашивающих активацию в сети.

Узлы KMS учитывают последние подключения. Когда клиент или сервер обращается к узлу KMS, узел добавляет идентификатор компьютера к счетчику, а затем возвращает значение текущего счетчика в ответе. Клиент или сервер активируется при достаточно высоком значении счетчика. Клиенты будут активированы, если счетчик равен 25 или выше. Выпуски для серверов или томов для продуктов Microsoft Office, будут активированы, если счетчик равен пяти или выше. KMS считает только уникальные подключения за последние 30 дней и хранит только 50 последних контактов.

Активации KMS допустимы в течение 180 дней (период проверки действительности активации). Клиенты KMS должны возобновлять активацию путем подключения к узлу KMS не реже одного раза в 180 дней. По умолчанию клиентские компьютеры KMS пытаются возобновлять активацию каждые семь дней. После возобновления активации клиента отсчет срока действия активации начинается снова.

Один узел KMS может поддерживать неограниченное количество клиентов KMS. Если в среде более 50 клиентов, рекомендуется выделить хотя бы два узла KMS на случай, если один из них станет недоступен. Большинство организаций могут использовать всего лишь два узла KMS для всей своей инфраструктуры.

После активации первого узла KMS можно применить использованный на нем CSVLK для активации до пяти дополнительных узлов KMS в сети (итого шесть). После активации узла KMS администраторы могут до девяти раз повторно активировать тот же узел с одним и тем же ключом.

Если вашей организации требуется более шести узлов KMS, следует запросить дополнительные активации для CSVLK организации — например, если одно корпоративное лицензионное соглашение действует для 10 физических расположений и в каждом из них нужен локальный узел KMS. Чтобы запросить это исключение, обратитесь в местный Центр активации Майкрософт.

Компьютеры, на которых выполняются выпуски Windows Server и клиент Windows с корпоративным лицензированием, по умолчанию являются клиентами KMS, для которых не требуется дополнительная настройка.

При преобразовании узла KMS, компьютера, использующего ключ MAK или работающего под управлением розничной лицензионной версии Windows, в клиенте KMS необходимо установить соответствующий ключ установки клиента KMS. Дополнительные сведения см. на странице Ключи установки клиента KMS.

Требования к сети

Для активации на основе KMS требуется подключение TCP/IP. Узлы и клиенты KMS по умолчанию используют службу доменных имен (DNS). Узлы KMS используют динамическое обновление DNS для автоматической публикации информации, которая нужна клиентам KMS для поиска этих узлов и подключения к ним. Можно принять эти параметры по умолчанию, либо — в случае особых требований сети и конфигурации безопасности — можно вручную настроить узлы и клиенты KMS.

По умолчанию узел KMS настроен для использования протокола TCP через порт 1688.

Версии активации

В следующей таблице перечислены версии узла и клиента KMS для сетей, включающих клиенты Windows Server 2016 и Windows.

> ⓘ **Важно!**
>
> - Для поддержки активации новых клиентов может потребоваться установить обновления Windows на сервере KMS. Если возникнут ошибки активации, убедитесь, что установлены необходимые обновления, перечисленные под этой таблицей.

Группа CSVLK	CSVLK можно разместить в следующих версиях	Выпуски Windows, активируемые этим узлом KMS

Группа CSVLK	CSVLK можно разместить в следующих версиях	Выпуски Windows, активируемые этим узлом KMS
Корпоративная лицензия для Windows Server 2022	• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	• Windows Server 2022 (все выпуски) • Windows Server, Semi-Annual Channel • Windows Server 2019 (все выпуски) • Windows Server 2016 (все выпуски) • Windows 11 Корпоративная/ Корпоративная N • Windows 11 Профессиональная/ Профессиональная N • Windows 11 Профессиональная для рабочих станций/Профессиональная N для рабочих станций • Windows 11 для образовательных учреждений/для образовательных учреждений N • Windows 10 Корпоративная LTSC/LTSC N/LTSB • Windows 10 Корпоративная/ Корпоративная N • Windows 10 Профессиональная/ Профессиональная N • Windows 10 Профессиональная для рабочих станций/Профессиональная N для рабочих станций • Windows 10 для образовательных учреждений/для образовательных учреждений N • Windows Server 2012 R2 (все выпуски) • Windows 8.1 Профессиональная • Windows 8.1 Корпоративная • Windows Server 2012 (все выпуски) • Windows Server 2008 R2 (все выпуски) • Windows Server 2008 (все выпуски) • Windows 7 Профессиональная • Windows 7 Корпоративная

Группа CSVLK	CSVLK можно разместить в следующих версиях	Выпуски Windows, активируемые этим узлом KMS
Корпоративная лицензия для Windows Server 2019	• Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2	• Windows Server, Semi-Annual Channel • Windows Server 2019 (все выпуски) • Windows Server 2016 (все выпуски) • Windows 10 Корпоративная LTSC/LTSC N/LTSB • Windows 10 Корпоративная/ Корпоративная N • Windows 10 Профессиональная/ Профессиональная N • Windows 10 Профессиональная для рабочих станций/Профессиональная N для рабочих станций • Windows 10 для образовательных учреждений/для образовательных учреждений N • Windows Server 2012 R2 (все выпуски) • Windows 8.1 Профессиональная • Windows 8.1 Корпоративная • Windows Server 2012 (все выпуски) • Windows Server 2008 R2 (все выпуски) • Windows Server 2008 (все выпуски) • Windows 7 Профессиональная • Windows 7 Корпоративная

Группа CSVLK	CSVLK можно разместить в следующих версиях	Выпуски Windows, активируемые этим узлом KMS
Корпоративная лицензия для Windows Server 2016	• Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012	• Windows Server, Semi-Annual Channel • Windows Server 2016 (все выпуски) • Windows 10 LTSB (2015 и 2016) • Windows 10 Корпоративная/ Корпоративная N • Windows 10 Профессиональная/ Профессиональная N • Windows 10 Профессиональная для рабочих станций/Профессиональная N для рабочих станций • Windows 10 для образовательных учреждений/для образовательных учреждений N • Windows Server 2012 R2 (все выпуски) • Windows 8.1 Профессиональная • Windows 8.1 Корпоративная • Windows Server 2012 (все выпуски) • Windows Server 2008 R2 (все выпуски) • Windows Server 2008 (все выпуски) • Windows 7 Профессиональная • Windows 7 Корпоративная
Корпоративная лицензия для Windows 10	• Windows 10 • Windows 8.1 • Windows 7	• Windows 10 Профессиональная • Windows 10 Профессиональная N • Windows 10 Корпоративная • Windows 10 Корпоративная N • Windows 10 для образовательных учреждений • Windows 10 для образовательных учреждений N • Windows 10 Корпоративная с долгосрочным обслуживанием (2015) • Windows 10 Корпоративная с долгосрочным обслуживанием N (2015) • Windows 10 Pro для рабочих станций • Windows 8.1 Профессиональная • Windows 8.1 Корпоративная • Windows 7 Профессиональная • Windows 7 Корпоративная

Необходимые обновления узла KMS

В зависимости от того, какая операционная система используется на узле KMS и какие ОС требуется активировать, может потребоваться установить одно или несколько из следующих обновлений. Это необходимо, если вы хотите активировать версию Windows, которая является более новой по сравнению с версией, на которой выполняется узел KMS.

> **Примечание**
>
> Ниже перечислены минимальные необходимые обновления. В качестве вариантов приводятся накопительные обновления или ежемесячные обновления, но лучше установить последнюю доступную версию для операционной системы, чтобы использовать дополнительные исправления системы безопасности и другие исправления.

Версия ОС узла KMS	Версия ОС клиент KMS для активации	Требуемое обновление
Windows Server 2019	• Windows Server 2022	8 июня 2021 года—KB5003646 или более позднее накопительное обновление
Windows Server 2016	• Windows Server 2022 • Windows Server 2019	8 июня 2021 года—KB5003638 или более позднее накопительное обновление
Windows Server 2016	• Windows Server 2019	3 декабря 2018 г. —KB4478877 или более позднее накопительное обновление
Windows Server 2012 R2	• Windows Server 2019 • Windows Server 2016 • Windows 10	27 ноября 2018 г. —KB4467695 (предварительная версия ежемесячного накопительного пакета) или более поздняя
Windows Server 2012 R2	• Windows Server 2016 • Windows 10	Накопительный пакет обновления для Windows 8.1 и Windows Server 2012 R2 за июль 2016 г. или более поздняя версия

Версия ОС узла KMS	Версия ОС клиент KMS для активации	Требуемое обновление
Windows Server 2012	• Windows Server 2016 • Windows Server 2012 R2 • Windows 10	Накопительный пакет обновления для Windows Server 2012 за июль 2016 г. или более поздняя версия
Windows Server 2008 R2	• Windows Server 2012 R2 • Windows Server 2012 • Windows 10	Обновление, которое позволяет узлам KMS под управлением Windows 7 и Windows Server 2008 R2 активировать Windows 10
Windows 8.1	• Windows 10	Накопительный пакет обновления для Windows 8.1 и Windows Server 2012 R2 за июль 2016 г. или более поздняя версия
Windows 7	• Windows 10	Обновление, которое позволяет узлам KMS под управлением Windows 7 и Windows Server 2008 R2 активировать Windows 10

Пакет компонентов для обеспечения совместимости приложений основных серверных компонентов по требованию

Статья • 28.01.2023 • Чтение занимает 8 мин

Пакет компонентов для обеспечения совместимости приложений основных серверных компонентов по требованию (FOD) — это дополнительный пакет компонентов, который можно добавить в установки основных серверных компонентов Windows Server (начиная с Windows Server 2019) или установки Windows Server Semi-Annual Channel в любое время.

Дополнительные сведения о других пакетах компонентов по требованию см. в этой статье.

Зачем устанавливать FOD для обеспечения совместимости приложений?

Обеспечение совместимости приложений (FOD для основных серверных компонентов) значительно улучшает совместимость приложений для варианта установки "Основные серверные компоненты" за счет включения подмножества двоичных файлов и пакетов из варианта установки "Сервер с возможностями рабочего стола" без добавления графической среды. Этот дополнительный пакет доступен в отдельном ISO-файле или в клиентском компоненте Центра обновления Windows, и его можно добавлять только в образы и установки основных серверных компонентов.

FOD для обеспечения совместимости приложений предоставляет два таких основных преимущества:

- Повышает совместимость основных серверных компонентов с серверными приложениями, которые уже представлены на рынке или уже разработаны и развернуты организациями.
- Помогает в предоставлении компонентов ОС и повышает совместимость приложений с программными средствами, используемыми в сценариях оперативной диагностики и устранения неполадок.

Компоненты операционной системы, которые доступны как часть FOD для обеспечения совместимости приложений основных серверных компонентов, включают в себя:

- Консоль управления (MMC) (mmc.exe).
- Средство "Просмотр событий" (Eventvwr.msc).
- Системный монитор (PerfMon.exe).
- Монитор ресурсов (Resmon.exe).
- Диспетчер устройств (Devmgmt.msc).
- Проводник (Explorer.exe).
- Windows PowerShell (Powershell_ISE.exe).
- Средство управления дисками (Diskmgmt.msc).
- Диспетчер отказоустойчивости кластеров (CluAdmin.msc).

> ⓘ **Примечание**
>
> Для диспетчера отказоустойчивости кластеров необходимо сначала добавить компонент отказоустойчивой кластеризации Windows Server, выполнив следующую команду из сеанса PowerShell с повышенными привилегиями:

```PowerShell
Install-WindowsFeature -Name Failover-Clustering -
IncludeManagementTools
```

Начиная с Windows Server версии 1903, также поддерживаются следующие компоненты (если используется та же версия FOD для обеспечения совместимости приложений):

- Диспетчер Hyper-V (virtmgmt.msc).
- Планировщик заданий (taskschd.msc).

Установка пакета компонентов по требованию для обеспечения

совместимости приложений

> ⓘ **Важно!**
>
> FOD для обеспечения совместимости приложений можно установить только для основных серверных компонентов Не пытайтесь добавить FOD для обеспечения совместимости приложений основных серверных компонентов в вариант установки Windows Server с возможностями рабочего стола.

> ⓘ **Важно!**
>
> Для серверов с Windows Server 2022 перед установкой FOD совместимости приложений убедитесь, что вы установили **накопительную предварительную версию обновления 2022-01 для операционной системы Microsoft Server версии 21H2 для 64-разрядных систем (KB5009608)** или более позднее накопительное обновление. Это можно проверить по номеру сборки операционной системы — он должен быть не меньше 20348.502. Ранее, если вы пытались подключиться к серверу с помощью протокола удаленного рабочего стола (RDP), мог отобразиться черный экран, после чего подключение разрывалось.

С подключением к Интернету

1. Если сервер может подключиться к клиентскому компоненту Центра обновления Windows, необходимо просто запустить приведенную ниже команду из сеанса PowerShell с повышенными правами, а затем перезапустить Windows Server после ее выполнения.

```
PowerShell

Add-WindowsCapability -Online -Name
ServerCore.AppCompatibility~~~~0.0.1.0
```

Без подключения к Интернету

1. Если сервер не может подключиться к Центру обновления Windows, скачайте файл ISO-образа пакета языков и дополнительных компонентов Windows Server и скопируйте их в общую папку в вашей локальной сети:

- При наличии корпоративной лицензии вы можете скачать файл ISO-образа пакета языков и дополнительных компонентов Windows Server с портала, на котором был получен файл ISO-образа операционной системы: Volume Licensing Service Center.
- Файл ISO-образа пакета языков и дополнительных компонентов Windows Server также доступен для подписчиков в Центре оценки Майкрософт или на портале Visual Studio.

> **Примечание**
>
> Файл ISO-образа пакета языков и дополнительных компонентов является новым для Windows Server 2022. В предыдущих версиях Windows Server используется ISO-образ пакета компонентов по запросу (FOD).

2. Войдите в систему с использованием учетной записи администратора на компьютере с основными серверными компонентами, который подключен к локальной сети и на который вы хотите добавить FOD для совместимости приложений.

Подключение ISO-образа FOD

1. Используйте команду `New-PSDrive` из PowerShell, `net use` из командной строки или другой метод для подключения к расположению ISO-образа FOD. Например, из сеанса PowerShell с повышенными правами выполните следующую команду:

```
PowerShell

$credential = Get-Credential

New-PSDrive -Name FODShare -PSProvider FileSystem -Root
"\\server\share" -Credential $credential
```

2. Скопируйте ISO-образ FOD в локальную папку на ваш выбор (это может занять некоторое время). Измените приведенные ниже переменные, указав расположение вашей папки и имя файла ISO, и выполните следующие команды, например:

```
PowerShell

$isoFolder = "C:\SetupFiles\WindowsServer\ISOs"
$fodIsoFilename = "FOD_ISO_filename.iso"
```

```
New-Item -ItemType Directory -Path $isoFolder
Copy-Item -Path "FODShare:\$fodIsoFilename" -Destination $isoFolder -
Verbose
```

3. Подключите ISO-образ FOD с помощью следующей команды:

```
PowerShell

$fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
```

4. Выполните следующую команду, чтобы узнать букву диска, к которой подключен ISO-образ FOD:

```
PowerShell

$fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
```

5. Выполните приведенную ниже команду (в зависимости от версии операционной системы).

   Для Windows Server 2022:

```
PowerShell

Add-WindowsCapability -Online -Name
ServerCore.AppCompatibility~~~~0.0.1.0 -Source
${fodDriveLetter}:\LanguagesAndOptionalFeatures\ -LimitAccess
```

   Для предыдущих версий Windows Server:

```
PowerShell

Add-WindowsCapability -Online -Name
ServerCore.AppCompatibility~~~~0.0.1.0 -Source ${fodDriveLetter}:\ -
LimitAccess
```

6. После заполнения индикатора выполнения перезапустите операционную систему.

Добавление Internet Explorer 11 в основные серверные компоненты (необязательно)

Примечание

Чтобы добавить Internet Explorer 11, требуется FOD для обеспечения совместимости приложений основных серверных компонентов, но при добавлении этого FOD Internet Explorer 11 не требуется.

> **ⓘ Примечание**
>
> Начиная с Windows Server 2022, несмотря на то что Internet Explorer 11 можно добавить в установки основных серверных компонентов Windows Server, вместо него следует использовать **Microsoft Edge**. В Microsoft Edge встроен **режим Internet Explorer** ("режим IE"), поэтому вы можете получать доступ к устаревшим веб-сайтам и приложениям на основе Internet Explorer прямо из Microsoft Edge. Информацию о политике жизненного цикла Internet Explorer см. на **этой странице**.

1. Войдите в систему в качестве администратора на компьютере с основными серверными компонентами, на котором уже добавлен FOD для обеспечения совместимости приложений, а необязательный пакет ISO-образа FOD для сервера скопирован локально.

2. Подключите ISO-образ FOD с помощью приведенной ниже команды. На этом шаге предполагается, что вы уже скопировали ISO-образ FOD локально. Если это не так, выполните шаги 1 и 2 из раздела Подключение ISO-образа FOD. Приведенные ниже команды выполняются после этих двух шагов. Измените приведенные ниже переменные, указав расположение вашей папки и имя файла ISO, и выполните следующие команды, например:

   PowerShell

   ```
   $isoFolder = "C:\SetupFiles\WindowsServer\ISOs"
   $fodIsoFilename = "FOD_ISO_filename.iso"

   $fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
   ```

3. Выполните следующую команду, чтобы узнать букву диска, к которой подключен ISO-образ FOD:

   PowerShell

   ```
   $fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
   ```

4. Выполните следующие команды (в зависимости от версии операционной системы), используя переменную `$packagePath` как путь к CAB-файлу Internet

Explorer:

Для Windows Server 2022:

```PowerShell
$packagePath =
"${fodDriveLetter}:\LanguagesAndOptionalFeatures\Microsoft-Windows-
InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~.cab"

Add-WindowsPackage -Online -PackagePath $packagePath
```

Для предыдущих версий Windows Server:

```PowerShell
$packagePath = "${fodDriveLetter}:\Microsoft-Windows-InternetExplorer-
Optional-Package~31bf3856ad364e35~amd64~~.cab"

Add-WindowsPackage -Online -PackagePath $packagePath
```

5. После заполнения индикатора выполнения перезапустите операционную систему.

Заметки о выпуске и предложения

> **ⓘ Важно!**
>
> Компоненты по запросу, установленные в версиях Semi-Annual Channel для Windows Server, не сохранятся после обновления по месту до более новой версии Semi-Annual Channel. Поэтому после обновления их нужно будет установить снова. Кроме того, перед обновлением можно добавить пакет компонентов по требованию для обеспечения совместимости приложений в новый источник установки Windows Server. Это гарантирует, что новая версия пакета компонентов по требованию для обеспечения совместимости приложений будет оставаться в системе после завершения обновления. Дополнительные сведения см. в разделе **Добавление возможностей и дополнительных пакетов в автономный образ основных серверных компонентов WIM**.

- После установки FOD для обеспечения совместимости приложений и перезагрузки сервера цвет рамки окна командной консоли изменится на другой оттенок синего.

- Если вы решили также установить дополнительный пакет Internet Explorer 11, обратите внимание, что открытие локально сохраненных HTM-файлов по двойному щелчку не поддерживается. **Щелкните правой кнопкой мыши** и выберите команду **Открыть с помощью Internet Explorer** или откройте файлы прямо в Internet Explorer, щелкнув пункты **Файл** ->**Открыть**.

- Чтобы еще больше повысить совместимость приложений основных серверных компонентов при наличии FOD для обеспечения совместимости приложений, в качестве дополнительного компонента в основные серверные компоненты была добавлена консоль управления IIS. Чтобы использовать консоль управления IIS, сначала необходимо добавить FOD для обеспечения совместимости приложений. Консоль управления IIS использует консоль MMC (mmc.exe), которая доступна только в основных серверных компонентах, в которых добавлен FOD для обеспечения совместимости приложений. Чтобы добавить консоль управления IIS, выполните командлет PowerShell **Install-WindowsFeature**.

  PowerShell

  ```
  Install-WindowsFeature -Name Web-Mgmt-Console
  ```

- Как правило, при установке приложений в основные серверные компоненты (с этими дополнительными пакетами или без них) иногда необходимо использовать параметры и инструкции для автономной установки.

Добавление в автономный образ основных серверных компонентов WIM

1. Скачайте файлы ISO-образа пакета языков и дополнительных компонентов и ISO-образа Windows Server в локальную папку на компьютере Windows. Это может быть настольный компьютер с Windows, но не обязательно под управлением Windows Server с вариантом установки "Основные серверные компоненты".

   - При наличии корпоративной лицензии вы можете скачать файл ISO-образа пакета языков и дополнительных компонентов Windows Server с портала, на котором был получен файл ISO-образа операционной системы: Volume Licensing Service Center.
   - Файл ISO-образа пакета языков и дополнительных компонентов Windows Server также доступен для подписчиков в Центре оценки Майкрософт или на портале Visual Studio.

> ⓘ **Примечание**
>
> Файл ISO-образа пакета языков и дополнительных компонентов является новым для Windows Server 2022. В предыдущих версиях Windows Server используется ISO-образ пакета компонентов по запросу (FOD).

2. Подключите ISO-образ пакета языков и дополнительных компонентов и ISO-образ Windows Server с помощью приведенных ниже команд в сеансе PowerShell с повышенными привилегиями. Измените приведенные ниже переменные, указав расположение вашей папки и имя файла ISO, и выполните следующие команды, например:

```PowerShell
$isoFolder = "C:\SetupFiles\WindowsServer\ISOs"
$fodIsoFilename = "FOD_ISO_filename.iso"
$wsIsoFilename = "Windows_Server_ISO_filename.iso"

$fodIso = Mount-DiskImage -ImagePath "$isoFolder\$fodIsoFilename"
$wsIso = Mount-DiskImage -ImagePath "$isoFolder\$wsIsoFilename"
```

3. Выполните следующую команду, чтобы получить буквы дисков, к которым подключен ISO-образ FOD и ISO-образ Windows Server:

```PowerShell
$fodDriveLetter = ($fodIso | Get-Volume).DriveLetter
$wsDriveLetter = ($wsIso | Get-Volume).DriveLetter
```

4. Скопируйте содержимое файла ISO-образа Windows Server в локальную папку например, **C:\SetupFiles\WindowsServer\Files**. Это может занять некоторое время.

```PowerShell
$wsFiles = "C:\SetupFiles\WindowsServer\Files"
New-Item -ItemType Directory -Path $wsFiles

Copy-Item -Path ${wsDriveLetter}:\* -Destination $wsFiles -Recurse
```

5. Получите имя образа, который вы хотите изменить, в файле Install.wim с помощью следующей команды. В переменную `$installWimPath` добавьте путь к файлу install.wim, расположенному в папке **sources** файла ISO-образа

Windows Server. Обратите внимание на имена образов, доступные в этом файле install.wim, в выходных данных.

```
PowerShell

$installWimPath =
"C:\SetupFiles\WindowsServer\Files\sources\install.wim"

Get-WindowsImage -ImagePath $installWimPath
```

6. Подключите файл Install.wim в новой папке с помощью следующей команды, заменив значения переменных в примере собственными и повторно использовав переменную `$installWimPath` из предыдущей команды.

   - `$wimImageName`: введите имя образа, который нужно подключить, из выходных данных предыдущей команды. В этом примере используется **Windows Server 2022 Datacenter**.
   - `$wimMountFolder`: укажите пустую папку, которая будет использоваться при доступе к содержимому файла install.wim.

```
PowerShell

$wimImageName = "Windows Server 2022 Datacenter"
$wimMountFolder = "C:\SetupFiles\WindowsServer\WIM"

New-Item -ItemType Directory -Path $wimMountFolder
Set-ItemProperty -Path $installWimPath -Name IsReadOnly -Value $false
Mount-WindowsImage -ImagePath $installWimPath -Name $wimImageName -Path
$wimMountFolder
```

7. Добавьте нужные возможности и пакеты к подключенному образу install.wim с помощью следующих команд (в зависимости от версии), заменив значения переменных в примере собственными значениями.

   - `$capabilityName` — укажите имя возможности, которую необходимо установить (в данном случае возможность **AppCompatibility**).
   - `$packagePath` — укажите путь к пакету, который необходимо установить (в данном случае к CAB-файлу **Internet Explorer**).

   Для Windows Server 2022:

```
PowerShell

$capabilityName = "ServerCore.AppCompatibility~~~~0.0.1.0"
$packagePath =
"${fodDriveLetter}:\LanguagesAndOptionalFeatures\Microsoft-Windows-
```

```
InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~~.cab"

Add-WindowsCapability -Path $wimMountFolder -Name $capabilityName -
Source "${fodDriveLetter}:\LanguagesAndOptionalFeatures" -LimitAccess
Add-WindowsPackage -Path $wimMountFolder -PackagePath $packagePath
```

Для предыдущих версий Windows Server:

PowerShell

```
$capabilityName = "ServerCore.AppCompatibility~~~~0.0.1.0"
$packagePath = "${fodDriveLetter}:\Microsoft-Windows-InternetExplorer-
Optional-Package~31bf3856ad364e35~amd64~~.cab"

Add-WindowsCapability -Path $wimMountFolder -Name $capabilityName -
Source "${fodDriveLetter}:\" -LimitAccess
Add-WindowsPackage -Path $wimMountFolder -PackagePath $packagePath
```

8. Отключите образ и зафиксируйте изменения в файле Install.wim с помощью следующей команды, которая использует переменную `$wimMountFolder` из предыдущих команд:

PowerShell

```
Dismount-WindowsImage -Path $wimMountFolder -Save
```

Теперь можно обновить сервер, запустив файл setup.exe из папки, которую вы создали для файлов установки Windows Server (в этом примере: **C:\SetupFiles\WindowsServer\Files**). Эта папка теперь содержит установочные файлы Windows Server с дополнительными возможностями и пакетами.

Совместимость Windows Server 2022 и серверных приложений корпорации Майкрософт

Статья • 28.01.2023 • Чтение занимает 2 мин

В этой таблице перечислены серверные приложения корпорации Майкрософт, поддерживающие установку и работу в Windows Server 2022. Эти сведения приведены для справки и не предназначены для замены отдельных спецификаций, требований, объявлений или заявлений общего характера для каждого из серверных приложений. Полноценное описание совместимости и параметров см. в официальной документации по каждому продукту.

> **Совет**
>
> Если вы являетесь партнером-поставщиком программного обеспечения, которому нужны дополнительные сведения о совместимости Windows Server с приложениями сторонних разработчиков, посетите **портал сертификации коммерческих приложений**.

Продукт	Поддерживается основными серверными компонентами	Поддерживается на сервере с возможностями рабочего стола	Выпущено	Веб-ссылка на продукт
Azure DevOps Server 2020.1	Да*	Да	Да	Заметки о выпуске Azure DevOps Server 2020.1
Configuration Manager (версия 2107)	Да, как управляемый клиент и точка распространения. Нет, как сервер сайта.	Да, как сервер сайта/системы сайта и управляемый клиент.	Да	Поддержка Windows Server 2022
Exchange Server 2019 CU12 и более поздних версий	Да	Да	Да	Таблица поддержки Exchange Server

Продукт	Поддерживается основными серверными компонентами	Поддерживается на сервере с возможностями рабочего стола	Выпущено	Веб-ссылка на продукт
Host Integration Server 2020	Да	Да	Да	HIS 2020 — новые возможности, заметки о выпуске, требования к системе и установка
Сервер Office Online	Нет	Да	Да	Планирование сервера Office Online
Project Server 2019	Нет	Да	Да	Требования к программному обеспечению для Project Server 2019 — Project Server
Project Server Subscription Edition	Да	Да	Да	Требования к программному обеспечению Project Server Subscription Edition
SharePoint Server 2019	Нет	Да	Да	Требования к аппаратному и программному обеспечению для SharePoint Server 2019
SharePoint Server Subscription Edition	Да	Да	Да	Системные требования для SharePoint Server Subscription Edition

Продукт	Поддерживается основными серверными компонентами	Поддерживается на сервере с возможностями рабочего стола	Выпущено	Веб-ссылка на продукт
SQL Server 2017	Да*	Да	Да	Требования к аппаратному и программному обеспечению для установки SQL Server 2017
SQL Server 2019	Да*	Да	Да	Требования к оборудованию и программному обеспечению для установки SQL Server 2019
System Center Data Protection Manager 2019	Да, как рабочая нагрузка резервного копирования. Нет, как сервер DPM.	Да, как рабочая нагрузка резервного копирования. Нет, как сервер DPM.	Да	Подготовка среды для System Center Data Protection Manager
System Center Data Protection Manager 2022	Да*	Да	Да	Подготовка среды для System Center Data Protection Manager
System Center Operations Manager 2019	Да, как агент. Нет, как сервер управления**	Да, как агент. Нет, как сервер управления**.	Да	Системные требования для System Center Operations Manager
System Center Operations Manager 2022	Да*	Да	Да	Системные требования для System Center Operations Manager
System Center Virtual Machine Manager 2022	Да*	Да	Да	Требования к системе для System Center Virtual Machine Manager

* Могут действовать ограничения или может потребоваться функция совместимости приложений основных серверных компонентов по требованию (FOD). Дополнительные сведения см. в документации по конкретному продукту или функции по требованию.

** См. веб-ссылку на продукт

Совместимость Windows Server 2019 и серверных приложений корпорации Майкрософт

Статья • 28.01.2023 • Чтение занимает 2 мин

В этой таблице перечислены серверные приложения Майкрософт, поддерживающие установку и работу в Windows Server 2019. Эти сведения приведены для справки и не предназначены для замены отдельных спецификаций, требований, объявлений или заявлений общего характера для каждого из серверных приложений. Полноценное описание совместимости и параметров см. в официальной документации по каждому продукту.

> **Совет**
>
> Если вы являетесь партнером-поставщиком программного обеспечения, которому нужны дополнительные сведения о совместимости Windows Server с приложениями сторонних разработчиков, посетите **портал сертификации коммерческих приложений**.

Продукт	Поддерживается основными серверными компонентами	Поддерживается на сервере с возможностями рабочего стола	Выпущено	Веб-ссылка на продукт
Azure DevOps Server 2019	Да*	Да	Да	Azure DevOps Server 2019
Azure DevOps Server 2020	Да*	Да	Да	Azure DevOps Server 2020
Configuration Manager (версия 1806)	Да, если это управляемый клиент; нет, если это сервер сайта.	Да, если это управляемый клиент; нет, если это сервер сайта.	Да	Новые возможности в версии Configuration Manager 1806 (Current Branch)
Exchange Server 2019	Да	Да	Да	Требования к системе для Exchange Server

Продукт	Поддерживается основными серверными компонентами	Поддерживается на сервере с возможностями рабочего стола	Выпущено	Веб-ссылка на продукт
Host Integration Server 2016 с накопительным обновлением 3 (CU3)	Да	Да	Да	Требования к системе для Host Integration Server
Сервер Office Online	Нет	Да	Да	Планирование сервера Office Online
Project Server 2016	Нет	Да	Да	Требования к программному обеспечению для Project Server 2016
Project Server 2019	Нет	Да	Да	Требования к программному обеспечению для Project Server 2019
Project Server Subscription Edition	Да	Да	Да	Требования к программному обеспечению Project Server Subscription Edition
SharePoint Server 2016	Нет	Да	Да	Требования к оборудованию и программному обеспечению для SharePoint Server 2016
SharePoint Server 2019	Нет	Да	Да	Требования к аппаратному и программному обеспечению для SharePoint Server 2019

Продукт	Поддерживается основными серверными компонентами	Поддерживается на сервере с возможностями рабочего стола	Выпущено	Веб-ссылка на продукт
SharePoint Server Subscription Edition	Да	Да	Да	Системные требования для SharePoint Server Subscription Edition
Skype для бизнеса 2019	Нет	Да	Да	Установка необходимых компонентов для Skype для бизнеса Server
SQL Server 2014	Да*	Да	Да	Требования к аппаратному и программному обеспечению для установки SQL Server 2014
SQL Server 2016	Да*	Да	Да	Требования к оборудованию и программному обеспечению для установки SQL Server 2016
SQL Server 2017	Да*	Да	Да	Требования к аппаратному и программному обеспечению для установки SQL Server 2017
SQL Server 2019	Да*	Да	Да	Требования к оборудованию и программному обеспечению для установки SQL Server 2019

Продукт	Поддерживается основными серверными компонентами	Поддерживается на сервере с возможностями рабочего стола	Выпущено	Веб-ссылка на продукт
System Center Data Protection Manager 2019	Нет	Да	Да	Подготовка среды для System Center Data Protection Manager
System Center Operations Manager 2019	Да*	Да	Да	Системные требования для System Center Operations Manager
System Center Virtual Machine Manager 2019	Да*	Да	Да	Требования к системе для System Center Virtual Machine Manager

*Могут действовать ограничения или может потребоваться функция совместимости приложений основных серверных компонентов по требованию (FOD). Обратитесь к документации по конкретному продукту или FOD.

Совместимость Windows Server 2016 и серверных приложений корпорации Майкрософт

Статья • 28.01.2023 • Чтение занимает 2 мин

В этой таблице перечислены серверные приложения корпорации Майкрософт, поддерживающие установку и работу в Windows Server 2016. Эти сведения приведены для справки и не предназначены для замены отдельных спецификаций, требований, объявлений или заявлений общего характера для каждого из серверных приложений. Полноценное описание совместимости и параметров см. в официальной документации по каждому продукту.

> **Совет**
>
> Если вы являетесь партнером-поставщиком программного обеспечения, которому нужны дополнительные сведения о совместимости Windows Server с приложениями сторонних разработчиков, посетите **портал сертификации коммерческих приложений**.

Продукт	Выпущено	Веб-ссылка на продукт
BizTalk Server 2016	Да	Microsoft BizTalk Server
Диспетчер конфигураций (версии 1606)	Да	Новые возможности в диспетчере конфигураций версии 1606
Exchange Server 2016	Да	Обновления для Exchange 2016
Host Integration Server 2016	Да	Новые возможности HIS 2016
Сервер Office Online	Да	Планирование сервера Office Online
Project Server 2016	Да	Требования к программному обеспечению для Project Server 2016
Project Server 2019	Да	Требования к программному обеспечению для Project Server 2019
SharePoint Server 2016	Да	Требования к оборудованию и программному обеспечению для SharePoint Server 2016

Продукт	Выпущено	Веб-ссылка на продукт
SharePoint Server 2019	Да	Требования к аппаратному и программному обеспечению для SharePoint Server 2019
Skype для бизнеса Server 2015	Да	Как установить Скайп для бизнеса Server 2015 в Windows Server 2016
SQL Server 2012	Да	Требования к оборудованию и программному обеспечению для установки SQL Server 2012
SQL Server 2014	Да	Требования к аппаратному и программному обеспечению для установки SQL Server 2014
SQL Server 2016	Да	SQL Server 2016
System Center Virtual Machine Manager 2016	Да	Новые возможности System Center
System Center Operations Manager 2016:	Да	Новые возможности System Center
System Center Data Protection Manager 2016	Да	Новые возможности System Center
Visual Studio Team Foundation Server 2017	Да	Team Foundation Server 2017

Преимущество гибридного использования Azure для Windows Server

Статья • 11.04.2023

Преимущество гибридного использования Azure — это экономичное преимущество, которое позволяет использовать локальные лицензии с лицензиями Software Assurance (SA) или подписок, чтобы получить виртуальные машины Windows в Azure по сниженной цене. В этой статье рассматриваются преимущества лицензий Windows Server с sa или подпиской: экономия затрат на виртуальные машины Windows Server в Azure, Azure Stack HCI и варианты гибридного развертывания Служба Azure Kubernetes (AKS).

Другие преимущества гибридного использования Azure (например, SQL Server) см. в разделе Преимущество гибридного использования Azure.

Что подходит для Преимущество гибридного использования Azure?

Чтобы получить право на Преимущество гибридного использования Azure для Windows Server, вам потребуются локальные основные лицензии для Windows Server с активными лицензиями Software Assurance или подпиской. Лицензии software Assurance и подписки доступны только в рамках коммерческого лицензионного соглашения. Дополнительные сведения о коммерческом лицензировании см. в статье Ресурсы по лицензированию Майкрософт. Дополнительные сведения о лицензиях windows Server core см. в разделе Лицензирование продуктов Windows Server.

> **ⓘ Важно!**
>
> Рабочие нагрузки, использующие Преимущество гибридного использования Azure, могут выполняться только в течение срока действия лицензии Software Assurance или подписки. Когда срок действия лицензии Software Assurance или подписки приближается, необходимо либо продлить соглашение с Software Assurance, либо с лицензией на подписку, либо отключить функцию преимущества гибридного использования, либо отменить подготовку рабочих нагрузок, использующих Преимущество гибридного использования Azure.

Что входит в Преимущество гибридного использования Azure?

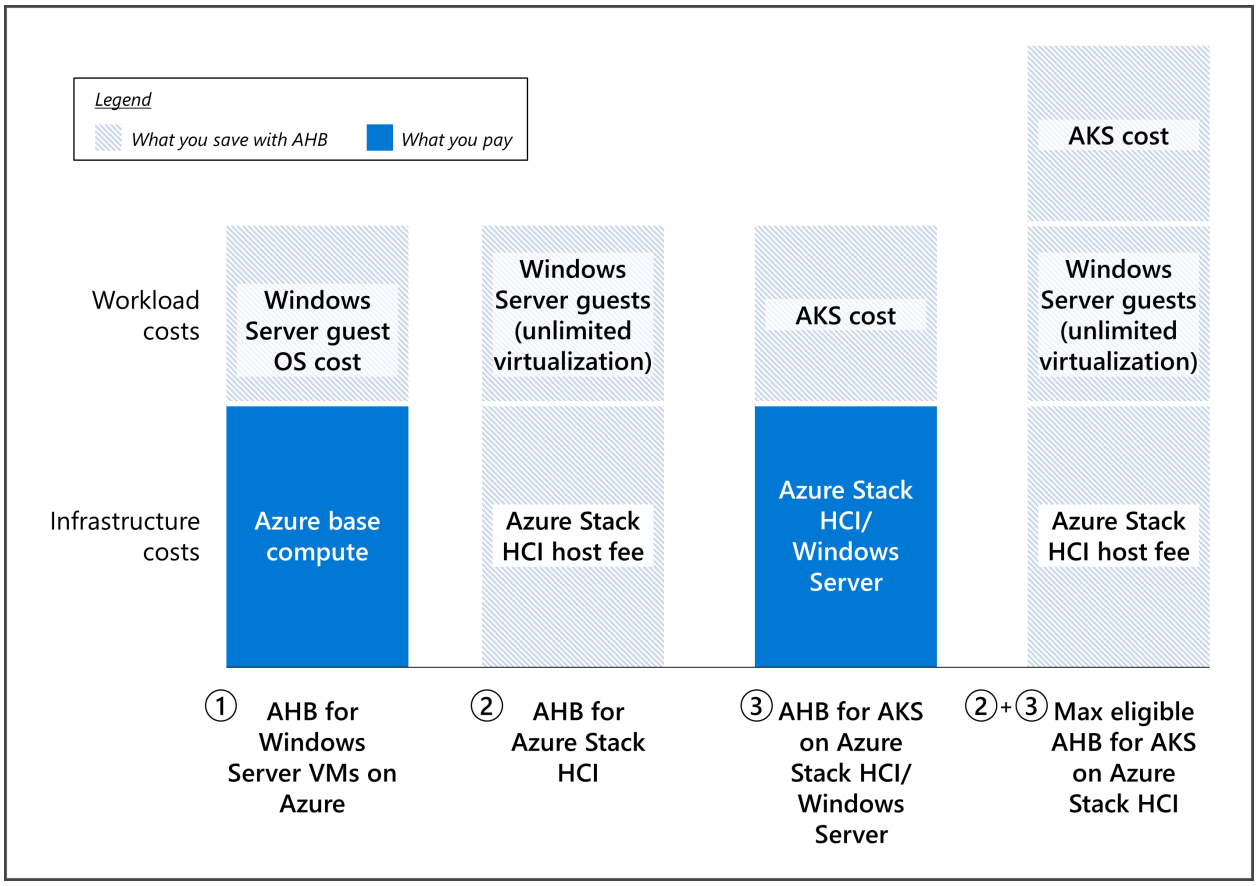
Клиенты с лицензией Windows Server Software Assurance или лицензией по подписке могут использовать Преимущество гибридного использования Azure для дальнейшего сокращения затрат в облаке, в центрах обработки данных и пограничных расположениях.

Преимущество гибридного использования Azure включает в себя следующие средства:

- **Виртуальные машины Windows Server в Azure:** Лицензия на Windows Server распространяется на Преимущество гибридного использования Azure, поэтому необходимо платить только за базовую ставку вычислений виртуальной машины. Базовая скорость вычислений равна скорости Linux для виртуальных машин.

- **Azure Stack HCI:** Плата за размещение Azure Stack HCI и плата за подписку Windows Server отменяются с Преимущество гибридного использования Azure. То есть неограниченные права на виртуализацию предоставляются без дополнительных затрат. Вы по-прежнему оплачиваете другие расходы, связанные с Azure Stack HCI (например, управляемое клиентом оборудование, службы Azure и рабочие нагрузки).

- **AKC:** Запустите AKS в Windows Server и Azure Stack HCI без дополнительных затрат. Вы по-прежнему будете платить за базовую инфраструктуру узлов и все лицензии для контейнеров Windows, если только вы не имеете права на Преимущество гибридного использования Azure для Azure Stack HCI. С помощью Преимущество гибридного использования Azure для Azure Stack HCI вы можете отказаться от платы за узел Azure Stack HCI и подписку Windows Server.



Цены на Преимущество гибридного использования Azure

Чтобы оценить потенциальную экономию средств, можно использовать следующие ресурсы:

- **Виртуальные машины Windows в Azure:**цены на виртуальные машины Windows. Используйте калькулятор экономии Преимущество гибридного использования Azure для оценки экономии или сравните цены на виртуальные машины Windows с Преимущество гибридного использования Azure и без нее.
- **Azure Stack HCI:**цены на Azure Stack HCI.
- **Служба Azure Kubernetes (AKS):**цены на AKS в Azure Stack HCI.

Получение Преимущество гибридного использования Azure для виртуальных машин Windows в Azure

Следуйте указаниям в этом разделе, чтобы получить и поддерживать Преимущество гибридного использования Azure для виртуальных машин Windows в Azure.

лицензирование необходимых компонентов;

Чтобы претендовать на Преимущество гибридного использования Azure для виртуальных машин Windows в Azure, необходимо выполнить следующие предварительные требования к лицензированию.

Типы лицензий

- Windows Server Standard с активной программой Software Assurance или подпиской.
- Windows Server Datacenter с активной программой Software Assurance или подпиской.

Количество лицензий

Для каждой виртуальной машины потребуется не менее 8 ядер (выпуск Datacenter или Standard). Вы также можете запускать экземпляры размером более 8 ядер, выделяя лицензии, равные размеру ядра экземпляра. Например, для 12-ядерного экземпляра требуется 12 лицензий на ядра, однако при запуске 4-ядерного экземпляра по-прежнему требуется 8 лицензий. Для клиентов с лицензиями на процессор каждая лицензия на два ядра эквивалентна 16 лицензиям на процессор.

Права на использование

- **Выпуск Windows Server Standard:** Лицензии должны использоваться как локально, так и в Azure, но не одновременно. Единственным исключением является однократный перенос рабочих нагрузок в Azure на срок до 180 дней.

- **Выпуск Windows Server Datacenter:** Лицензии позволяют одновременно использовать локально и в Azure. Права двойного использования не применяются к лицензиям, выделенным для неограниченных прав виртуализации.

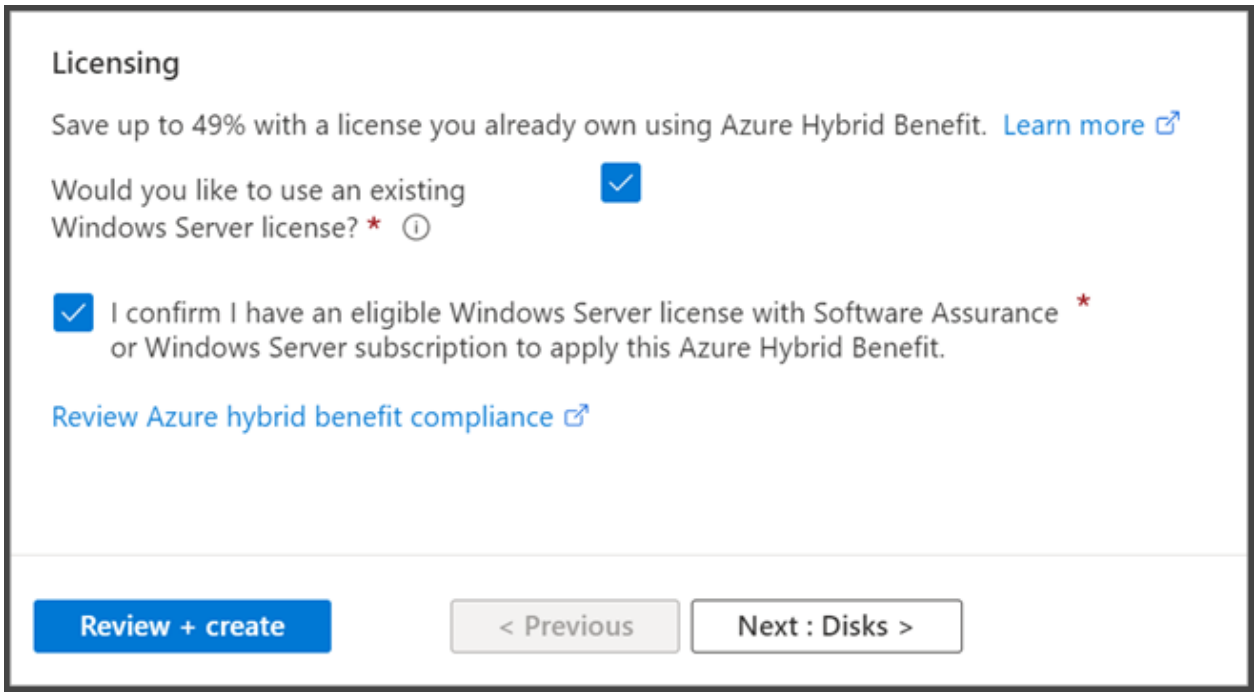
Неограниченная виртуализация

Неограниченные права виртуализации — это право использовать любое количество виртуальных машин Windows Server на узле.

- **Выпуск Windows Server Datacenter:** Вы можете использовать любое количество виртуальных машин Windows Server на выделенном узле Azure, если выделить лицензии Windows Server Datacenter с активной sa или подпиской для всех доступных физических ядер на этом сервере Azure.
- **Выпуск Windows Server Standard:** Неограниченные права на виртуализацию недоступны.

Применение Преимущество гибридного использования Azure для виртуальных машин Windows в Azure

Чтобы узнать, как развернуть виртуальные машины Windows Server в Azure с помощью Преимущество гибридного использования Azure, выполните действия, описанные в статье Изучение Преимущество гибридного использования Azure для виртуальных машин Windows. Одним из способов активации Преимущество гибридного использования Azure для виртуальной машины Windows Server является проверка поле **Лицензирование** во время создания виртуальной машины, как показано ниже.



Обеспечение соответствия

Если вы применяете Преимущество гибридного использования Azure к виртуальным машинам Windows Server, проверьте количество соответствующих лицензий и период покрытия Software Assurance (или подписки), прежде чем активировать это преимущество. Используйте приведенные выше рекомендации,

чтобы обеспечить правильное развертывание количества виртуальных машин Windows Server с этим преимуществом.

Если у вас уже есть виртуальные машины Windows Server, работающие с Преимущество гибридного использования Azure, выполните инвентаризацию, чтобы узнать, сколько единиц вы используете, и проверка это число для лицензий Software Assurance или подписки. Вы можете обратиться к специалисту по лицензированию Майкрософт, чтобы проверить свою позицию по лицензированию Software Assurance.

Чтобы просмотреть и подсчитать все виртуальные машины, развернутые с Преимущество гибридного использования Azure в подписке Azure, выведите список всех виртуальных машин и масштабируемых наборов виртуальных машин, выполнив действия, описанные в разделе Изучение Преимущество гибридного использования Azure для виртуальных машин Windows.

Вы также можете просмотреть счет за Microsoft Azure, чтобы определить, сколько виртуальных машин с Преимущество гибридного использования Azure для Windows Server вы используете. Сведения о количестве экземпляров с преимуществом см. в разделе **Дополнительные сведения**:

JSON


```
"
{"ImageType":"WindowsServerBYOL","ServiceType":"Standard_A1","VMName":"","Us
ageType":"ComputeHR"}"
```


Выставление счетов не применяется в режиме реального времени. Ожидается задержка в несколько часов после активации виртуальной машины Windows Server с Преимущество гибридного использования Azure, прежде чем виртуальная машина появится в счете.

Чтобы получить полное представление о вашей позиции лицензирования, выполните инвентаризацию в каждой подписке Azure. Убедитесь, что у вас есть полная лицензия на виртуальные машины Windows Server, работающие с Преимущество гибридного использования Azure. Вам не нужно предпринимать никаких дальнейших действий.

Регулярно проводите инвентаризацию, чтобы убедиться, что вы используете все лицензионные преимущества, на которые вы имеете право. Регулярные инвентаризации помогут вам сократить затраты и убедиться, что у вас всегда достаточно лицензий для покрытия виртуальных машин Windows Server, развернутых с помощью Преимущество гибридного использования Azure.

Если у вас недостаточно соответствующих лицензий Windows Server для развернутых виртуальных машин, можно выбрать три варианта:

- Приобретите дополнительные лицензии Windows Server, охватываемые Software Assurance или подпиской, в рамках коммерческого лицензионного соглашения.
- Отключите Преимущество гибридного использования Azure для некоторых виртуальных машин и приобретите их по почасовой ставке Azure.
- Отмените выделение некоторых виртуальных машин.

> ⓘ **Примечание**
>
> Майкрософт оставляет за собой право в любое время провести аудит клиентов для подтверждения прав на использование Преимущества гибридного использования Azure.

Получение Преимущество гибридного использования Azure для Azure Stack HCI

Используйте инструкции в этом разделе, чтобы получить Преимущество гибридного использования Azure для инфраструктуры Azure Stack HCI.

лицензирование необходимых компонентов;

Чтобы претендовать на Преимущество гибридного использования Azure для Azure Stack HCI, необходимо выполнить следующие предварительные требования к лицензированию.

Типы лицензий

- Windows Server Datacenter только с активными лицензиями Software Assurance или подпиской

Количество лицензий

- Каждая лицензия windows Server core дает право использовать 1 физическое ядро Azure Stack HCI. Вам потребуется выделить достаточно лицензий на ядра для всех физических ядер на серверах в кластере Azure Stack HCI.

Неограниченная виртуализация

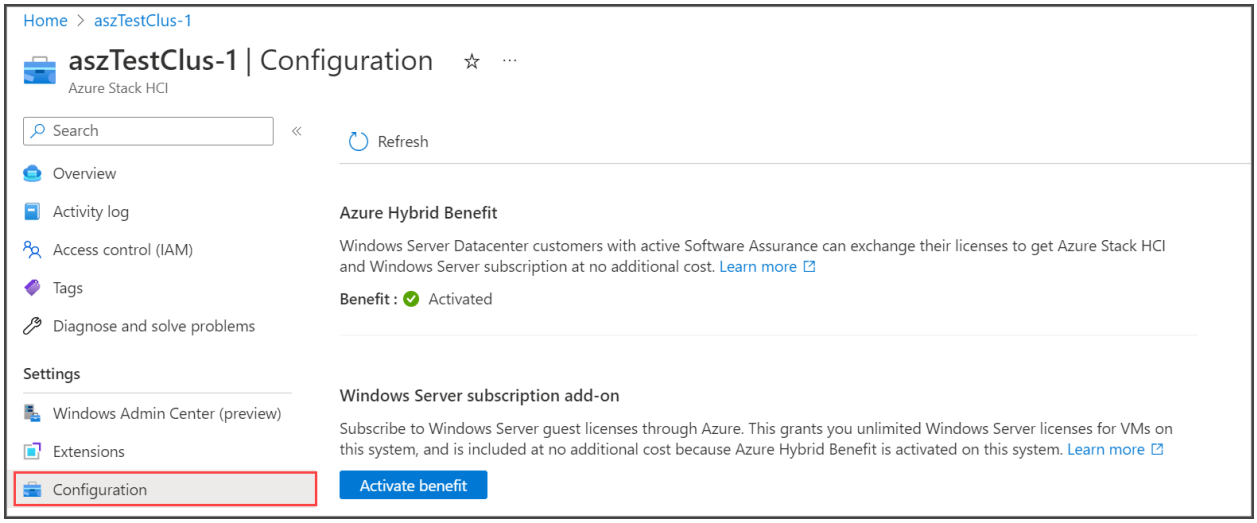
- Вы можете использовать любое количество виртуальных машин Windows Server в кластере Azure Stack HCI, если выделить достаточно лицензий на ядра для всех физических ядер на серверах в кластере Azure Stack HCI.

Права на использование

- Лицензии должны использоваться как в локальной среде, так и в Azure Stack HCI, но не в обоих вариантах. Для переноса серверов у вас будет 180 дней параллельного лицензирования.

Применение Преимущество гибридного использования Azure для Azure Stack HCI

Вы можете узнать, как развернуть Преимущество гибридного использования Azure для Azure Stack HCI, выполнив действия, описанные в статье Выставление счетов и оплата Azure Stack HCI. Одним из способов является активация преимущества из области **Конфигурация** ресурса Azure Stack HCI, как показано ниже.



Получение Преимущество гибридного использования Azure для AKS

Следуйте указаниям в этом разделе, чтобы получить Преимущество гибридного использования Azure для AKS.

лицензирование необходимых компонентов;

Чтобы претендовать на Преимущество гибридного использования Azure для AKS, необходимо выполнить следующие предварительные требования к лицензированию.

Подходящие узлы

- Windows Server 2019 или более поздней версии (Datacenter или Standard) или
- Azure Stack HCI

Типы лицензий

- Windows Server Standard с активной программой Software Assurance или подпиской.
- Windows Server Datacenter с активной программой Software Assurance или подпиской.

Количество лицензий

- Каждая лицензия windows Server core дает право на использование в 1 виртуальном ядре AKS.

Права на использование

- Преимущество гибридного использования Azure для AKS является аддитивным. Основные лицензии, используемые для Преимущество гибридного использования Azure для AKS, можно использовать одновременно с локальным лицензированием Windows Server, а также Преимущество гибридного использования Azure для других рабочих нагрузок, приведенных в этой статье.

Применение Преимущество гибридного использования Azure для AKS

Чтобы приступить к работе с Преимущество гибридного использования Azure для AKS, см. Преимущество гибридного использования Azure для AKS.

Вопросы и ответы: Преимущество гибридного использования Azure

В каких регионах можно Преимущество гибридного использования Azure?

Преимущество гибридного использования Azure доступна во всех регионах Azure и национальных облаках.

Что произойдет с моими преимуществами, если истекает срок действия моего Software Assurance или подписки?

Чтобы использовать эти преимущества, ваша программа Software Assurance или подписки должны быть активными. Если вы решите не продлевать подписку software Assurance или подписку по истечении срока действия, вам потребуется удалить преимущества из ресурсов в портал Azure.

Что такое Software Assurance?

Software Assurance предоставляет другие преимущества для максимального увеличения инвестиций в ИТ. Программа Software Assurance доступна только в рамках корпоративного лицензирования и приобретается при покупке или продлении соглашения о корпоративном лицензировании. Он входит в некоторые соглашения и является необязательной покупкой с другими. Преимущества Software Assurance включают новые права на версию продукта, поддержку, права на мобильность лицензий и уникальный набор технологий и служб.

Сведения о корпоративном лицензировании см. в разделе Лицензирование Майкрософт. Дополнительные сведения о преимуществах Software Assurance и о том, как каждое преимущество может помочь в удовлетворении бизнес-потребностей, см. в статье Преимущества Software Assurance.

Что такое лицензия на подписку?

Лицензии на подписку — это лицензии на запуск программного обеспечения только в течение срока действия подписки. Лицензии на подписку не включают бессрочные права на запуск программного обеспечения.

Как клиенты могут получить Software Assurance?

Вы можете приобрести Software Assurance по программе корпоративного лицензирования. Преимущества Software Assurance активируются в центре корпоративного лицензирования (VLSC). Если в вашей организации есть соглашение о продуктах и услугах Майкрософт (MPSA), бизнес-центр будет

вашим назначением для упрощения управления преимуществами Software Assurance.

Что такое сервер secured-core?

Статья • 11.04.2023

> Область применения: Windows Server 2022, Azure Stack HCI версии 21H2 и более поздних версий

Secured-Core — это набор возможностей, которые предлагают встроенные функции безопасности оборудования, встроенного ПО, драйверов и операционной системы. Защита, предоставляемая системами с защищенными ядрами, начинается до загрузки операционной системы и продолжается во время работы. Сервер secured-core предназначен для предоставления безопасной платформы для критически важных данных и приложений.

Сервер secured-core основан на трех основных принципах безопасности:

- Создание корня доверия с аппаратной поддержкой.
- Защита от атак на уровне встроенного ПО.
- Защита ОС от выполнения непроверенного кода.

Что делает сервер защищенных ядер

Инициатива secured-core началась с компьютеров с Windows благодаря тесной совместной работе между корпорацией Майкрософт и партнерами по производству компьютеров, чтобы обеспечить наиболее высокий уровень безопасности Windows когда-либо. Корпорация Майкрософт расширила партнерские отношения с партнерами по производству серверов, чтобы гарантировать, что Windows Server обеспечивает безопасную среду операционной системы.

Windows Server тесно интегрируется с оборудованием для обеспечения более высокого уровня безопасности:

- Рекомендуемый базовый план: рекомендуемый минимум для всех систем для обеспечения целостности базовой системы с помощью доверенного платформенного модуля 2.0 для аппаратного корня доверия и безопасной загрузки. Для сертификации оборудования Windows Server требуются TPM2.0 и безопасная загрузка. Дополнительные сведения см. в статье Корпорация Майкрософт повышает уровень безопасности для следующего основного выпуска Windows Server.

- Сервер с защищенными ядрами: рекомендуется для систем и отраслей, требующих более высокого уровня гарантии. Сервер с защищенными ядрами основан на предыдущих функциях и использует расширенные возможности процессора для защиты от атак на встроенное ПО.

В следующей таблице показано, как каждая концепция и функция безопасности используются для создания сервера с защищенным ядром.

Концепция	**Компонент**	**Требование**	**Рекомендуемые базовые показатели**	**сервер Secured-Core**
Создание корня доверия с аппаратной поддержкой				
	Безопасная загрузка	Безопасная загрузка включена в BIOS UEFI по умолчанию.	✓	✓
	доверенный платформенный модуль (TPM) 2.0;	Соответствие последним требованиям Майкрософт для спецификации Trusted Computing Group (TCG).	✓	✓
	Сертифицировано для Windows Server	Демонстрирует, что серверная система соответствует наивысшей технической планки Майкрософт по обеспечению безопасности, надежности и управляемости.	✓	✓
	Защита DMA загрузки	Поддержка на устройствах с единицей управления памятью ввода-вывода (IOMMU). Например, Intel VT-D или AMD-Vi.		✓

Концепция	Компонент	Требование	Рекомендуемые базовые показатели	сервер Secured-Core
Защита от атак на уровне встроенного ПО				
	безопасный запуск System Guard	Включена в операционной системе с оборудованием Intel и AMD, совместимым с dynamic root of Trust for Measurement (DRTM).		✓
Защита ОС от выполнения непроверенного кода				
	Безопасность на основе виртуализации	Требуется гипервизор Windows, который поддерживается только на 64-разрядных процессорах с расширениями виртуализации, включая Intel VT-X и AMD-v.	✓	✓
	Гипервизор с улучшенной целостностью кода (HVCI)	Драйверы, совместимые с целостностью кода гипервизора (HVCI), а также требования к VBS.	✓	✓

Создание корня доверия с аппаратной поддержкой

Безопасная загрузка UEFI — это стандарт безопасности, который защищает серверы от вредоносных программ rootkit путем проверки компонентов загрузки систем. Безопасная загрузка проверяет, что доверенный автор имеет цифровую подпись для драйверов и приложений встроенного ПО UEFI. При запуске сервера

встроенное ПО проверяет подпись каждого компонента загрузки, включая драйверы встроенного ПО и ОС. Если подписи действительны, сервер загружается, а встроенное ПО предоставляет управление операционной системе.

Дополнительные сведения о процессе загрузки см. в статье Защита процесса загрузки Windows.

TPM 2.0 предоставляет безопасное аппаратное хранилище для конфиденциальных ключей и данных. Каждый компонент, загруженный во время загрузки, измеряется и измерения, хранящиеся в TPM. Проверка корня доверия оборудования повышает уровень защиты, предоставляемый такими возможностями, как BitLocker, который использует доверенный платформенный модуль 2.0 и упрощает создание рабочих процессов на основе аттестации. Эти рабочие процессы на основе аттестации можно включить в стратегии безопасности с нулевым доверием.

Узнайте больше о доверенных платформенных модулях и о том, как Windows использует TPM.

Наряду с безопасной загрузкой и TPM 2.0, Защищенное ядро Windows Server использует защиту DMA загрузки на совместимых процессорах с единицей управления памятью ввода-вывода (IOMMU). Например, Intel VT-D или AMD-Vi. С помощью защиты DMA загрузки системы защищены от атак прямого доступа к памяти (DMA) во время загрузки и во время выполнения операционной системы.

Защита от атак на уровне встроенного ПО

Решения для защиты конечных точек и обнаружения обычно имеют ограниченную видимость встроенного ПО, учитывая, что встроенное ПО выполняется под операционной системой. Встроенное ПО имеет более высокий уровень доступа и привилегий, чем ядро операционной системы и низкоуровневой оболочки, что делает его привлекательной целью для злоумышленников. Атаки, направленные на встроенное ПО, подрывают другие меры безопасности, реализованные операционной системой, что затрудняет обнаружение компрометации системы или пользователя.

Начиная с Windows Server 2022, безопасный запуск System Guard защищает процесс загрузки от атак встроенного ПО с помощью аппаратных возможностей AMD и Intel. Благодаря поддержке процессора технологии Dynamic Root of Trust for Measurement (DRTM) серверы с защищенными ядрами помещают встроенное ПО в аппаратную песочницу, помогая ограничить последствия уязвимостей в коде встроенного ПО с высоким уровнем привилегий. System Guard использует возможности DRTM, встроенные в совместимые процессоры, для запуска

операционной системы, гарантируя, что система запускается в доверенном, указанном с использованием проверенного кода.

Защита ОС от выполнения непроверенного кода

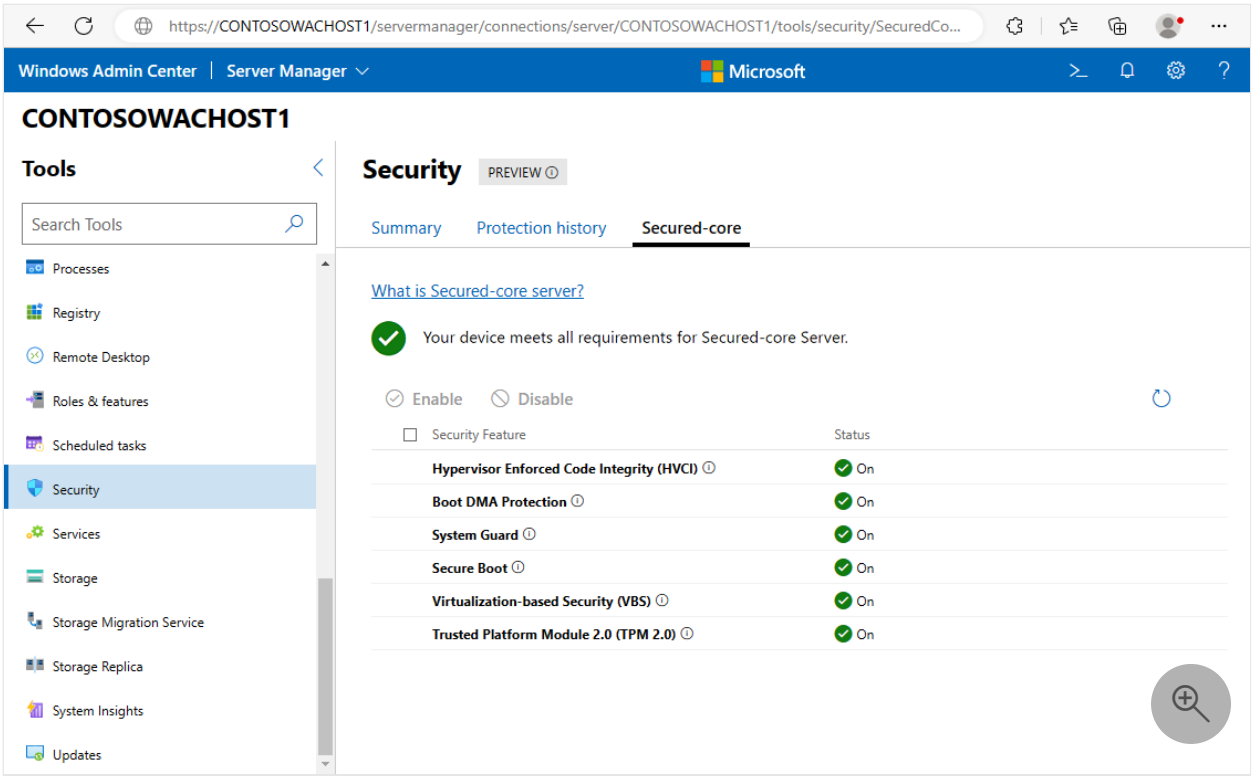
Сервер secured-core использует безопасность на основе виртуализации (VBS) и целостность кода, защищенную гипервизором (HVCI), чтобы создать и изолировать безопасную область памяти от обычной операционной системы. VBS использует гипервизор Windows для создания виртуального безопасного режима (VSM) для предоставления границ безопасности в операционной системе, которые можно использовать для других решений по обеспечению безопасности.

HVCI, обычно называемый защитой целостности памяти, — это решение для обеспечения безопасности, которое позволяет гарантировать, что в ядре может выполняться только подписанный и доверенный код. Использование только подписанного и доверенного кода предотвращает атаки, которые пытаются изменить код в режиме ядра. Например, атаки, которые изменяют драйверы, или эксплойты, такие как WannaCry, которые пытаются внедрить вредоносный код в ядро.

Дополнительные сведения о требованиях к VBS и оборудованию см. в статье Безопасность на основе виртуализации.

Упрощенное управление

Вы можете просматривать и настраивать функции безопасности ОС систем с защищенными ядрами с помощью Windows PowerShell или расширения безопасности в Windows Admin Center. Благодаря интегрированным системам Azure Stack HCI производственные партнеры еще больше упростили процесс настройки для клиентов, чтобы обеспечить наилучшую безопасность сервера Корпорации Майкрософт.



Дополнительные сведения о Windows Admin Center.

Профилактическая защита

Вы можете упреждающе защититься от многих способов, которые злоумышленники используют для использования систем, включив функциональность Secured-Core. Сервер с защищенными ядрами включает расширенные функции безопасности на нижних уровнях технологического стека, защищая наиболее привилегированные области системы до того, как многие средства безопасности знают об эксплойтах. Это также происходит без дополнительных задач или мониторинга со стороны ИТ-отделов и команд SecOps.

Начало работы с защищенным ядром

Оборудование, сертифицированное для сервера с защищенными ядрами, можно найти в каталоге Windows Server и серверах Azure Stack HCI в каталоге Azure Stack HCI. Эти сертифицированные серверы полностью оснащены ведущими в отрасли средствами защиты, встроенными в оборудование, встроенное ПО и операционную систему, чтобы помочь сорвать некоторые из самых сложных векторов атак.

Дальнейшие действия

Теперь вы понимаете, что такое сервер Secured-Core. Ниже приведены некоторые ресурсы для начала работы. Узнайте, как:

- Корпорация Майкрософт обеспечивает расширенную безопасность оборудования для серверов и пограничных вычислений с помощью secured-core в блоге о безопасности Майкрософт.
- Новые защищенные серверы с ядрами теперь доступны в экосистеме Майкрософт для защиты инфраструктуры в блоге о безопасности Майкрософт.
- Создание совместимых с Windows устройств, систем и драйверов фильтров на всех платформах Windows в спецификациях и политиках программы совместимости оборудования Windows.

Как создать узел активации служб управления ключами (KMS)

Статья • 28.01.2023 • Чтение занимает 4 мин

KMS использует модель "клиент — сервер" для активных клиентов Windows. Сама служба используется для активации корпоративных лицензий в вашей локальной сети. Для активации клиенты KMS подключаются к серверу KMS, который называется узлом KMS. Клиенты KMS, которых может активировать узел KMS, зависят от ключа узла, используемого для активации узла KMS. В этой статье показано, как создать узел KMS. Дополнительные сведения о KMS и исходном планировании см. в статье Планирование активации служб управления ключами (KMS).

Предварительные требования

Один узел KMS может поддерживать неограниченное количество клиентов KMS. Если в среде более 50 клиентов, рекомендуется выделить хотя бы два узла KMS на случай, если один из них станет недоступен. Большинство организаций могут использовать всего лишь два узла KMS для всей своей инфраструктуры.

Узлы KMS не обязательно должны быть выделенными серверами, и службы KMS могут размещаться на сервере вместе с другими службами. Вы можете запустить узел KMS в любой физической или виртуальной системе, в которой работает поддерживаемая клиентская операционная система Windows Server или Windows.

Версия Windows, используемая для узла KMS, определяет версию Windows, которую можно активировать для клиентов KMS. См. таблицу версий активации, чтобы определить, какая из них подходит для вашей среды.

По умолчанию узлы KMS автоматически публикуют записи ресурсов SRV в DNS. Это позволяет клиентам KMS автоматически обнаруживать узел KMS и активировать его без необходимости настраивать клиент KMS. Автоматическую публикацию можно отключить, а записи можно создать вручную, что также требуется при автоматической активации, если служба DNS не поддерживает динамические обновления.

Вам потребуется:

- Компьютер, на котором работает Windows Server или Windows. Узел KMS, работающий под управлением операционной системы Windows Server, может

активировать компьютеры под управлением как серверной, так и клиентской операционных систем. Однако узел KMS, работающий под управлением клиентской операционной системы Windows, может активировать только компьютеры, работающие под управлением клиентских операционных систем.

- Используемая учетная запись должна быть членом группы администраторов на узле KMS.
- Ключ узла KMS для организации. Этот ключ можно получить в разделе "Ключи продуктов" на странице Volume Licensing Service Center.

Установка и настройка узла KMS

1. В сеансе PowerShell с повышенными привилегиями выполните следующую команду, чтобы установить роль служб активации корпоративных лицензий:

```
PowerShell

Install-WindowsFeature -Name VolumeActivation -IncludeManagementTools
```

2. Настройте Брандмауэр Windows, чтобы разрешить службе управления ключами принимать сетевой трафик. Вы можете разрешить это для всех сетевых профилей (по умолчанию) или любого сочетания профилей доменной, частной и общедоступной сетей. По умолчанию узел KMS настроен для использования протокола TCP через порт 1688. В примере ниже правило брандмауэра настроено, чтобы разрешить сетевой трафик только для профилей доменной и частной сетей:

```
PowerShell

Set-NetFirewallRule -Name SPPSVC-In-TCP -Profile Domain,Private -
Enabled True
```

3. Запустите мастер средств активации корпоративных лицензий, выполнив следующую команду:

```
PowerShell

vmw.exe
```

4. На начальном экране щелкните **Далее**. Выберите **Служба управления ключами (KMS)** в качестве типа активации и введите `localhost`, чтобы настроить локальный сервер или имя узла сервера.

5. Выберите **Установить ключ узла KMS** и введите ключ продукта для своей организации, а затем щелкните **Зафиксировать**.

6. После установки ключа продукта продукт нужно активировать. Щелкните **Далее**.

7. В раскрывающемся меню выберите продукт, который нужно активировать, а затем укажите, как выполнить активацию: через Интернет или по телефону. Выберите для этого примера **Активировать через Интернет** и щелкните **Зафиксировать**.

8. После успешной активации отобразится конфигурация узла KMS. Если вам нужна именно такая конфигурация, щелкните **Закрыть**, чтобы выйти из мастера. Будут созданы записи DNS, и вы сможете начать активацию клиентов KMS. См. раздел ниже, если вам нужно создать записи DNS вручную. Если вы хотите изменить параметры конфигурации, щелкните **Далее**.

9. **Необязательно.** Измените значения конфигурации с учетом своих требований и щелкните **Зафиксировать**.

> ⓘ **Примечание**
>
> Теперь вы можете начать **активацию клиентов KMS**, но в сети должно быть минимальное количество компьютеров (так называемый порог активации). Узлы KMS учитывают количество недавних подключений, и поэтому, когда клиент или сервер обращается к узлу KMS, узел добавляет идентификатор компьютера к своему счетчику, а затем возвращает текущее значение счетчика в ответе. Клиент или сервер активируется при достаточно высоком значении счетчика. Клиенты Windows будут активированы, если значение счетчика равно 25 или выше. Windows Server и корпоративные выпуски продуктов Microsoft Office активируются, если это значение равно пяти или выше. KMS считает только уникальные подключения за последние 30 дней и хранит только 50 последних контактов.

Создание записей DNS вручную

Если служба DNS не поддерживает динамическое обновление, записи ресурсов нужно создать вручную для публикации узла KMS. Создайте записи ресурсов DNS для KMS вручную с помощью службы DNS, используя приведенную ниже информацию (изменив номер порта по умолчанию, если вы изменили его в конфигурации узла KMS):

Свойство.	**Значение**
Тип	SRV
Служба или имя	_vlmcs
Протокол	_tcp
Приоритет	0
Вес	0
Номер порта	1688;
Hostname (Имя узла)	*FQDN узла KMS*.

Вы также должны отключить публикацию на всех узлах KMS, если ваша служба DNS не поддерживает динамическое обновление, чтобы журналы событий не собирали события публикации DNS, завершившиеся сбоем.

> **Совет**
>
> Записи ресурсов, созданные вручную, также могут сосуществовать с записями ресурсов, которые узлы KMS автоматически публикуют в других доменах, если все записи поддерживаются для предотвращения конфликтов.

Отключение публикации записей DNS

Чтобы отключить публикацию записей DNS узлом KMS, сделайте следующее:

1. Запустите мастер средств активации корпоративных лицензий, выполнив следующую команду:

```
PowerShell
vmw.exe
```

2. На начальном экране щелкните **Далее**. Выберите **Служба управления ключами (KMS)** в качестве типа активации и введите `localhost`, чтобы настроить локальный сервер или имя узла сервера.

3. Выберите **Перейти к конфигурации**, а затем щелкните **Далее**.

4. Снимите флажок включения публикации записей DNS, а затем щелкните **Зафиксировать**.

Активация клиента службы управления ключами (KMS) и ключи продуктов

Статья • 28.01.2023 • Чтение занимает 5 мин

Чтобы использовать KMS, в локальной сети должен быть доступен узел KMS. Компьютеры, активируемые с помощью узла KMS, должны иметь определенный ключ продукта. Этот ключ иногда называют ключом клиента KMS, но формально он называется универсальным корпоративным ключом многократной установки Microsoft (GVLK). Компьютеры, на которых выполняются выпуски Windows Server и клиент Windows с корпоративным лицензированием, умолчанию являются клиентами KMS, для которых не требуется дополнительная настройка, так как соответствующий ключ GVLK уже существует.

Но в некоторых сценариях требуется добавить GVLK на компьютер, который вы хотите активировать на узле KMS, например:

- при переключении компьютера из режима использования ключа многократной активации (MAK);
- при преобразовании розничной лицензии Windows в клиент KMS;
- если компьютер ранее был узлом KMS.

> ⓘ **Важно!**
>
> Чтобы использовать перечисленные здесь ключи (GVLK), в локальной среде должен быть узел KMS. Если у вас еще нет узла KMS, см. сведения в статье **Создание узла KMS**.
>
> Если вы хотите активировать Windows без доступного узла KMS и без активации тома (например, вы пытаетесь активировать розничную версию клиента Windows), **эти ключи не будут работать**. Вам нужно использовать другой метод активации Windows, например использование ключа MAK или приобретение розничной лицензии. Узнайте, как **найти ключ своего продукта Windows**, и что такое **лицензионные версии Windows**.

Установка ключа продукта

Если вы переключаете компьютер из режима использования узла KMS, ключа MAK или розничной версии Windows в режим клиента KMS, установите соответствующий ключ продукта (GVLK) из списка ниже. Чтобы установить ключ продукта клиента, откройте командную строку администратора на клиенте и выполните следующую команду, а затем нажмите клавишу `Enter`:

```
slmgr /ipk <product key>
```

Например, чтобы установить ключ продукта для выпуска Windows Server 2022 Datacenter, выполните следующую команду и нажмите клавишу `Enter`:

```
slmgr /ipk WX4NM-KYWYW-QJJR4-XV3QB-6VM33
```

Универсальные ключи многократной установки (GVLK)

В таблицах ниже вы найдете ключи GVLK для каждой версии и выпуска Windows. LTSC означает *Long-Term Servicing Channel*, а LTSB — *Long-Term Servicing Branch*.

Windows Server (версии LTSC)

Windows Server 2022

Версия операционной системы	Ключ продукта клиента KMS
Windows Server 2022 Datacenter	WX4NM-KYWYW-QJJR4-XV3QB-6VM33
Windows Server 2022 Standard	VDYBN-27WPP-V4HQT-9VMD4-VMK7H

Windows Server 2019

Версия операционной системы	Ключ продукта клиента KMS
Windows Server 2019 Datacenter	WMDGN-G9PQG-XVVXX-R3X43-63DFG
Windows Server 2019 Standard	N69G4-B89J2-4G8F4-WWYCC-J464C

Версия операционной системы	Ключ продукта клиента KMS
Windows Server 2019 Essentials	WVDHN-86M7X-466P6-VHXV7-YY726

Windows Server 2016

Версия операционной системы	Ключ продукта клиента KMS
Windows Server 2016 Datacenter	CB7KF-BWN84-R7R2Y-793K2-8XDDG
Windows Server 2016 Standard	WC2BQ-8NRM3-FDDYY-2BFGV-KHKQY
Windows Server 2016 Essentials	JCKRF-N37P4-C2D82-9YXRT-4M63B

Windows Server (версии Semi-Annual Channel)

Windows Server, версии 20H2, 2004, 1909, 1903 и 1809

Версия операционной системы	Ключ продукта клиента KMS
Windows Server Datacenter	6NMRW-2C8FM-D24W7-TQWMY-CWH2D
Windows Server Standard	N2KJX-J94YW-TQVFB-DG9YT-724CC

Windows 11 и Windows 10 (версии Semi-Annual Channel)

См. в разделе Справочные материалы по жизненному циклу Windows сведения о поддерживаемых версиях и конечных датах обслуживания.

Версия операционной системы	Ключ продукта клиента KMS
Windows 11 Pro Windows 10 Pro	W269N-WFGWX-YVC9B-4J6C9-T83GX
Windows 11 Pro N Windows 10 Pro N	MH37W-N47XK-V7XM9-C7227-GCQG9
Windows 11 Pro для рабочих станций Windows 10 Pro для рабочих станций	NRG8B-VKK3Q-CXVCJ-9G2XF-6Q84J
Windows 11 Pro для рабочих станций N Windows 10 Pro для рабочих станций N	9FNHH-K3HBT-3W4TD-6383H-6XYWF
Windows 11 Pro для образовательных учреждений Windows 10 Pro для образовательных учреждений	6TP4R-GNPTD-KYYHQ-7B7DP-J447Y

Версия операционной системы	Ключ продукта клиента KMS
Windows 11 Pro для образовательных учреждений N Windows 10 Pro для образовательных учреждений N	YVWGF-BXNMC-HTQYQ-CPQ99-66QFC
Windows 11 для образовательных учреждений Windows 10 для образовательных учреждений	NW6C2-QMPVW-D7KKK-3GKT6-VCFB2
Windows 11 для образовательных учреждений N Windows 10 для образовательных учреждений N	2WH4N-8QGBV-H22JP-CT43Q-MDWWJ
Windows 11 Корпоративная Windows 10 Корпоративная	NPPR9-FWDCX-D2C8J-H872K-2YT43
Windows 11 Корпоративная N Windows 10 Корпоративная N	DPH2V-TTNVB-4X9Q3-TJR4H-KHJW4
Windows 11 Корпоративная G Windows 10 Корпоративная G	YYVX9-NTFWV-6MDM3-9PT4T-4M68B
Windows 11 Корпоративная G N Windows 10 Корпоративная G N	44RPN-FTY23-9VTTB-MP9BX-T84FV

Windows 10 (версии LTSC и LTSB)

Windows 10 LTSC 2021 и 2019

Версия операционной системы	Ключ продукта клиента KMS
Windows 10 Корпоративная LTSC 2021 Windows 10 Корпоративная LTSC 2019	M7XTQ-FN8P6-TTKYV-9D4CC-J462D
Windows 10 Корпоративная N LTSC 2021 Windows 10 Корпоративная N LTSC 2019	92NFX-8DJQP-P6BBQ-THF9C-7CG2H

Windows 10 LTSB 2016

Версия операционной системы	Ключ продукта клиента KMS
Windows 10 Корпоративная LTSB 2016	DCPHK-NFMTC-H88MJ-PFHPY-QJ4BJ
Windows 10 Корпоративная N LTSB 2016	QFFDN-GRT3P-VKWWX-X7T3R-8B639

Windows 10 LTSB 2015

Версия операционной системы	Ключ продукта клиента KMS
Windows 10 Корпоративная 2015 с долгосрочным обслуживанием	WNMTR-4C88C-JK8YV-HQ7T2-76DF9
Windows 10 Корпоративная 2015 с долгосрочным обслуживанием N	2F77B-TNFGY-69QQF-B8YKP-D69TJ

Предшествующие версии Windows Server

Windows Server версии 1803

Версия операционной системы	Ключ продукта клиента KMS
Windows Server Datacenter	2HXDN-KRXHB-GPYC7-YCKFJ-7FVDG
Windows Server Standard	PTXN8-JFHJM-4WC78-MPCBR-9W4KR

Windows Server версии 1709

Версия операционной системы	Ключ продукта клиента KMS
Windows Server Datacenter	6Y6KB-N82V8-D8CQV-23MJW-BWTG6
Windows Server Standard	DPCNP-XQFKJ-BJF7R-FRC8D-GF6G4

Windows Server 2012 R2

Версия операционной системы	Ключ продукта клиента KMS
Windows Server 2012 R2 Standard	D2N9P-3P6X9-2R39C-7RTCD-MDVJX
Windows Server 2012 R2 Datacenter	W3GGN-FT8W3-Y4M27-J84CP-Q3VJ9
Windows Server 2012 R2 Essentials	KNC87-3J2TX-XB4WP-VCPJV-M4FWM

Windows Server 2012

Версия операционной системы	Ключ продукта клиента KMS
Windows Server 2012	BN3D2-R7TKB-3YPBD-8DRP2-27GG4
Windows Server 2012 N	8N2M2-HWPGY-7PGT9-HGDD8-GVGGY

Версия операционной системы	Ключ продукта клиента KMS
Windows Server 2012 для одного языка	2WN2H-YGCQR-KFX6K-CD6TF-84YXQ
Windows Server 2012 для конкретной страны	4K36P-JN4VD-GDC6V-KDT89-DYFKP
Windows Server 2012 Standard	XC9B7-NBPP2-83J2H-RHMBY-92BT4
Windows Server 2012 MultiPoint Standard	HM7DN-YVMH3-46JC3-XYTG7-CYQJJ
Windows Server 2012 MultiPoint Premium	XNH6W-2V9GX-RGJ4K-Y8X6F-QGJ2G
Windows Server 2012 Datacenter	48HP8-DN98B-MYWDG-T2DCC-8W83P

Windows Server 2008 R2

Версия операционной системы	Ключ продукта клиента KMS
Windows Server 2008 R2 Web	6TPJF-RBVHG-WBW2R-86QPH-6RTM4
Windows Server 2008 R2 HPC Edition	TT8MH-CG224-D3D7Q-498W2-9QCTX
Windows Server 2008 R2 Standard	YC6KT-GKW9T-YTKYR-T4X34-R7VHC
Windows Server 2008 R2 Enterprise	489J6-VHDMP-X63PK-3K798-CPX3Y
Windows Server 2008 R2 Datacenter	74YFP-3QFB3-KQT8W-PMXWJ-7M648
Windows Server 2008 R2 for Itanium-based Systems	GT63C-RJFQ3-4GMB6-BRFB9-CB83V

Windows Server 2008

Версия операционной системы	Ключ продукта клиента KMS
Windows Web Server 2008	WYR28-R7TFJ-3X2YQ-YCY4H-M249D
Windows Server 2008 Standard	TM24T-X9RMF-VWXK6-X8JC9-BFGM2
Windows Server 2008 Standard без Hyper-V	W7VD6-7JFBR-RX26B-YKQ3Y-6FFFJ
Windows Server 2008 Enterprise	YQGMW-MPWTJ-34KDK-48M3W-X4Q6V
Windows Server 2008 Enterprise без Hyper-V	39BXF-X8Q23-P2WWT-38T2F-G3FPG
Windows Server 2008 HPC	RCTX3-KWVHP-BR6TB-RB6DM-6X7HP

Версия операционной системы	Ключ продукта клиента KMS
Windows Server 2008 Datacenter	7M67G-PC374-GR742-YH8V4-TCBY3
Windows Server 2008 Datacenter без Hyper-V	22XQ2-VRXRG-P8D42-K34TD-G3QQC
Windows Server 2008 для систем на базе процессоров Itanium	4DWFP-JF3DJ-B7DTH-78FJB-PDRHK

Предшествующие версии Windows

Windows 8.1

Версия операционной системы	Ключ продукта клиента KMS
Windows 8.1 Профессиональная	GCRJD-8NW9H-F2CDX-CCM8D-9D6T9
Windows 8.1 Pro N	HMCNV-VVBFX-7HMBH-CTY9B-B4FXY
Windows 8.1 Корпоративная	MHF9N-XY6XB-WVXMC-BTDCT-MKKG7
Windows 8.1 Корпоративная N	TT4HM-HN7YT-62K67-RGRQJ-JFFXW

Windows 8

Версия операционной системы	Ключ продукта клиента KMS
Windows 8 Профессиональная	NG4HW-VH26C-733KW-K6F98-J8CK4
Windows 8 Pro N	XCVCF-2NXM9-723PB-MHCB7-2RYQQ
Windows 8 Корпоративная	32JNW-9KQ84-P47T8-D8GGY-CWCK7
Windows 8 Корпоративная N	JMNMF-RHW7P-DMY6X-RF3DR-X2BQT

Windows 7

Версия операционной системы	Ключ продукта клиента KMS
Windows 7 Профессиональная	FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4
Windows 7 Профессиональная N	MRPKT-YTG23-K7D7T-X2JMM-QY7MG
Windows 7 Профессиональная E	W82YF-2Q76Y-63HXB-FGJG9-GF7QX

Версия операционной системы	Ключ продукта клиента KMS
Windows 7 Корпоративная	33PXH-7Y6KF-2VJC9-XBBR8-HVTHH
Windows 7 Корпоративная N	YDRBP-3D83W-TY26F-D46B2-XCKRJ
Windows 7 Корпоративная E	C29WB-22CC8-VJ326-GHFJW-H9DH4

Windows Vista

Версия операционной системы	Ключ продукта клиента KMS
Windows Vista Business	YFKBB-PQJJV-G996G-VWGXY-2V3X8
Windows Vista Business N	HMBQG-8H2RH-C77VX-27R82-VMQBT
Windows Vista Enterprise	VKK3X-68KWM-X2YGT-QR4M6-4BWMV
Windows Vista Enterprise N	VTC42-BM838-43QHV-84HX6-XJXKV

Сведения о том, как получить дополнительные обновления для системы безопасности (ESU) для Windows Server

Статья • 28.01.2023 • Чтение занимает 6 мин

Дополнительные обновления для системы безопасности Windows Server содержат обновления для системы безопасности и бюллетени с оценкой *критические* и *важные*. Прежде чем использовать дополнительные обновления для системы безопасности, ознакомьтесь со статьей Общие сведения о дополнительных обновлениях для системы безопасности Windows Server, поскольку в ней содержатся сведения о том, что такое дополнительные обновления для системы безопасности, как долго они будут доступны и какие варианты вы имеете.

Способ получения дополнительных обновлений для системы безопасности зависит от того, где размещается сервер. Соответствующие виртуальные машины (ВМ), размещенные в Azure, будут автоматически и к тому же бесплатно получать дополнительные обновления для системы безопасности.

Для других сред, таких как локальные виртуальные машины или физические серверы, дополнительные обновления для системы безопасности необходимо запросить и настроить вручную. Вы можете приобрести дополнительные обновления для системы безопасности, в рамках программ корпоративного лицензирования, таких как Соглашение Enterprise (EA), подписка с Соглашением Enterprise (EAS), Enrollment for Education Solutions (EES) или Server and Cloud Enrollment (SCE).

Чтобы использовать дополнительные обновления для системы безопасности на виртуальных машинах, не относящихся к Azure, необходимо создать ключ многократной активации (MAK) и применить его к соответствующим серверам с Windows Server. Этот ключ MAK позволяет серверам Центра обновления Windows понять, что вы можете продолжать принимать обновления для системы безопасности.

> ⓘ **Примечание**
>
> После приобретения расширенных обновлений безопасности для локальных виртуальных машин или физических серверов ключ множественной активации станет доступен в течение 3–5 рабочих дней. Вашей организации

также может потребоваться время для планирования и развертывания новых ключей. При приобретении расширенных обновлений для системы безопасности, следует учитывать эти сроки.

Виртуальные машины Azure

Соответствующие виртуальные машины (ВМ), размещенные в Azure, будут автоматически и к тому же бесплатно получать дополнительные обновления для системы безопасности. Вам не нужно ничего настраивать, и дополнительная плата за использование для виртуальных машин Azure дополнительных обновлений для системы безопасности не взимается. Дополнительные обновления для системы безопасности автоматически доставляются на виртуальные машины Azure, если они настроены для получения обновлений.

> ⓘ **Примечание**
>
> Классические виртуальные машины Azure (Microsoft.ClassicCompute) требуют дополнительной настройки для получения обновлений расширенной системы безопасности, так как у них нет доступа к **службе метаданных экземпляров Azure**, которая определяет возможность установки обновлений расширенной системы безопасности. Сюда входят другие продукты Azure, такие как Выделенный узел Azure, Решение Azure VMWare, решение Azure Nutanix и Azure Stack (Hub, Edge и HCI). Обратитесь за помощью в **службу поддержки Майкрософт**.

Зарегистрируйтесь для получения дополнительных обновлений для системы безопасности для серверов, не относящихся к Azure, и получите ключ многократной активации

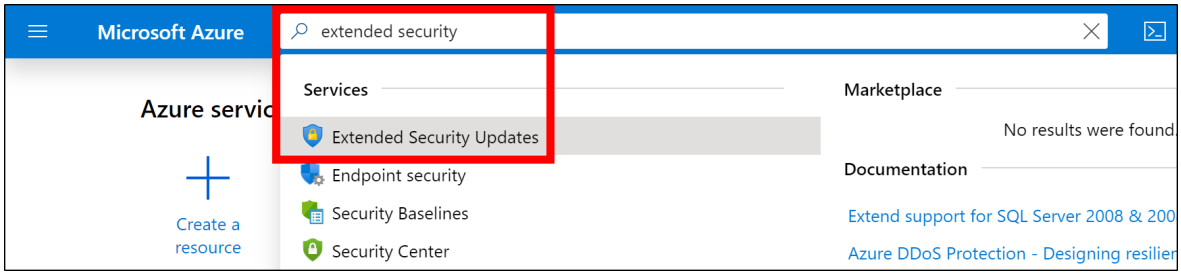
Приобретя дополнительные обновления для системы безопасности, зарегистрируйте сначала покупку на портале Azure, чтобы получить ключ многократной активации. Регистрация для получения дополнительных обновлений для системы безопасности выполняется с помощью портала Azure, даже если вы используете только локальные компьютеры.

> **Примечание**
>
> Если вы используете Windows Server на виртуальных машинах Azure, регистрироваться для получения дополнительных обновлений для системы безопасности не нужно, поскольку они предоставляются по умолчанию и совершенно бесплатно. Прежде чем пытаться зарегистрироваться для получения дополнительных обновлений для системы безопасности и использовать их для других сред, таких как локальные виртуальные машины или физические серверы, **сначала необходимо приобрести эти обновления**.

Чтобы зарегистрировать сервер для получения дополнительных обновлений для системы безопасности и создать ключ, откройте портал Azure и выполните следующие действия:

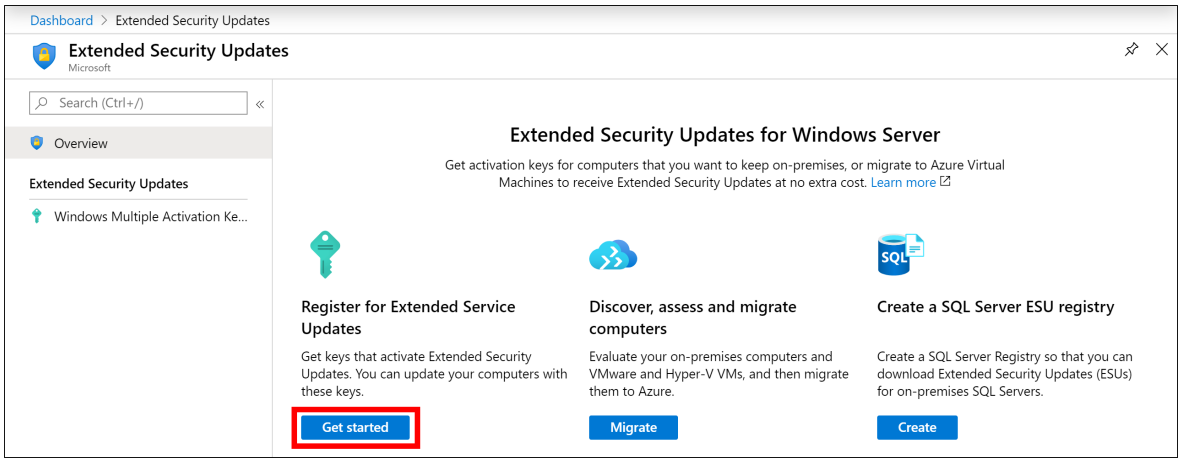
1. Войдите на портал Azure.

2. В поле поиска в верхней части портала Azure найдите и выберите **Extended Security Updates** (Дополнительные обновления для системы безопасности).

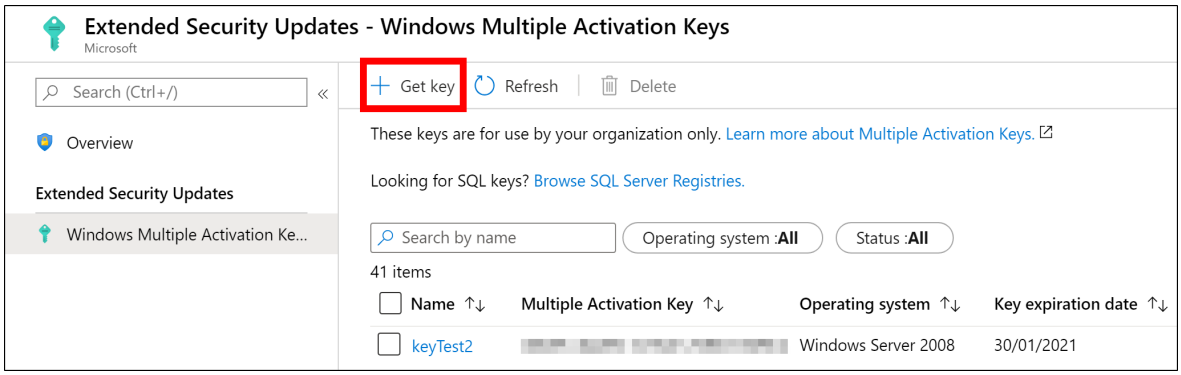


   Если вы еще не использовали дополнительные обновления для системы безопасности, то сначала выберите + **Create** (Создать), чтобы создать ресурс дополнительного обновления безопасности. В противном случае выберите ресурс из списка.

3. В разделе **Register for Extended Service Updates** (Регистрация на получение дополнительных обновлений служб) выберите **Начало работы**.



4. Чтобы создать первый ключ, выберите **Получить ключ**.



Для создания ресурса и ключа дополнительных обновлений безопасности требуется подписка Azure, связанная с вашей учетной записью. Если у вас нет подписки Azure, связанной с вашей учетной записью, выполните вход с помощью другой учетной записи пользователя или создайте подписку Azure на портале Azure.

Для работы обновления для системы безопасности в подписке Azure также должна быть назначена роль участника. Чтобы проверить роль, введите в поле поиска "Подписки". Вы увидите таблицу, в которой будет показано вашу роль рядом с идентификатором и именем подписки.

Если вы не являетесь участником, попросите владельца подписки изменить вашу роль. Чтобы узнать, кто владеет подпиской, перейдите к таблице роли, описанной в предыдущем абзаце, и выберите имя своей подписки. Затем перейдите в меню в левой части страницы и выберите **Управление доступом (IAM)** > **Назначения ролей** и найдите раздел **Владельцы** в таблице.

5. Если отображается страница с заголовком **Register to get a Multiple Activation Key** (Зарегистрируйтесь для получения ключа многократной активации), для использования дополнительных обновлений для системы безопасности необходимо сначала запросить доступ к предварительной версии. Если эта страница не отображается, перейдите к шагу 6.

Чтобы запросить доступ, выберите **join the private preview** (Присоединиться к предварительной версии). Откроется окно сообщения электронной почты. Этот адрес электронной почты является вашим запросом на доступ к команде разработчиков Майкрософт.

Включите в запрос следующие сведения:

- имя пользователя;
- идентификатор подписки Azure;
- номер соглашения (для ESU);
- количество серверов ESU.

Когда все будет готово, отправьте сообщение электронной почты.

Команда будет просматривать сведения, указанные в сообщении с запросом. Если все нормально, они добавят вас в список утвержденных лиц.

Если команда не утвердит ваш запрос, вы увидите следующую ошибку:

```
The resource type could not be found in the namespace
'Microsoft.WindowsESU'
```

6. В разделе **Сведения об Azure** выберите подписку Azure, группу ресурсов и расположение для своего ключа.

   В разделе **Сведения о регистрации** введите следующие сведения:

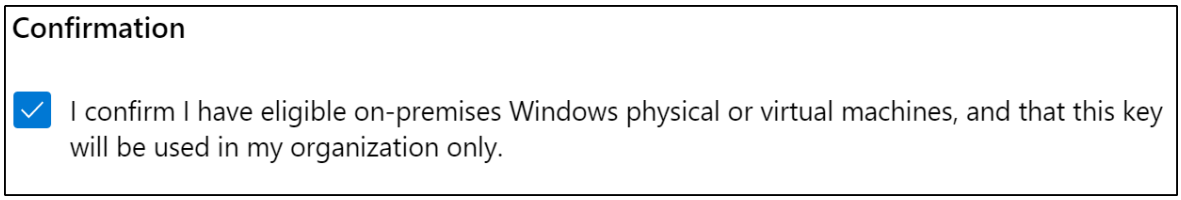
Параметр	**Применение**
Имя ключа	Отображаемое имя ключа, например `Agreement01`.
Номер соглашения	Номер соглашения, созданный системой управления контрактами корпоративного лицензирования, или MSLicense для программ по соглашениям Enterprise.
Количество компьютеров	Выберите количество компьютеров, на которых требуется установить дополнительные обновления для системы безопасности с помощью этого ключа.
Операционная система	Выберите операционную систему, с которой следует использовать этот ключ, например Windows Server 2008 R2.

   Когда все будет готово, выберите **Review + register** (Проверить и зарегистрироваться).

> **Примечание**
>
> Убедитесь, что выбрали подписку Azure, с помощью которой вы присоединились к предварительной версии, используя глобальный фильтр. Выберите кнопку **Фильтр** на ленте портала Azure, чтобы проверить ваш фильтр глобальных подписок.
>
> 

7. После успешной проверки отображается сводка по выбранному для нового ресурса реестра. При необходимости исправьте все найденные ошибки или измените свои варианты конфигурации. Для Azure доступны Условия использования и Политика конфиденциальности.

   Установите флажок, чтобы подтвердить, что у вас есть соответствующие компьютеры, и ключ должен использоваться только в вашей организации:

   Когда все будет готово, выберите команду **Создать**, чтобы создать ключ многократной активации.

Теперь регистрация для получения дополнительных обновлений безопасности доступна для использования с вашими серверами. Созданный ключ должен применяться на серверах под управлением Windows Server 2008 и 2008 R2, на которых понадобятся обновления безопасности.

Получение доступа к ключу многократной активации на сайте Volume Licensing Service Center

Успешно зарегистрировав и создав ключ многократной активации, вы можете просмотреть и скачать его с помощью Volume Licensing Service Center.

Чтобы получить ключ из Volume Licensing Service Center, сделайте следующее.

1. Перейдите на страницу Volume Licensing Service Center и выполните вход с помощью учетных данных Azure.

2. Выберите **Лицензии**>**Сводка связей**>**Номер лицензии**>**Ключи продуктов**.

Загрузка и применение дополнительных обновлений для системы безопасности

Доставка, скачивание и применение дополнительных обновлений для системы безопасности Windows Server такие же, как и для других обновлений Windows. Однако они предоставляются только для *системы безопасности*.

Эти обновления можно установить с помощью любых уже существующих средств и процессов. Единственное отличие заключается в том, что система должна быть зарегистрирована с использованием ключа, созданного в предыдущем разделе, для загрузки и установки обновлений.

Для виртуальных машин, размещенных в Azure, процесс активации сервера для получения дополнительных обновлений для системы безопасности выполняется автоматически. Обновления должны загружаться и устанавливаться без дополнительной настройки.

Дополнительные сведения см. в записи блога Tech Community, посвященной получению дополнительных обновлений для системы безопасности для соответствующих требованиям устройств Windows.

Включение горячего исправления для виртуальных машин Azure Edition Server Core, созданных на основе ISO (предварительная версия)

Статья • 28.01.2023 • Чтение занимает 2 мин

> ⓘ **Важно!**
>
> - Горячее исправление для виртуальных машин Azure Edition Server Core, созданных на основе ISO, в настоящее время доступно в предварительной версии. Эти сведения относятся к предварительной версии продукта, который может быть существенно изменен перед выпуском. Корпорация Майкрософт не дает никаких гарантий, явных или подразумеваемых, в отношении предоставленной здесь информации.
> - Эта статья применяется только при развертывании Windows Server Datacenter: Azure Edition Server Core из ISO-образа. Он не применяется при развертывании с помощью Azure Marketplace.

Горячее исправление для Windows Server 2022 Datacenter: Azure Edition Server Core позволяет устанавливать обновления для системы безопасности без необходимости перезагрузки после установки. В этой статье описано, как настроить Hotpatch после установки или обновления операционной системы с помощью ISO.

При использовании Hotpatch для компьютера, развернутого по ISO в Azure Stack HCI, существует несколько важных отличий от функции Hotpatch по сравнению с использованием Hotpatch в рамках автоматического управления Azure для виртуальных машин Azure.

Ниже описаны различия.

- Конфигурация горячего исправления недоступна в Диспетчере обновлений Azure.
- Не удается отключить горячее исправление.
- Автоматическая оркестрация исправлений недоступна.
- Оркестрация должна выполняться вручную (например, с помощью клиентский компонент Центра обновления Windows через SConfig).

Предварительные требования

Чтобы включить hotpatch, перед началом работы необходимо выполнить следующие предварительные требования.

- Windows Server 2022 Datacenter: Azure Edition Server Core, размещенный на поддерживаемой платформе, такой как Azure или Azure Stack HCI с включенными преимуществами Azure.
  - Azure Stack HCI должна иметь версию 21H2 или более позднюю.
- Ознакомьтесь с разделом Как работает hotpatch статьи Hotpatch для новых виртуальных машин.
- Исходящий сетевой доступ или правило исходящего порта, разрешающее трафик HTTPS (TCP/443) к следующим конечным точкам:
  - `go.microsoft.com`
  - `software-static.download.prss.microsoft.com`

Подготовка компьютера

Прежде чем включить горячее исправление для виртуальной машины, необходимо подготовить компьютер, выполнив следующие действия.

1. Войдите на компьютер. В меню SConfig введите параметр **15**, а затем нажмите клавишу ввод, чтобы открыть сеанс PowerShell.

2. Включите безопасность на основе виртуализации, выполнив следующую команду PowerShell, чтобы настроить правильные параметры реестра:

   PowerShell

   ```
   $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard"
   $parameters = $parameters = @{
       Path = $registryPath
       Name = "EnableVirtualizationBasedSecurity"
       Value = "0x1"
       Force = $True
   }
   New-Item $registryPath -Force
   New-ItemProperty @parameters
   ```

3. Настройте размер таблицы Hotpatch в реестре, выполнив следующую команду PowerShell:

   PowerShell

```
$registryPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Session
Manager\Memory Management"
$parameters = $parameters = @{
    Path = $registryPath
    Name = "HotPatchTableSize"
    Value = "0x1000"
    Force = $True
}
New-Item $registryPath -Force
New-ItemProperty @parameters
```

4. Настройте конечную точку клиентский компонент Центра обновления Windows для hotpatch в реестре, выполнив следующую команду PowerShell:

PowerShell

```
$registryPath = "HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Update\TargetingInfo\DynamicInstalled\Hotpatch.amd64"
$nameParameters = $parameters = @{
    Path = $registryPath
    Name = "Name"
    Value = "Hotpatch Enrollment Package"
    Force = $True
}
$versionParameters = $parameters = @{
    Path = $registryPath
    Name = "Version"
    Value = "10.0.20348.465"
    Force = $True
}
New-Item $registryPath -Force
New-ItemProperty @nameParameters
New-ItemProperty @versionParameters
```

Теперь вы подготовили компьютер и можете установить пакет обслуживания hotpatch.

Установка пакета обслуживания hotpatch

> ⓘ **Примечание**
>
> База знаний, необходимых для горячего исправления, в настоящее время не опубликована в каталоге Центра обновления Майкрософт.

Чтобы получать обновления hotpatch, необходимо скачать и установить пакет обслуживания Hotpatch. В сеансе PowerShell выполните следующие действия.

1. Скачайте автономный пакет (KB5003508) Центра обновления Майкрософт из каталога Центра обновления Майкрософт и скопируйте его на компьютер с помощью следующей команды PowerShell:

   PowerShell

   ```
   $parameters = @{
       Uri = "https://go.microsoft.com/fwlink/?linkid=2211714"
       OutFile = ".\KB5003508.msu"
   }
   Invoke-WebRequest @parameters
   ```

2. Чтобы установить автономный пакет, выполните следующую команду:

   PowerShell

   ```
   wusa.exe .\KB5003508.msu
   ```

3. Следуйте инструкциям. После завершения нажмите кнопку Готово.

4. Чтобы проверить установку, выполните следующую команду:

   PowerShell

   ```
   Get-HotFix | Where-Object {$_.HotFixID -eq "KB5003508"}
   ```

> ⓘ **Примечание**
>
> При использовании основных серверных компонентов обновления устанавливаются вручную по умолчанию. Этот параметр можно изменить с помощью служебной программы SConfig.

Дальнейшие действия

Теперь вы настроили компьютер для горячего исправления. Ниже приведены некоторые статьи, которые могут помочь вам в обновлении компьютера:

- Исправление установки основных серверных компонентов.
- Дополнительные сведения о Windows Server Update Services (WSUS).

Обновление Windows Server на месте

Статья • 28.01.2023 • Чтение занимает 3 мин

При обновлении на месте вы переходите с более старой версии операционной системы на более новую, сохраняя свои параметры, роли сервера и данные. Из этой статьи вы узнаете, как перейти на более позднюю версию Windows Server путем обновления на месте.

> ⓘ **Важно!**
>
> Хотите выполнить обновление windows Server на месте, работающего на виртуальной машине Azure? См. **раздел Обновление на месте для виртуальных машин под управлением Windows Server в Azure**.

Предварительные требования

Прежде чем начать обновление, обеспечьте соответствие компьютера следующим требованиям:

- Определите, до какой версии нужно обновить Windows Server.
- Оборудование соответствует требованиям к оборудованию для Windows Server или превышает их.
- Не должен выполняться в Azure.
- Установочный носитель готов к использованию.
- Доступны действительный ключ продукта и метод активации. Ключи и методы могут зависеть от канала распространения, из которого вы получили носитель Windows Server, например от программы коммерческого лицензирования, канала розничной торговли, изготовителя оборудования (OEM) и т. д.
- Необходимо установить PowerShell 5.1 или более поздней версии.
- Расположение для хранения файлов вне компьютера (например, USB-устройство флэш-памяти или расположение в сети).
- Просмотрите статью Обновление и перенос ролей и компонентов в Windows Server.
- Просмотрите статью Совместимость серверных приложений Майкрософт.
- Просмотрите требования, касающиеся поддержки сторонних поставщиков приложений.

Сбор диагностических сведений

Рекомендуем выполнить сбор данных с устройств для диагностики и устранения неполадок в том случае, если обновление не удастся выполнить. Кроме того, мы рекомендуем хранить сведения в расположении, к которому вы можете получить доступ, даже если устройство недоступно.

Сбор информации:

1. Откройте командную строку PowerShell с повышенными привилегиями, запишите текущий каталог и выполните следующие команды.

   PowerShell

   ```
   Get-ComputerInfo -Property WindowsBuildLabEx,WindowsEditionID | Out-File -FilePath .\computerinfo.txt
   systeminfo.exe | Out-File -FilePath systeminfo.txt
   ipconfig /all | Out-File -FilePath ipconfig.txt
   ```

2. Используя **проводник**, перейдите к каталогу, который вы записали, и **скопируйте** файлы с компьютера на USB-устройство флэш-памяти или в расположение в сети.

> **Совет**
>
> Get-ComputerInfo требуется PowerShell 5.1 или более поздней версии. Если ваша версия Windows Server не включает PowerShell, эти сведения можно найти в реестре. Откройте редактор реестра, перейдите к разделу **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion**, а затем скопируйте и вставьте значения **BuildLabEx** и **EditionID** для Windows Server.

После получения всех данных, относящихся к Windows Server, мы рекомендуем создать резервную копию операционной системы сервера, приложений и виртуальных машин. Кроме того, необходимо завершить работу, а также выполнить быстрый или динамический перенос всех виртуальных машин, выполняющихся в данный момент на сервере. Во время обновления на месте виртуальные машины не могут работать.

выполнение обновления.

Теперь, когда вы выполнили предварительные требования и собрали диагностические сведения, можно переходить к обновлению. При работе с этим разделом вы будете использовать программу установки Windows Server для

выбора параметров для обновления. Программа установки Windows Server будет использовать эти параметры для обновления версии Windows Server, во время которого ваш компьютер перезагрузится несколько раз.

Обновление на месте:

1. С помощью **проводника** перейдите к носителю для установки Windows Server. Затем откройте **setup.exe**. Например, если вы используете носитель для удаления, путь к файлу может быть *D:\setup.exe*.

   > ⓘ **Важно!**
   >
   > В зависимости от параметров безопасности от функции контроля учетных записей может поступить запрос на разрешение на внесение программой установки изменений на устройство. Если вы готовы продолжить, выберите ответ **Да**.

2. По умолчанию программа установки автоматически скачивает обновления для установки. Если вам подходят параметры по умолчанию, чтобы продолжить, нажмите кнопку **Далее**.

   Если вы не хотите, чтобы программа установки автоматически загружала обновления:

   - Выберите элемент **Изменить способ скачивания обновлений программой установки**, выберите соответствующий вариант для своей среды, а затем нажмите кнопку **Далее**.

3. При появлении запроса введите ключ продукта, а затем нажмите кнопку **Далее**.

4. Выберите выпуск Windows Server, который хотите установить, а затем нажмите кнопку **Далее**.

5. Просмотрите применимые уведомления и условия лицензии. Если вы принимаете условия, нажмите кнопку **Принять**.

6. Выберите элемент **Сохранить личные файлы и приложения**, чтобы выполнить обновление на месте, а затем нажмите кнопку **Далее**.

7. После анализа устройства в программе установки отобразится экран "Готово к установке". Чтобы продолжить обновление, нажмите кнопку **Установить**.

Начнется обновление на месте, и отобразится индикатор выполнения. После завершения обновления сервер перезапустится.

Проверка успешности обновления

После обновления до Windows Server необходимо убедиться, что оно прошло успешно.

Проверка успешности обновления:

1. Откройте командную строку PowerShell с повышенными привилегиями. Затем выполните следующую команду, чтобы убедиться, что версия и выпуск соответствуют носителю и значениям, выбранным во время установки.

   ```
   PowerShell

   Get-ComputerInfo -Property WindowsProductName
   ```

2. Убедитесь, что все приложения работают, и что подключения клиентов к приложениям выполняются успешно.

Если после обновления компьютер не работает должным образом, обратитесь в службу поддержки Майкрософт для получения технической помощи.

Дальнейшие действия

Теперь, когда вы обновили Windows Server, ознакомьтесь со следующими статьями, которые могут помочь вам при использовании новой версии:

- Установка и удаление ролей, служб ролей и компонентов
- Общие сведения об управлении Windows Server
- Начало работы с Windows Admin Center
- Планирование активации на основе службы управления ключами (KMS)
- Активация с помощью Active Directory

Если вы хотите больше узнать о развертывании, настройке после установки и вариантах активации, ознакомьтесь со схемой обучения, посвященной развертыванию, настройке и администрированию Windows Server.

Устранение неполадок с активацией корпоративных лицензий Windows

Статья • 28.01.2023 • Чтение занимает 2 мин

Активация продукта — это проверка программного обеспечения после того, как оно было установлено на конкретном компьютере. Активация подтверждает, что продукт является подлинной копией и что ключ или серийный номер продукта действительны и не были скомпрометированы или аннулированы. Активация также устанавливает связь между ключом продукта и установленной копией.

Активация корпоративных лицензий — это процесс активации продуктов с корпоративной лицензией. Чтобы иметь возможность выполнять корпоративное лицензирование, организации необходимо заключить с корпорацией Майкрософт соглашение о корпоративном лицензировании. Корпорация Майкрософт предлагает программы корпоративного лицензирования, соответствующие размеру и покупательским предпочтениям организации. Дополнительные сведения см. на веб-сайте Microsoft Volume Licensing Service Center.

Руководство по активации Windows Server 2016 преимущественно посвящено технологии активации с помощью службы управления ключами (KMS). В этом разделе рассматриваются распространенные проблемы, а также рекомендации по устранению неполадок KMS и ряда других технологий активации корпоративных лицензий.

Рекомендации оп активации корпоративных лицензий

В следующих статьях содержатся технические сведения и рекомендации по технологиям активации корпоративных лицензий корпорации Майкрософт.

Служба управления ключами (KMS).

- Планирование активации корпоративных лицензий
- Общие сведения о KMS
- Развертывание активации KMS
- Настройка узлов KMS
- Настройка DNS
- Активация с помощью службы управления ключами

Активация с помощью Active Directory (ADBA)

- Развертывание активации с помощью Active Directory
- Активация с помощью Active Directory
- Общие сведения об активации с помощью Active Directory

Активация с помощью ключей многократной активации (MAK)

- Активация с помощью MAK
- Общие сведения об активации с помощью MAK
- Активация клиентов MAK

Активация подписки

- Активация подписки Windows 10
- Развертывание лицензий Windows 10 Корпоративная
- Windows 10 Корпоративная E3 в CSP

Материалы по устранению проблем с активацией

В следующих статьях приводятся рекомендации и сведения о средствах устранения неполадок, связанных с активацией корпоративных лицензий.

- Рекомендации по устранению неполадок службы управления ключами (KMS)
- Параметры Slmgr.vbs для получения сведений об активации корпоративных лицензий
- Пример. Устранение неполадок клиентов ADBA, которые не активируются

В следующих статьях приведены рекомендации по устранению конкретных проблем с активацией.

- Разрешение распространенных кодов ошибок активации
- Активация KMS: известные проблемы
- Активация MAK: известные проблемы
- Рекомендации по устранению проблем с активацией, связанных с DNS
- Как перестроить файл Tokens.dat

Рекомендации по устранению неполадок службы управления ключами (KMS)

Статья • 28.01.2023 • Чтение занимает 12 мин

В процессе развертывания многие корпоративные клиенты настраивают службу управления ключами (KMS), чтобы включить активацию Windows в своей среде. Это простой процесс настройки узла KMS, после завершения которого клиенты KMS обнаруживают узел и пытаются выполнить активацию самостоятельно. Но что произойдет, если этот процесс не заработает? Что делать дальше? В этой статье описываются ресурсы, необходимые для устранения проблемы. Дополнительные сведения о записях журнала событий и сценарии Slmgr.vbs см. в техническом справочнике по активации корпоративных лицензий.

Общие сведения о KMS

Начнем с быстрого повторения материала об активации KMS. Служба KMS использует модель "клиент — сервер". По сути, она напоминает DHCP. Вместо передачи IP-адресов клиентам по их запросу KMS обеспечивает активацию продукта. Служба KMS также использует модель продления, в которой клиенты пытаются выполнить повторную активацию через равные промежутки времени. Существуют две роли: узел *KMS* и клиент *KMS*.

- На **узле KMS** работает служба активации. Именно он обеспечивает активацию в среде. Чтобы настроить узел KMS, необходимо установить ключ KMS из центра поддержки корпоративных лицензий (VLSC), а затем активировать службу.
- **Клиент KMS** — это операционная система Windows, которая развернута в среде и должна быть активирована. Клиенты KMS могут работать под управлением любого выпуска Windows, использующего активацию корпоративных лицензий. Клиенты KMS поставляются с предварительно установленным ключом, который называется универсальным ключом многократной установки (GVLK) или ключом установки клиента KMS. Наличие GVLK означает, что данная система — клиент KMS. Клиенты KMS используют записи SRV DNS (_vlmcs._tcp) для определения узла KMS. Затем клиенты автоматически пытаются обнаружить и использовать эту службу для самостоятельной активации. В течение 30-дневного льготного периода они

пытаются выполнить активацию каждые два часа. После активации клиенты KMS пытаются продлевать активацию каждые семь дней.

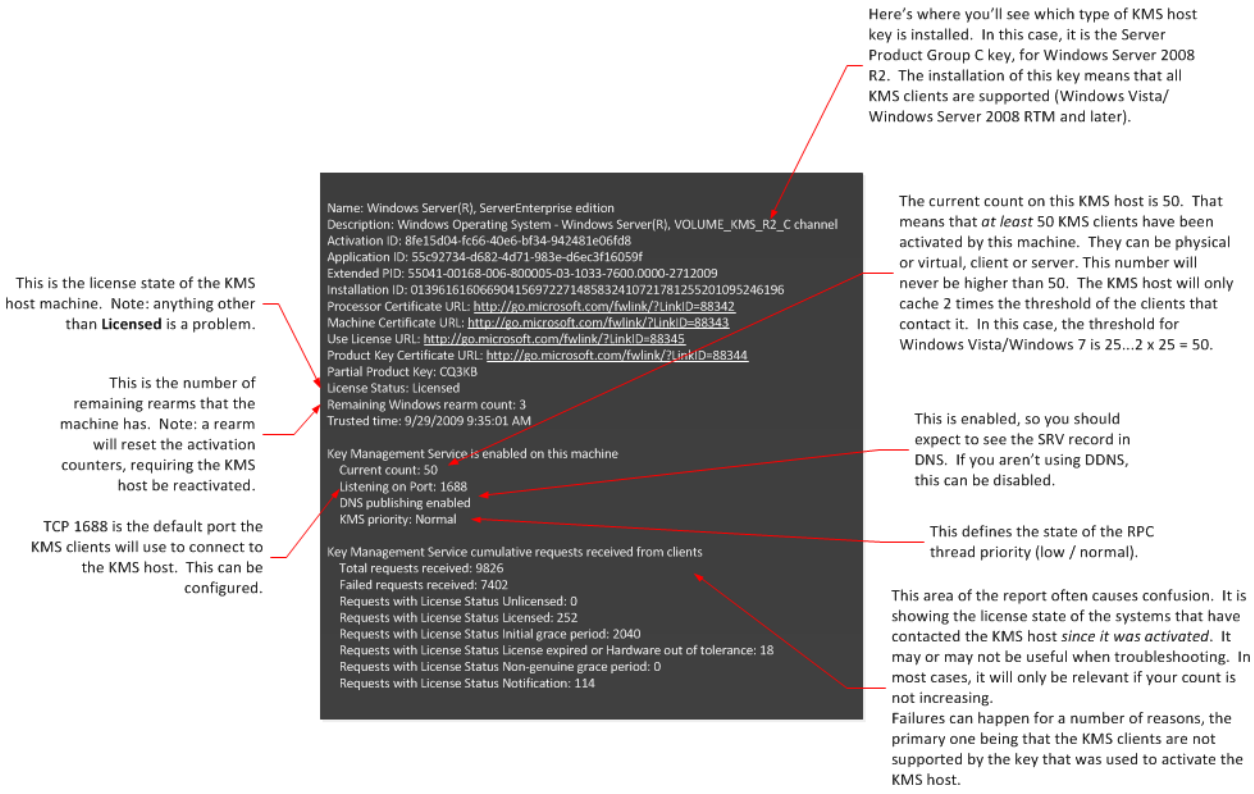
При устранении неполадок, возможно, придется рассмотреть обе стороны (узел и клиент), чтобы выяснить, что происходит.

Узел KMS

Существуют две области, которые необходимо изучить на узле KMS. Сначала проверьте состояние службы лицензий на программное обеспечение узла. Во вторых, с помощью Просмотра событий проверьте наличие событий, связанных с лицензированием или активацией.

Сценарий Slmgr.vbs и служба лицензий на программное обеспечение

Чтобы просмотреть подробные выходные данные службы лицензий на программное обеспечение, откройте окно командной строки с повышенными привилегиями и введите в нем **slmgr.vbs/dlv**. На следующем снимке экрана показаны результаты выполнения этой команды на одном из узлов KMS в корпорации Майкрософт.



Ниже приведены наиболее важные поля для устранения неполадок. Искомые сведения могут быть разными в зависимости от устраняемой проблемы.

- **Сведения о версии**. В верхней части файла выходных данных **slmgr.vbs/dlv** указана версия службы лицензий на программное обеспечение. Она может быть полезна для того, чтобы узнать, установлена ли актуальная версия службы. Например, обновления для службы KMS в Windows Server 2003 поддерживают разные ключи узла KMS. Эти данные можно использовать, чтобы оценить, является ли версия актуальной и поддерживает ли она ключ узла KMS, который вы пытаетесь установить. Дополнительные сведения об этих обновлениях см. в разделе Обновление для Windows Vista и Windows Server 2008 для KMS-активации расширения поддержки для Windows 7 и Windows Server 2008 R2.

- **Имя**. Указывает выпуск Windows, установленный в системе узла KMS. Это может быть важно для устранения проблем с добавлением или изменением ключа узла KMS (например, чтобы убедиться, что этот ключ поддерживается в текущем выпуске ОС).

- **Описание**. Здесь отображается установленный ключ. Используйте это поле, чтобы проверить, какой ключ использован для активации службы и подходит ли он для развернутых клиентов KMS.

- **License Status** (Состояние лицензии). Это состояние системы узла KMS. Значение должно быть **Лицензировано**. Любое другое значение означает, что произошла ошибка и может потребоваться повторная активация узла.

- **Current Count** (Текущее количество). Отображаемое число будет находиться в диапазоне от **0** до **50**. Счетчик является накопительным для нескольких операционных систем. Он указывает количество допустимых систем, которые выполняли попытки активации в течение 30-дневного периода.

  Если число равно **0**, то либо служба была активирована только недавно, либо нет допустимых клиентов, подключенных к узлу KMS.

  Значение счетчика не будет превышать **50**, независимо от того, сколько допустимых систем имеется в среде. Это обусловлено тем, что задано кэширование только удвоенного максимального числа клиентов согласно политике максимального числа лицензий, возвращаемой клиентом KMS. Политика максимального числа лицензий на сегодняшний день задается клиентской ОС Windows, и для активации узла KMS требуется не менее **25** клиентов. Таким образом, максимальное число клиентов на узле KMS составляет 2x25, то есть 50. Обратите внимание на то, что в средах, содержащих только клиенты KMS для Windows Server, максимальное число клиентов на узле KMS составит **10**. Это обусловлено тем, что порог для выпусков Windows Server равен **5** (а 2x5 равно 10).

Распространенная проблема, связанная с числом клиентов: в среде имеются активированный узел KMS и достаточное количество клиентов, но число клиентов не превышает единицу. Основная проблема заключается в том, что развернутый образ клиента настроен неправильно (**sysprep /generalize**) и в системах нет уникальных идентификаторов клиентского компьютера (CMID). Дополнительные сведения см. в разделах Клиент KMS и Текущее количество KMS не увеличивается при добавлении новой Windows Vista или Windows 7 на клиентских компьютерах в сети. Один из наших инженеров по эскалации технических проблем также описал эту проблему в блоге: KMS Host Client Count not Increasing Due to Duplicate CMID'S (Число клиентов KMS не увеличивается из-за одинаковых CMID).

Еще одна причина, по которой число может не увеличиться, заключается в том, что в среде слишком много узлов KMS, и количество клиентов распределено по всем ним.

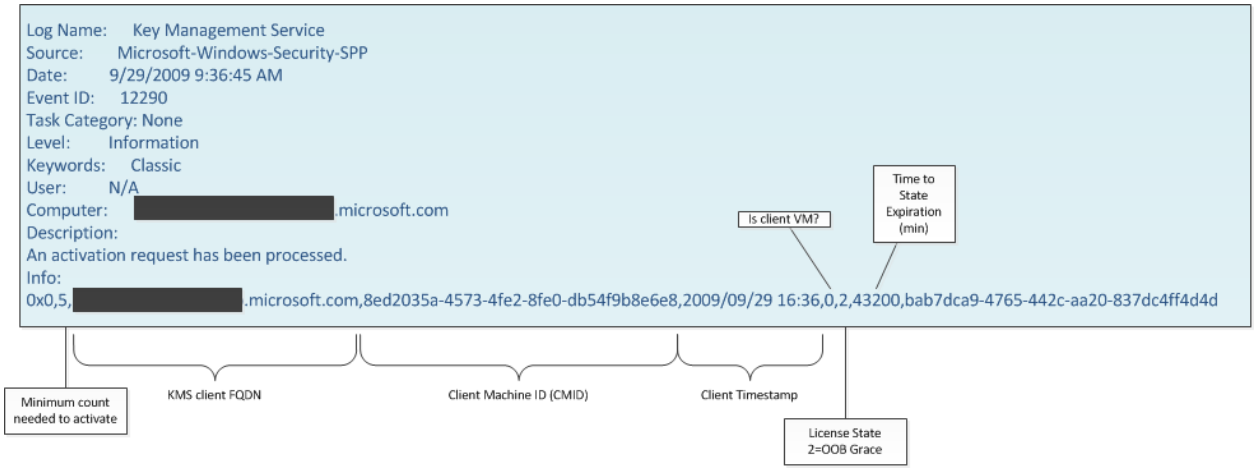
- **Listening on Port** (Ожидание передачи данных через порт). Для обмена данными с KMS используется анонимный RPC. По умолчанию клиенты используют TCP-порт 1688 для подключения к узлу KMS. Убедитесь, что этот порт открыт между клиентами KMS и узлом KMS. Вы можете изменить или настроить порт на узле KMS. Во время обмена данными узел KMS отправляет значение порта клиентам KMS. Если вы измените порт на клиенте KMS, то при подключении клиента к узлу значение порта будет перезаписано.

Нас часто спрашивают о разделе "Cumulative requests" (Совокупные запросы) в выходных данных **slmgr.vbs /dlv**. Обычно эти данные не помогают в устранении неполадок. Узел KMS хранит текущую запись состояния каждого клиента KMS, который пытается выполнить активацию или повторную активацию. Неудачные запросы указывают на клиенты KMS, которые не поддерживаются узлом KMS. Например, если клиент KMS для Windows 7 пытается выполнить активацию на узле KMS, который был активирован с помощью ключа KMS для Windows Vista, то активация завершится ошибкой. В строках "Requests with License Status" (Запросы с состоянием лицензии) описаны все возможные состояния лицензии: прошлые и текущее. С точки зрения устранения неполадок эти данные важны, только если это число не увеличивается должным образом. В этом случае должно расти число неудачных запросов. Это означает, что следует проверить ключ продукта, который был использован для активации системы узла KMS. Кроме того, обратите внимание на то, что значения совокупных запросов сбрасываются только при переустановке системы узла KMS.

Полезные события узла KMS

Идентификатор события 12290

Узел KMS регистрирует событие с идентификатором 12290, когда клиент KMS обращается к узлу для активации. Событие с идентификатором 12290 содержит значительный объем информации, которую можно использовать, чтобы выяснить, какого типа клиент обращался к узлу и почему произошла ошибка. Приведенный ниже сегмент записи события с идентификатором 12290 взят из журнала событий службы управления ключами узла KMS.



Описание события содержит следующие сведения.

- **Минимальное число клиентов, необходимое для активации**. Клиент KMS сообщает, что для активации число клиентов на узле KMS должно быть равно **5**. Это означает, что это операционная система Windows Server, хотя и не указывается ее конкретный выпуск. Если клиенты не активируются, убедитесь, что на узле достаточное число клиентов.
- **Идентификатор клиентского компьютера (CMID)** . Это уникальное значение в каждой системе. Если это значение не является уникальным, значит, образ для дистрибутива был неправильно подготовлен (**sysprep /generalize**). Эта проблема проявляется на сервере службы KMS так: количество клиентов не увеличивается, даже если в среде их достаточно. Дополнительные сведения см. в разделе Текущее количество KMS не увеличивается при добавлении новой Windows Vista или Windows 7 на клиентских компьютерах в сети .
- **Состояние лицензии и время до истечения срока состояния**. Это текущее состояние лицензии клиента. Оно поможет вам отличить клиента, который пытается выполнить активацию впервые, от клиента, который пытается выполнить повторную активацию. Запись времени показывает, сколько еще клиент останется в этом состоянии, если ничего не изменится.

Если при устранении неполадок с клиентом не удается обнаружить на узле KMS соответствующее событие с идентификатором 12290, то клиент не подключается к

узлу KMS. Ниже приведены некоторые причины, по которым может отсутствовать запись события с идентификатором 12290.

- Произошел сбой сети.
- Узел не разрешается или не зарегистрирован в DNS.
- Брандмауэр блокирует TCP-порт 1688. Этот порт может быть заблокирован во многих местах в среде, в том числе в самой системе узла KMS. По умолчанию на узле KMS задано исключение брандмауэра для KMS, но оно не включается автоматически. Необходимо включить это исключение.
- Журнал аудита заполнен.

Клиенты KMS регистрируют два соответствующих события — с идентификаторами 12288 и 12289. Дополнительные сведения об этих событиях см. в разделе Клиент KMS.

Идентификатор события 12293

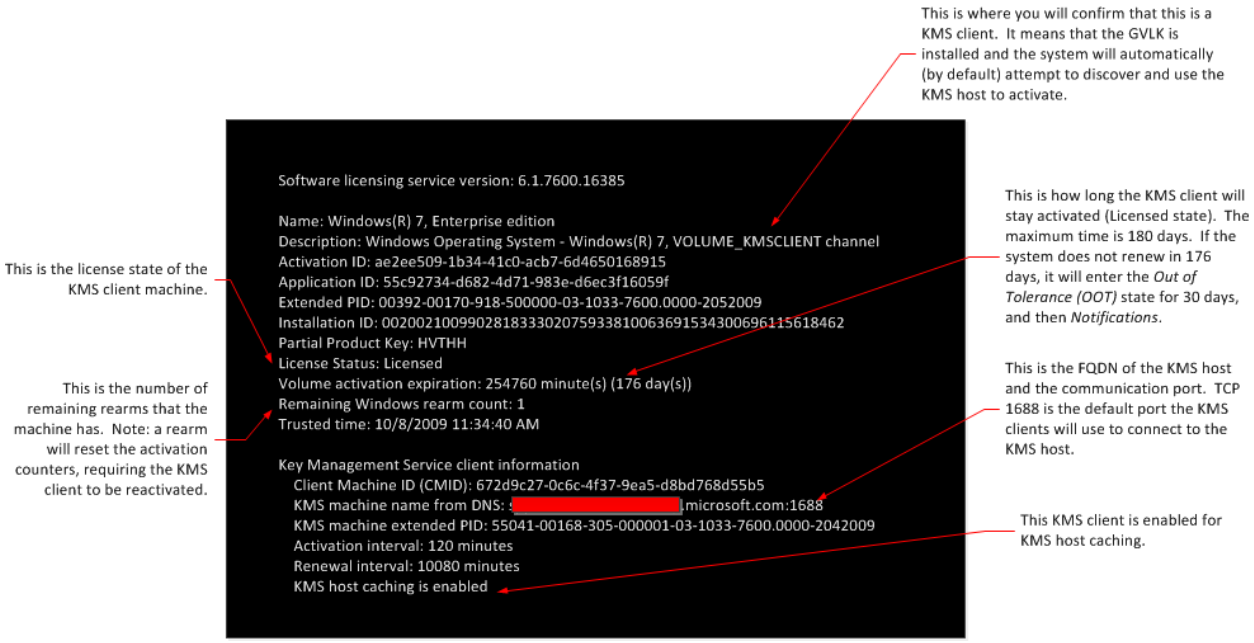
Еще одно значимое событие, которое следует искать на узле KMS, — событие с идентификатором 12293. Это событие означает, что узел не опубликовал необходимые записи в DNS. Эта ситуация вызывает сбои, и ее наличие необходимо проверить *после* установки узла и *перед* развертыванием клиентов. Дополнительные сведения о проблемах с DNS см. в статье Общие процедуры устранения неполадок с KMS и DNS.

Клиент KMS

На клиентах для устранения неполадок активации используются одни и те же инструменты (Slmgr и Просмотр событий).

Сценарий Slmgr.vbs и служба лицензий на программное обеспечение

Чтобы просмотреть подробные выходные данные службы лицензий на программное обеспечение, откройте окно командной строки с повышенными привилегиями и введите в нем **slmgr.vbs/dlv**. На следующем снимке экрана показаны результаты выполнения этой команды на одном из узлов KMS в корпорации Майкрософт.



Ниже приведен список наиболее важных полей для устранения неполадок. Искомые сведения могут быть разными в зависимости от устраняемой проблемы.

- **Имя**. Это значение указывает выпуск Windows, установленный в системе клиента KMS. Используйте его, чтобы убедиться, что версия Windows, которую вы пытаетесь активировать, может использовать KMS. Например, наша служба технической поддержки сталкивалась с инцидентами, в которых клиенты пытались установить ключ установки клиента KMS в выпуске Windows, не использующем активацию корпоративных лицензий, например Windows Vista Ultimate.
- **Описание**. Это значение — установленный ключ. VOLUME_KMSCLIENT указывает, что установлен ключ установки клиента KMS (или GVLK) (конфигурация по умолчанию для носителя для корпоративных лицензий) и что эта система автоматически пытается выполнить активацию с помощью узла KMS. Если вы видите что-то другое, например MAK, то вам потребуется переустановить GVLK, чтобы настроить эту систему в качестве клиента KMS. Можно вручную установить ключ с помощью команды **slmgr.vbs /ipk <*GVLK*>** (как описано в разделе Ключи установки клиента KMS) или использовать средство управления активацией корпоративных лицензий (VAMT). Сведения о том, как получить и испольщзовать VAMT, приведены в техническом справочнике по средству управления активацией корпоративных лицензий (VAMT).
- **Partial Product Key** (Частичный ключ продукта). Как и поле **Name** (Имя), эти сведения можно использовать, чтобы определить, установлен ли на компьютере правильный ключ установки клиента KMS (иными словами, что ключ соответствует операционной системе, установленной на клиенте KMS). По умолчанию правильный ключ содержится в системах, созданных с

помощью носителя с портала центра поддержки корпоративных лицензий (VLSC). В некоторых случаях клиенты могут использовать активацию с помощью ключа многократной активации (MAK), пока в среде достаточное количество систем для поддержки активации KMS. На этих системах необходимо установить ключ установки клиента KMS, чтобы перевести их с использования MAK на использование KMS. Используйте VAMT для установки этого ключа и убедитесь, что применен правильный ключ.

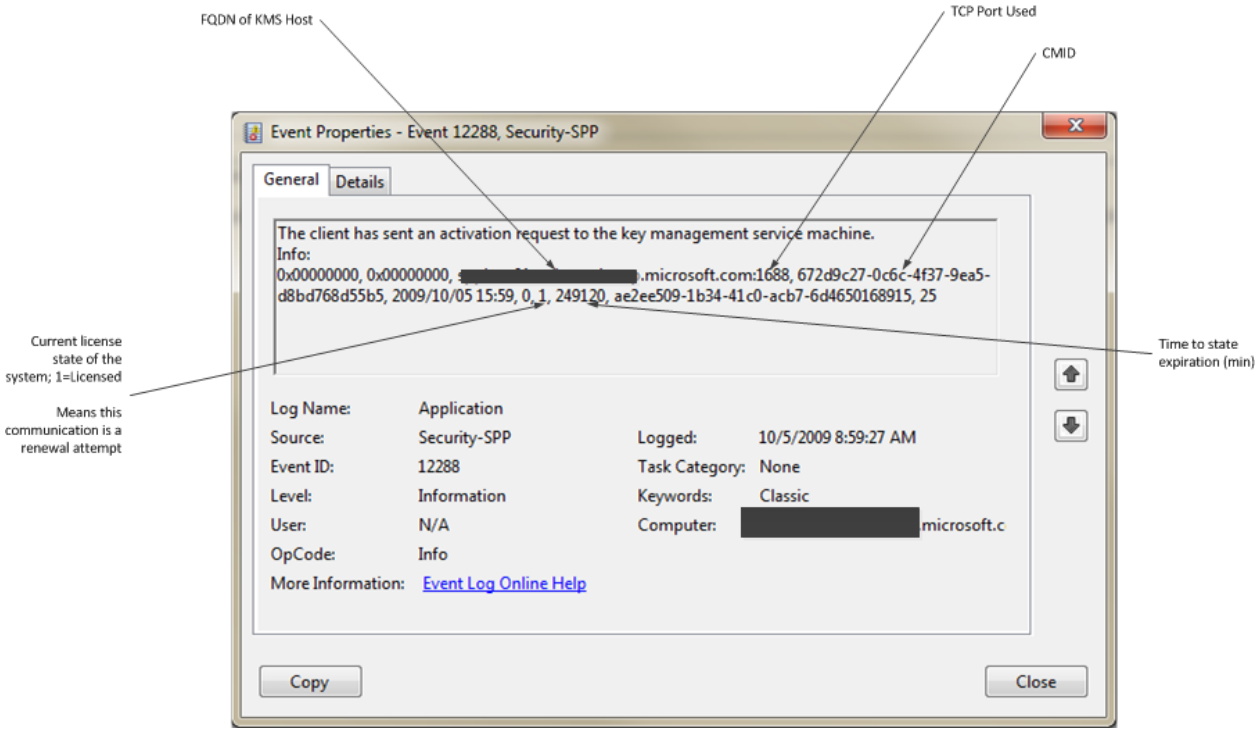
- **License Status** (Состояние лицензии). Это значение показывает состояние системы клиента KMS. Для системы, которая была активирована с помощью KMS, это должно быть значение **Licensed** (Лицензировано). Любое другое значение может указывать на проблему. Например, если узел KMS работает правильно и клиент KMS не активируется (например, он остается в состоянии **Grace** (Льготный период)), возможно, клиент не может связаться с системой узла (например, из-за проблемы с брандмауэром, сбоя сети или чего-то подобного).
- **Идентификатор клиентского компьютера (CMID)** . Каждый клиент KMS должен иметь уникальный идентификатор CMID. Как упоминалось в разделе Узел KMS, распространена следующая проблема с количеством клиентов: в среде имеются активированный узел KMS и достаточное количество клиентов, но число клиентов не превышает **1**. Дополнительные сведения см. в разделе Текущее количество KMS не увеличивается при добавлении новой Windows Vista или Windows 7 на клиентских компьютерах в сети .
- **KMS Machine Name from DNS** (Имя компьютера KMS из DNS). Это значение содержит полное доменное имя узла KMS, которое клиент успешно использовал для активации, и TCP-порт, используемый для связи.
- **KMS Host Caching** (Кэширование узла KMS). Окончательное значение указывает, включено ли кэширование. По умолчанию оно включено. Это означает, что клиент KMS сохраняет в кэше имя узла KMS, которое использовалось для активации, и непосредственно взаимодействует с этим узлом (вместо запроса DNS), когда наступает время повторной активации. Если клиент не может связаться с кэшированным узлом KMS, он отправляет запрос в DNS для обнаружения нового узла KMS.

Полезные события клиента KMS

Идентификаторы событий 12288 и 12289

После успешной активации или повторной активации клиента KMS он регистрирует два события — с идентификаторами 12288 и 12289. Приведенный

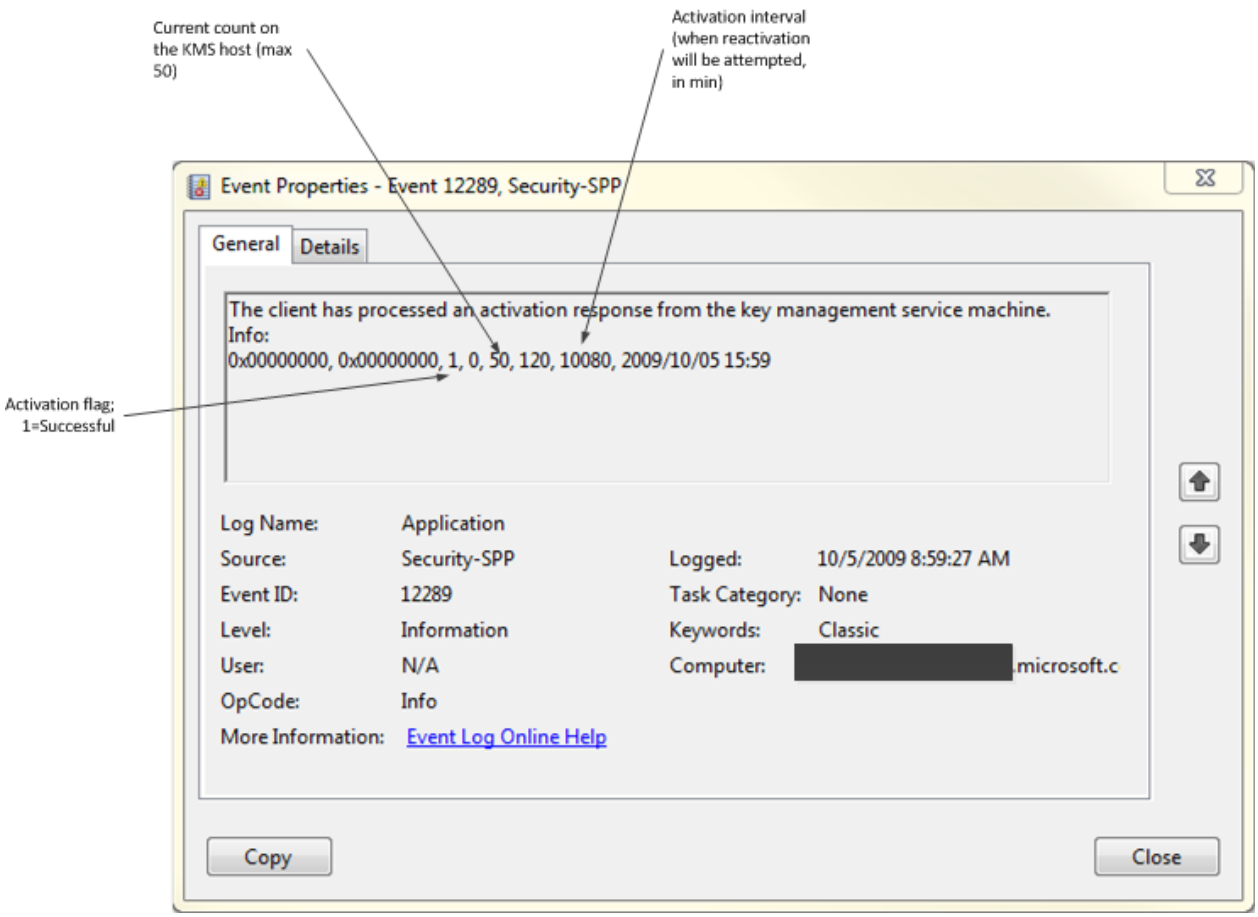
ниже сегмент записи события с идентификатором 12288 взят из журнала событий службы управления ключами клиента KMS.



Если отображается только событие с идентификатором 12288 (без соответствующего события с идентификатором 12289), это означает, что клиенту KMS не удалось подключиться к узлу KMS, узел KMS не ответил или клиент не получил ответ. В этом случае убедитесь, что узел KMS доступен для обнаружения и что клиенты KMS могут с ним связаться.

Наиболее важная информация в событии с идентификатором 12288 — это данные в разделе "Info" (Информация). Например, в этом разделе показано текущее состояние клиента, а также полное доменное имя и TCP-порт, использованные клиентом при попытке активации. Полное доменное имя можно использовать для устранения неполадок, из-за которых количество клиентов на узле KMS не увеличивается. Например, если клиентам доступно слишком много узлов KMS (как подлинных, так и мошеннических систем), то количество клиентов может распределяться по всем ним.

Неудачная активация не всегда означает, что для клиента имеется событие с идентификатором 12288, а события с идентификатором 12289 нет. При неудачной или повторной активации могут присутствовать оба эти события. В этом случае необходимо изучить второе событие, чтобы выяснить причину сбоя.



В разделе "Info" (Информация) события с идентификатором 12289 содержатся следующие сведения.

- **Флаг активации**. Это значение указывает, успешно выполнена активация (**1**) или произошел сбой (**0**).
- **Текущее число клиентов на узле KMS**. Это значение отражает значение счетчика на узле KMS, когда клиент пытается выполнить активацию. Если активация завершается сбоем, это может быть вызвано недостаточным значением счетчика для данной клиентской операционной системы или недостаточным количеством систем в среде для значения счетчика.

Что следует сообщить сотруднику службы поддержки?

При обращении в службу поддержки для устранения неполадок активации инженер службы поддержки обычно запрашивает следующие сведения.

- Выходные данные команды **Slmgr.vbs /dlv**, выполненной на узле KMS и клиентских системах KMS. Если вы используете Wscript или Cscript для выполнения команды, можно нажать клавиши CTRL+C, чтобы скопировать выходные данные, а затем вставить их в Блокнот, чтобы отправить их сотруднику службы поддержки.

- Журналы событий с узла KMS (журнал службы управления ключами) и из клиентских систем KMS (журнал приложений).

Дополнительные ссылки

- Ask the Core Team: #Activation (Вопрос группе разработчиков основных компонентов: #Activation)

Параметры slmgr.vbs для получения сведений об активации корпоративных лицензий

Статья • 28.01.2023 • Чтение занимает 10 мин •

Применяется к: Windows Server 2012 R2, Windows 10, Windows 8.1

Ниже описывается синтаксис сценария Slmgr.vbs, а в таблицах в этой статье приведено описание всех параметров командной строки.

```cmd
slmgr.vbs [<ComputerName> [<User> <Password>]] [<Options>]
```

> ⓘ **Примечание**
>
> В этой статье в квадратных скобках, [], указаны необязательные аргументы, а в угловых скобках, <>, указаны заполнители. При вводе этих инструкций опустите квадратные скобки и замените заполнители соответствующими значениями.

> ⓘ **Примечание**
>
> Сведения о других программных продуктах, использующих активацию корпоративных лицензий, приведены в документации по этим приложениям.

Использование сценария Slmgr на удаленных компьютерах

Для управления удаленными клиентами используйте средство управления активацией корпоративных лицензий (VAMT) 1.2 или более поздней версии либо создайте собственные сценарии WMI, в которых учитываются отличия платформ. Дополнительные сведения о свойствах и методах WMI для активации корпоративных лицензий см. в разделе Свойства и методы WMI для активации корпоративных лицензий.

> ⓘ **Важно!**

Из-за изменений WMI в Windows 7 и Windows Server 2008 R2 сценарий Slmgr.vbs не предназначен для работы на разных платформах. Использование Slmgr.vbs для управления системой Windows 7 или Windows Server 2008 R2 из операционной системы Windows Vista® не поддерживается. При попытке управления системой предыдущих версий из Windows 7 или Windows Server 2008 R2 произойдет ошибка несоответствия версий. Например, при выполнении **cscript slmgr.vbs <vista_machine_name> /dlv** получаются следующие выходные данные:

> Сервер сценариев Windows (Microsoft (R)) версия 5.8. (C) Корпорация Майкрософт (Microsoft Corp.). Все права защищены.
>
> Удаленный компьютер не поддерживает эту версию SLMgr.vbs

Общие параметры Slmgr.vbs

Параметр	Описание
[<ComputerName>]	Имя удаленного компьютера (по умолчанию используется локальный компьютер)
[<User>]	Учетная запись с необходимыми разрешениями на удаленном компьютере.
[<Password>]	Пароль учетной записи с необходимыми разрешениями на удаленном компьютере.

Глобальные параметры

Параметр	Описание

Параметр	Описание
/ipk <ProductKey>	Попытки установить ключ продукта 5×5. Ключ продукта, заданный параметром, проверяется на допустимость и применимость для установленной операционной системы. Если это не так, возвращается ошибка. Если ключ допустим и применим, он устанавливается. Если ключ уже установлен, он автоматически заменяется. Во избежание нестабильной работы службы лицензий необходимо перезапустить систему или службу защиты программного обеспечения. Эту операцию нужно выполнять в командной строке с повышенными привилегиями, либо должно быть задано значение реестра "Standard User Operations" (Стандартные операции пользователя), позволяющее непривилегированным пользователям получать расширенный доступ к службе защиты программного обеспечения.
/ato [<Идентификатор активации>]	Для розничных выпусков и корпоративных систем с установленным ключом узла KMS или ключом многократной активации (MAK) параметр **/ato** указывает Windows попытаться выполнить активацию через Интернет. Для систем с установленным универсальным ключом многократной установки (GVLK) выдается запрос на активацию KMS. Если в системе приостановлена автоматическая активация KMS (**/stao**), при выполнении с параметром **/ato** все равно будет осуществлена попытка активации KMS. **Примечание**. Начиная с Windows 8 (и Windows Server 2012), параметр **/stao** является устаревшим. Вместо него используется параметр **/act-type**. <**ИД активации**> в **/ato** позволяет определить выпуск Windows, установленный на компьютере. Когда указан <**ИД активации**>, параметр /ato действует только для выпуска, связанного с этим атрибутом. Выполните команду **Slmgr.vbs /dlv all**, чтобы получить все значения Activation ID для установленной версии Windows. Если требуется организовать поддержку других приложений, дополнительные инструкции приведены в руководстве для соответствующего приложения. Активация KMS не требует повышенных привилегий. Однако повышенные привилегии нужны для активации через Интернет, либо должно быть задано значение реестра Standard User Operations (Стандартные операции пользователя), позволяющее непривилегированным пользователям получать расширенный доступ к службе защиты программного обеспечения.

Параметр	Описание
/dli [<Идентификатор активации> | All]	Показывает сведения о лицензии. По умолчанию **/dli** показывает сведения о лицензии для установленного активного выпуска Windows. Если указать атрибут <**ИД активации**>, будут показаны сведения о лицензии для заданного выпуска, связанного с этим атрибутом. Если указать атрибут **All**, будут показаны сведения о лицензиях для всех применимых установленных продуктах. Эта операция не требует повышенных привилегий.
/dlv [<Идентификатор активации> | All]	Показывает подробные сведения о лицензии. По умолчанию **/dlv** показывает сведения о лицензии для установленной операционной системы. Если указать атрибут <**ИД активации**>, будут показаны сведения о лицензии для заданного выпуска, связанного с этим атрибутом. Если указать атрибут **All**, будут показаны сведения о лицензиях для всех применимых установленных продуктах. Эта операция не требует повышенных привилегий.
/xpr [<Идентификатор активации>]	Показывает дату истечения срока действия активации для продукта. По умолчанию это касается текущего выпуска Windows и в основном удобно для клиентов KMS, поскольку активация MAK и розничного выпуска является постоянной. Если указать атрибут <**ИД активации**>, будет показана дата истечения срока действия активации указанного выпуска, связанного с этим атрибутом. Эта операция не требует повышенных привилегий.

Дополнительные параметры.

Параметр	Описание
/cpky	Некоторые операции обслуживания требуют доступа к ключу продукта в реестре во время выполнения операций при первом включении компьютера (OOBE). Параметр **/cpky** удаляет ключ продукта из реестра во избежание кражи ключа вредоносным кодом. Для розничных продуктов, в которых используются ключи, рекомендуется использовать этот параметр. Этот параметр не требуется для ключей MAK и ключей узла KMS, поскольку для таких ключей это порядок действий по умолчанию. Этот параметр требуется только для других типов ключей, для которых порядок действий по умолчанию не предусматривает удаления ключа из реестра. Эта операция должна запускаться из командной строки с повышенными привилегиями.

Параметр	Описание
/ilc <файл_лицензии>	Этот параметр устанавливает файл лицензии, заданный в необходимом параметре. Эти лицензии могут устанавливаться в качестве меры по борьбе с неполадками, для поддержки активации на основе маркеров или при установке стандартного приложения вручную. Во время этого процесса проверка лицензий не осуществляется: Сценарий Slmgr.vbs проверку лицензий не осуществляет. Проверка осуществляется службой защиты программного обеспечения во время выполнения. Эту операцию нужно выполнять в командной строке с повышенными привилегиями, либо должно быть задано значение реестра **Standard User Operations** (Стандартные операции пользователя), позволяющее непривилегированным пользователям получать расширенный доступ к службе защиты программного обеспечения.
/rilc	Этот параметр переустанавливает все лицензии, хранящиеся в каталогах %SystemRoot%\system32\oem и %SystemRoot%\System32\spp\tokens. Это заведомо хорошие копии, сохраняемые во время установки. Все соответствующие лицензии в надежном хранилище заменяются. Все другие лицензии, например лицензии на выдачу доверенного центра сертификации и лицензии для приложений, не затрагиваются. Эту операцию нужно выполнять в командной строке с повышенными привилегиями, либо должно быть задано значение реестра **Standard User Operations** (Стандартные операции пользователя), позволяющее непривилегированным пользователям получать расширенный доступ к службе защиты программного обеспечения.
/rearm	Этот параметр сбрасывает таймеры активации. Процесс **/rearm** также вызывается **sysprep /generalize**. Эта операция не выполняет никаких действий, если запись реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\SkipRearm** имеет значение **1**. Дополнительные сведения об этой записи реестра см. в разделе Параметры реестра для активации корпоративных лицензий. Эту операцию нужно выполнять в командной строке с повышенными привилегиями, либо должно быть задано значение реестра **Standard User Operations** (Стандартные операции пользователя), позволяющее непривилегированным пользователям получать расширенный доступ к службе защиты программного обеспечения.
/rearm-app <Идентификатор активации>	Сбрасывает состояние лицензирования для указанного приложения.
/rearm-sku <Идентификатор активации>	Сбрасывает состояние лицензирования для указанного SKU.

Параметр	Описание
/upk [<Идентификатор активации>]	Этот параметр удаляет ключ продукта для текущего выпуска Windows. После перезапуска система окажется в состоянии "Не имеет лицензии", если не установить новый ключ продукта. При желании можно использовать атрибут <**Activation ID**>, чтобы указать другой установленный продукт. Эта операция должна выполняться из командной строки с повышенными привилегиями.
/dti [<Идентификатор активации>]	Показывает идентификатор установки для автономной активации.
/atp <Идентификатор подтверждения>	Активирует продукт с предоставленным пользователем идентификатором подтверждения.

Параметры клиента KMS

Параметр	Описание
/skms <Name[:Port] | :port> [<Идентификатор активации>]	Этот параметр задает имя и при необходимости порт компьютера узла KMS, с которым устанавливается соединение. Когда выбрано это значение, автоматическое определение узла KMS отменяется. Если на узле KMS используется только протокол IPv6, адрес нужно указать в формате <имя_узла>:<порт>. IPv6-адреса содержат двоеточия (:), которые сценарий Slmgr.vbs неправильно анализирует. Эта операция должна выполняться из командной строки с повышенными привилегиями.
/skms-domain <FQDN> [<Идентификатор активации>]	Задает конкретный DNS-домен, в котором можно найти все записи KMS SRV. Этот параметр не оказывает никакого влияния, если конкретный единственный узел KMS настроен с параметром **/skms**. Используйте этот параметр, особенно в несвязанных пространствах имен, чтобы сервер KMS игнорировал список DNS-суффиксов и вместо этого искал записи узла KMS в указанном DNS-домене.
/ckms [<Идентификатор активации>]	Этот параметр удаляет имя, адрес и порт указанного узла KMS из реестра и восстанавливает режим автоматического обнаружения KMS. Эта операция должна выполняться из командной строки с повышенными привилегиями.

Параметр	Описание
/skhc	Этот параметр отключает кэширование узлов KMS (по умолчанию). После того как клиент обнаружит работающий узел KMS, этот параметр не позволит приоритету и весу службы доменных имен (DNS) влиять на обмен данными с этим узлом. Если система больше не может связаться с работающим узлом KMS, клиент пытается обнаружить новый узел. Эта операция должна выполняться из командной строки с повышенными привилегиями.
/ckhc	Этот параметр отключает кэширование узла KMS. Этот параметр предписывает клиенту использовать автоматическое обнаружение DNS при каждой попытке активации KMS (рекомендуется при использовании приоритета и веса). Эта операция должна выполняться из командной строки с повышенными привилегиями.

Параметры конфигурации узла KMS

Параметр	Описание
/sai <Интервал>	Этот параметр задает интервал в минутах, через который неактивированные клиенты пытаются подключиться к KMS. Интервал активации должен находиться в диапазоне от 15 минут до 30 дней. Рекомендуется использовать интервал по умолчанию — 2 часа. Изначально клиент KMS извлекает этот интервал из реестра, но после получения первого ответа KMS переходит на параметр KMS. Эта операция должна выполняться из командной строки с повышенными привилегиями.
/sri <Interval>	Этот параметр задает интервал продления в минутах, через который активированные клиенты пытаются подключиться к KMS. Интервал обновления должен находиться в диапазоне от 15 минут до 30 дней. Этот параметр изначально задается и на стороне сервера, и на стороне клиента KMS. По умолчанию используется значение "10 080 минут (7 дней)". Клиент KMS первоначально извлекает этот интервал из реестра, но после получения первого ответа KMS переходит на параметр KMS. Эта операция должна выполняться из командной строки с повышенными привилегиями.
/sprt <Порт>	Этот параметр задает порт, по которому узел KMS прослушивает запросы активации клиентов. Номер порта TCP по умолчанию — 1688. Эта операция должна выполняться из командной строки с повышенными привилегиями.

Параметр	Описание
/sdns	Включает публикацию DNS узлом KMS (по умолчанию). Эта операция должна выполняться из командной строки с повышенными привилегиями.
/cdns	Отключает публикацию DNS узлом KMS. Эта операция должна выполняться из командной строки с повышенными привилегиями.
/spri	Устанавливает приоритет KMS в значение "Обычный" (по умолчанию). Эта операция должна выполняться из командной строки с повышенными привилегиями.
/cpri	Устанавливает приоритет KMS в значение "Низкий". Используйте этот параметр, чтобы минимизировать конфликты со стороны KMS в связанной среде. Имейте в виду, что это может привести к нехватке ресурсов для KMS в зависимости от активности других приложений или ролей сервера. Следует использовать с осторожностью. Эта операция должна выполняться из командной строки с повышенными привилегиями.
/act-type [<Activation-Type>] [<Идентификатор активации>]	Этот параметр задает значение реестра, которое ограничивает многопользовательскую активацию одним типом. Тип активации **1** разрешает только активацию Active Directory, **2** — только активацию KMS, **3** — активацию на основе маркеров. **0** разрешает активацию любого типа и является значением по умолчанию.

Параметры конфигурации активации на основе маркеров

Параметр	Описание
/lil	Выводит список установленных лицензий на выдачу с активацией на основе маркеров.
/ril <ILID> <ILvID>	Удаляет установленную лицензию на выдачу с активацией на основе маркеров. Эта операция должна выполняться из командной строки с повышенными привилегиями.

Параметр	Описание
/stao	Устанавливает флаг **Token-based Activation Only**, отключая автоматическую активацию KMS. Эта операция должна выполняться из командной строки с повышенными привилегиями. Этот параметр был удален в Windows Server 2012 R2 и Windows 8.1. Вместо него используется **/act–type**.
/ctao	Снимает флаг **Token-based Activation Only** (по умолчанию), разрешая автоматическую активацию KMS. Эта операция должна выполняться из командной строки с повышенными привилегиями. Этот параметр был удален в Windows Server 2012 R2 и Windows 8.1. Вместо него используется параметр **/act-type**.
/ltc	Выводит список действительных сертификатов с активацией на основе маркеров, которые могут активировать установленное программное обеспечение.
/fta <Отпечаток сертификата> [<PIN>]	Принудительно задает активацию на основе маркеров с использованием указанного сертификата. Необязательный персональный идентификационный код (ПИН-код) предоставляется для снятия блокировки закрытого ключа без запроса ПИН-кода при использовании сертификатов с аппаратной защитой (например, смарт-карт).

Параметры конфигурации активации с помощью Active Directory

Параметр	Описание
/ad-activation-online <Ключ продукта> [<Имя объекта активации>]	Собирает данные Active Directory и запускает активацию леса Active Directory с помощью учетных данных, использованных для запуска командной строки. Доступ с правами локального администратора не требуется. Однако необходим доступ на чтение и запись для контейнера объекта активации в корневом домене леса.
/ad-activation-get-IID <Ключ продукта>	Этот параметр запускает активацию леса Active Directory в режиме телефона. Результатом является идентификатор установки (IID), который может использоваться для активации леса по телефону, когда отсутствует подключение к Интернету. При предоставлении IID во время телефонного звонка для активации возвращается CID, который используется для завершения активации.

Параметр	Описание
/ad-activation-apply-cid <Ключ продукта><ИД подтверждения> [<Имя объекта активации>]	При использовании этого параметра, чтобы завершить активацию, введите CID, предоставленный при телефонном звонке для активации.
[/name: <AO_Name>]	Также в конец любой из этих команд можно добавить параметр **/name**, чтобы задать имя объекта активации, хранящегося в Active Directory. Его длина не должна превышать 40 знаков Юникода. Используйте двойные кавычки для явного определения строки имени. В Windows Server 2012 R2 и Windows 8.1 имя можно добавить непосредственно после команд **/ad-activation-online <Ключ продукта>** и **/ad-activation-apply-cid** без необходимости использовать параметр **/name**.
/ao-list	Показывает все объекты активации, доступные локальному компьютеру.
/del-ao <AO_DN> /del-ao <AO_RDN>	Удаляет указанный объект активации из леса.

Дополнительные ссылки

- Технический справочник по активации корпоративных лицензий
- Обзор активации корпоративных лицензий

Устранение неполадок по коду ошибки активации Windows

Статья • 28.01.2023 • Чтение занимает 12 мин

Попробуйте воспользоваться виртуальным агентом.

Он помогает быстро выявлять и устранять распространенные проблемы, связанные с KMS и активацией MAK

Примечание

Эта статья предназначена для агентов технической поддержки и ИТ-специалистов. Если вам нужны дополнительные сведения о сообщениях об ошибках активации Windows, см. статью **Справка по ошибкам активации Windows**.

В этой статье приводятся сведения по устранению ошибок, которые могут возникнуть при попытке использовать ключ многократной активации (MAK) или службы управления ключами (KMS) для активации корпоративных лицензий на компьютерах с Windows. Найдите код ошибки в таблице ниже, а затем щелкните ссылку, чтобы просмотреть подробные сведения об ошибке с таким кодом и способах ее устранения.

Дополнительные сведения об активации корпоративных лицензий см. в статье Plan for volume activation (Планирование активации корпоративных лицензий).

Дополнительные сведения об активации корпоративных лицензий для текущих и последних версий Windows см. в этой статье.

Дополнительные сведения об активации корпоративных лицензий для более ранних версий Windows (Windows Vista, Windows Server 2008, Windows Server 2008 R2 и Windows 7) см. в статье базы знаний № 929712.

Средство диагностики

Примечание

Этот инструмент предназначен для устранения проблем с активацией Windows на компьютерах под управлением операционной системы Windows Корпоративная, Windows Профессиональная или Windows Server.

Служба поддержки Майкрософт и помощник по восстановлению (SaRA) упрощают устранение неполадок при активации Windows KMS.

Скачать Помощник

Это средство попытается активировать Windows. Если будет получен код ошибки активации, средство отобразит решения, соответствующие кодам ошибок.

Поддерживаются следующие коды ошибок: 0xC004F038, 0xC004F039, 0xC004F041, 0xC004F074, 0xC004C008, 0x8007007b, 0xC004C003, 0x8007232B.

Сводка кодов ошибок

Код ошибки	Сообщение об ошибке	Способ активации
0x8004FE21	Компьютер не работает под управлением подлинной Windows.	MAK Клиент KMS
0x80070005	Доступ запрещен. Для отправки запроса требуется более высокий уровень привилегий.	MAK Клиент KMS Узел KMS
0x8007007b	0x8007007b DNS-имя не существует.	Клиент KMS
0x80070490	Введенный ключ продукта не сработал. Проверьте ключ продукта и повторите попытку или введите другой ключ.	MAK
0x800706BA	Сервер RPC недоступен.	Клиент KMS
0x8007232A	Ошибка DNS-сервера.	Узел KMS
0x8007232B	DNS-имя не существует.	Клиент KMS
0x8007251D	Не найдены записи для запроса DNS.	Клиент KMS

Код ошибки	Сообщение об ошибке	Способ активации
0x80092328	DNS-имя не существует.	Клиент KMS
0xC004B100	Сервер активации определил, что этот компьютер не может быть активирован.	MAK
0xC004C001	Сервер активации определил, что указанный ключ продукта недопустим.	MAK
0xC004C003	Сервер активации определил, что указанный ключ продукта заблокирован.	MAK
0xC004C008	Сервер активации определил, что указанный ключ продукта нельзя использовать.	Сервер управления ключами
0xC004C020	Сервер активации сообщил, что у ключа многократной активации превышен предел активаций.	MAK
0xC004C021	Сервер активации сообщил, что превышен предел расширения для ключа многократной активации.	MAK
0xC004F009	Служба защиты программного обеспечения сообщила, что срок действия льготного периода истек.	MAK
0xC004F00F	Сервер лицензирования программного обеспечения сообщил, что идентификатор привязки оборудования выходит за границы допустимого отклонения.	MAK Клиент KMS Узел KMS
0xC004F014	Служба защиты программного обеспечения сообщила, что ключ продукта недоступен.	MAK Клиент KMS
0xC004F02C	Служба защиты программного обеспечения сообщила, что формат данных автономной активации неверен.	MAK Клиент KMS
0xC004F035	Служба защиты программного обеспечения сообщила, что на данном компьютере не удалось выполнить активацию с помощью ключа многократной установки.	Клиент KMS Узел KMS
0xC004F038	Служба защиты программного обеспечения сообщила, что компьютер невозможно активировать. Значение счетчика, переданное вашей службой управления ключами (KMS), слишком низкое. Обратитесь к системному администратору.	Клиент KMS

Код ошибки	Сообщение об ошибке	Способ активации
0xC004F039	Служба защиты программного обеспечения сообщила, что компьютер невозможно активировать. Служба управления ключами (KMS) не включена.	Клиент KMS
0xC004F041	Служба защиты программного обеспечения обнаружила, что служба управления ключами (KMS) выключена. Необходимо активировать KMS.	Клиент KMS
0xC004F042	Служба защиты программного обеспечения определила, что указанную службу управления ключами (KMS) невозможно использовать.	Клиент KMS
0xC004F050	Служба защиты программного обеспечения сообщила, что ключ продукта недействителен.	MAK Сервер управления ключами Клиент KMS
0xC004F051	Служба защиты программного обеспечения сообщила, что ключ продукта заблокирован.	MAK Сервер управления ключами
0xC004F064	Служба защиты программного обеспечения сообщила, что льготный период для ПО с неподтвержденной подлинностью закончился.	MAK
0xC004F065	Служба защиты программного обеспечения сообщила, что приложение выполняется в рамках допустимого периода для ПО с неподтвержденной подлинностью.	MAK Клиент KMS
0xC004F06C	Служба защиты программного обеспечения сообщила, что компьютер невозможно активировать. Служба управления ключами (KMS) сообщила, что отметка времени запроса недействительна.	Клиент KMS
0xC004F074	Служба защиты программного обеспечения сообщила, что компьютер невозможно активировать. Невозможно связаться со службой управления ключами (KMS). Дополнительные сведения см. в журнале событий приложения.	Клиент KMS

Причины и способы устранения ошибок

0x8004FE21 На этом компьютере запущена версия Windows, отличная от подлинной

Возможная причина

Эта проблема может возникать по следующим причинам. Скорее всего, языковые пакеты (MUI) были установлены на компьютерах под управлением версий Windows, не лицензированных для дополнительных языковых пакетов.

> ⓘ **Примечание**
>
> Это не обязательно указывает на несанкционированное использование. Некоторые приложения могут устанавливать многоязычную поддержку даже в том случае, если текущий выпуск Windows не имеет лицензий на эти языковые пакеты.

Эта проблема может возникать, если система Windows была изменена вредоносными программами, чтобы разрешить установку дополнительных компонентов. Эта проблема может также возникать, если повреждены определенные системные файлы.

Разрешение

Чтобы устранить проблему, необходимо переустановить операционную систему.

0x80070005 Доступ запрещен

Полный текст этого сообщения об ошибке выглядит так:

> Доступ запрещен. Для отправки запроса требуется более высокий уровень привилегий.

Возможная причина

Контроль учетных записей (UAC) запрещает запуск процессов активации в окне командной строки без повышенных привилегий.

Разрешение

Выполните команду **slmgr.vbs** из командной строки с повышенными привилегиями. Для этого в меню **Пуск** щелкните правой кнопкой мыши **cmd.exe** и выберите **Запуск от имени администратора**.

0x8007007b DNS-имя не существует

Возможная причина

Проблема возникает в том случае, если клиент KMS не может найти записи ресурсов SRV KMS в DNS.

Разрешение

Дополнительные сведения об устранении таких проблем, связанных с DNS, см. в статье Common troubleshooting procedures for KMS and DNS issues (Типичные процедуры для устранения проблем с KMS и DNS).

0x80070490 Введенный ключ продукта не подошел

Полный текст этого сообщения об ошибке выглядит так:

> Введенный ключ продукта не подошел. Проверьте ключ продукта и повторите попытку или введите другой ключ.

Возможная причина

Эта проблема возникает из-за ввода недопустимого ключа MAK или из-за известной проблемы в Windows Server 2019.

Разрешение

Чтобы устранить эту ошибку и активировать компьютер, выполните команду **slmgr -ipk <5x5 key>** в командной строке с повышенными привилегиями.

0x800706BA Сервер RPC недоступен

Возможная причина

На узле KMS не настроены параметры брандмауэра или записи SRV DNS устарели.

Разрешение

Убедитесь, что на узле KMS включено исключение брандмауэра для службы управления ключами (TCP-порт 1688).

Убедитесь, что записи SRV DNS указывают на действительный узел KMS.

Проведите диагностику сетевых подключений.

Дополнительные сведения об устранении таких проблем, связанных с DNS, см. в статье Common troubleshooting procedures for KMS and DNS issues (Типичные процедуры для устранения проблем с KMS и DNS).

0x8007232A Ошибка DNS-сервера

Возможная причина

В системе есть проблемы с сетью или DNS.

Разрешение

Проведите диагностику сети и DNS.

0x8007232B DNS-имя не существует

Возможная причина

Клиент KMS не может найти записи ресурсов сервера (SRV RR) KMS в DNS.

Разрешение

Убедитесь, что узел KMS установлен, а публикация DNS включена (по умолчанию). Если служба DNS недоступна, назначьте клиент KMS узлу KMS с помощью команды **slmgr.vbs /skms <*kms_host_name*>**.

Если узел KMS отсутствует, получите и установите ключ MAK. После этого активируйте систему.

Дополнительные сведения об устранении таких проблем, связанных с DNS, см. в статье Common troubleshooting procedures for KMS and DNS issues (Типичные процедуры для устранения проблем с KMS и DNS).

0x8007251D Не найдены записи для запроса DNS

Возможная причина

Клиент KMS не может найти записи SRV KMS в DNS.

Разрешение

Проведите диагностику сетевых подключений и DNS. Дополнительные сведения об устранении таких проблем, связанных с DNS, см. в статье Common troubleshooting procedures for KMS and DNS issues (Типичные процедуры для устранения проблем с KMS и DNS).

0x80092328 DNS-имя не существует

Возможная причина

Проблема возникает в том случае, если клиент KMS не может найти записи ресурсов SRV KMS в DNS.

Разрешение

Дополнительные сведения об устранении таких проблем, связанных с DNS, см. в статье Common troubleshooting procedures for KMS and DNS issues (Типичные процедуры для устранения проблем с KMS и DNS).

0xC004B100 Сервер активации определил, что этот компьютер не может быть активирован

Возможная причина

Ключ MAK не поддерживается.

Разрешение

Чтобы устранить эту проблему, убедитесь, что используется ключ MAK, предоставленный корпорацией Майкрософт. Чтобы проверить действительность ключа MAK, обратитесь в Центры активации лицензий Майкрософт.

0xC004C001 Сервер активации определил, что указанный ключ продукта недопустим

Возможная причина

Введен недопустимый ключ MAK.

Разрешение

Убедитесь, что MAK является ключом, предоставленным Майкрософт. За дополнительной помощью обратитесь в Центры активации лицензий Майкрософт.

0xC004C003 Сервер активации определил, что указанный ключ продукта заблокирован

Возможная причина

MAK заблокирован на сервере активации.

Разрешение

Чтобы получить новый ключ MAK, обратитесь в Центры активации лицензий Майкрософт. После получения нового ключа MAK попробуйте повторно установить и активировать Windows.

0xC004C008 Сервер активации обнаружил, что указанный ключ продукта не удалось использовать

Возможная причина

Для ключа службы управления ключами превышено предельное число активаций. Ключ узла KMS можно активировать не более 10 раз на шести разных компьютерах.

Разрешение

Если необходимо большее число активаций, обратитесь в Центры активации лицензий Майкрософт.

0xC004C020 Сервер активации сообщил, что превышен предел для ключа многократной активации.

Возможная причина

Для ключа MAK превышено предельное число активаций. По умолчанию ключи MAK можно активировать только определенное число раз.

Разрешение

Если необходимо большее число активаций, обратитесь в Центры активации лицензий Майкрософт.

0xC004C021 Сервер активации сообщил, что превышен предел расширения для ключа многократной активации

Возможная причина

Для ключа MAK превышено предельное число активаций. По умолчанию ключи MAK можно активировать только определенное число раз.

Разрешение

Если необходимо большее число активаций, обратитесь в Центры активации лицензий Майкрософт.

0xC004F009 Служба защиты программного обеспечения сообщила, что льготный период истек.

Возможная причина

Срок действия льготного периода истек до активации системы. Теперь система находится в состоянии уведомлений.

Разрешение

За помощью обратитесь в Центры активации лицензий Майкрософт.

0xC004F00F Сервер лицензирования программного обеспечения сообщил, что идентификатор привязки оборудования выходит за границы допустимого отклонения

Возможная причина

Изменилась конфигурация оборудования или в системе обновлены драйверы.

Разрешение

Если вы активируете лицензии с помощью ключей MAK, повторно активируйте систему в течение льготного периода OOT через Интернет или по телефону.

Если вы активируете лицензии с помощью KMS, перезапустите Windows или выполните команду **slmgr.vbs /ato**.

0xC004F014 Служба защиты программного обеспечения сообщила, что ключ продукта недоступен

Возможная причина

В системе не установлены ключи продукта.

Разрешение

Если вы активируете лицензии с помощью ключей MAK, установите ключ продукта MAK.

Если вы активируете лицензии с помощью KMS, найдите в файле Pid.txt (расположенном на установочном носителе в папке \sources) ключ установки с помощью KMS. Установите ключ.

0xC004F02C Служба защиты программного обеспечения сообщила, что формат данных

автономной активации неправильный.

Возможная причина

Система определила, что данные, введенные во время активации по телефону, недействительны.

Разрешение

Убедитесь, что CID введен правильно.

0xC004F035 Неправильный ключ пакета лицензий

Полный текст этого сообщения об ошибке выглядит так:

> Ошибка. Неправильный ключ пакета лицензий (VLK). Для активации нужно изменить ключ продукта на правильный многопользовательский ключ активации (MAK) или розничный ключ. Требуется соответствующая лицензия на ОС и корпоративная лицензия, лицензия на обновление Windows 7 либо полная лицензия для Windows 7 из розничного источника. ЛЮБАЯ ДРУГАЯ ПОПЫТКА УСТАНОВКИ ЭТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЯВЛЯЕТСЯ НАРУШЕНИЕМ ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ И ЗАКОНОВ ОБ АВТОРСКИХ ПРАВАХ.

Текст ошибки верен, но неоднозначен. Эта ошибка означает, что в BIOS компьютера отсутствует маркер Windows, который идентифицирует его как систему изготовителя оборудования, на которой выполняется соответствующий выпуск Windows. Эта информация требуется для активации клиента KMS. Более точное значение этого кода: "Ошибка: неправильный ключ многократной установки".

Возможная причина

Корпоративные выпуски Windows 7 лицензируются только для обновления. Майкрософт не разрешает установку корпоративной операционной системы на компьютере без установленной соответствующей требованиям операционной системы.

Разрешение

Для активации необходимо выполнить одно из следующих действий.

- Измените ключ продукта на правильный ключ многократной активации (MAK) или розничный ключ. Требуется соответствующая лицензия на ОС и корпоративная лицензия, лицензия на обновление Windows 7 либо полная лицензия для Windows 7 из розничного источника.

  > ⓘ **Примечание**
  >
  > В случае появления сообщения об ошибке 0x80072ee2 при попытке активации используйте приведенный ниже метод активации по телефону.

- Выполните активацию по телефону, сделав следующее.

  1. Выполните команду **slmgr /dti**, а затем запишите значение идентификатора установки.
  2. Чтобы получить идентификатор подтверждения, обратитесь в один из центров активации лицензий Майкрософт и сообщите идентификатор установки.
  3. Чтобы выполнить активацию с помощью идентификатора подтверждения, выполните команду **slmgr /atp <ИД_подтверждения>** .

0xC004F038 Значение счетчика, которое сообщила служба управления ключами (KMS), недостаточно.

Полный текст этого сообщения об ошибке выглядит так:

> Служба защиты программного обеспечения сообщила, что компьютер невозможно активировать. Значение счетчика, переданное вашей службой управления ключами (KMS), слишком низкое. Обратитесь к системному администратору.

Возможная причина

Значение счетчика на узле KMS недостаточно высоко. Для Windows Server значение счетчика KMS должно быть больше или равно 5. Для Windows (клиентская система) значение счетчика KMS должно быть больше или равно 25.

Разрешение

Чтобы можно было воспользоваться KMS для активации Windows, вам нужно увеличить число компьютеров в пуле KMS. Чтобы получить текущее значение счетчика на узле KMS, выполните команду **Slmgr.vbs /dli**.

0xC004F039 Служба управления ключами (KMS) не включена

Полный текст этого сообщения об ошибке выглядит так:

> Служба защиты программного обеспечения сообщила, что компьютер невозможно активировать. Служба управления ключами (KMS) не включена.

Возможная причина

Служба KMS не ответила на запрос KMS.

Разрешение

Проведите диагностику сетевого подключения между узлом и клиентом KMS. Убедитесь, что TCP-порт 1688 (по умолчанию) не заблокирован брандмауэром или другими фильтрами.

0xC004F041 Служба защиты программного обеспечения определила, что сервер управления ключами (KMS) не активирован

Полный текст этого сообщения об ошибке выглядит так:

> Служба защиты программного обеспечения обнаружила, что служба управления ключами (KMS) выключена. Необходимо активировать KMS.

Возможная причина

Узел KMS не активирован.

Разрешение

Активируйте узел KMS через Интернет или по телефону.

0xC004F042 Служба защиты программного обеспечения определила, что указанную службу управления ключами (KMS) невозможно использовать

Возможная причина

Эта ошибка возникает, если клиент KMS связывается с узлом KMS, который не может активировать клиентское программное обеспечение. Например, она часто встречается в смешанных средах, которые содержат специфические для приложений и операционной системы узлы KMS.

Разрешение

Убедитесь, что при использовании конкретных узлов KMS для активации определенных приложений или операционных систем клиенты KMS подключаются к правильным узлам.

0xC004F050 Служба защиты программного обеспечения сообщила, что ключ продукта недействителен

Возможная причина

Эта ошибка может быть вызвана опечаткой в ключе KMS или вводом ключа версии Beta для выпущенной версии операционной системы.

Разрешение

Установите соответствующий ключ KMS в нужной версии Windows. Проверьте правильность ввода. Если вы копируете и вставляете ключ, убедитесь, что длинное тире не заменено на дефис.

0xC004F051 Служба защиты программного обеспечения сообщила, что ключ продукта заблокирован

Возможная причина

Сервер активации определил, что ключ продукта был заблокирован Майкрософт.

Разрешение

Получите новый ключ MAK или KMS, установите его в системе и активируйте.

0xC004F064 Служба защиты программного обеспечения сообщила, что льготный период для ПО с неподтвержденной подлинностью закончился.

Возможная причина

Средства активации Windows (WAT) определили, что система не является подлинной.

Разрешение

За помощью обратитесь в Центры активации лицензий Майкрософт.

0xC004F065 Служба защиты программного обеспечения сообщила, что приложение выполняется в рамках допустимого периода для ПО с неподтвержденной подлинностью.

Возможная причина

Средства активации Windows определили, что система не является подлинной. Система продолжит работу в течение льготного периода для контрафактной версии.

Разрешение

Получите и установите подлинный ключ продукта и активируйте систему в течение льготного периода. В противном случае система перейдет в состояние "Уведомления" в конце этого периода.

0xC004F06C Недействительная метка времени для запроса

Полный текст этого сообщения об ошибке выглядит так:

> Служба защиты программного обеспечения сообщила, что компьютер невозможно активировать. Служба управления ключами (KMS) сообщила, что отметка времени запроса недействительна.

Возможная причина

Системное время на клиентском компьютере слишком сильно отличается от времени на узле KMS. Синхронизация времени имеет большое значение для системной и сетевой безопасности по самым разным причинам.

Разрешение

Устраните эту проблему, синхронизировав системное время на клиентском компьютере с узлом KMS. Мы рекомендуем использовать источник времени NTP или доменные службы Active Directory для синхронизации времени. Этот выпуск использует время UTP и не зависит от выбора часового пояса.

0xC004F074 Не удалось подключиться к службе управления ключами (KMS)

Полный текст этого сообщения об ошибке выглядит так:

> Служба защиты программного обеспечения сообщила, что компьютер невозможно активировать. Невозможно связаться со службой управления ключами (KMS). Дополнительные сведения см. в журнале событий приложения.

Возможная причина

Все системы узлов KMS вернули ошибку.

Разрешение

В журнале событий приложений найдите все события с идентификатором 12288, связанные с попыткой активации. Устраните ошибки на основе данных таких событий.

Дополнительные сведения об устранении таких проблем, связанных с DNS, см. в статье Common troubleshooting procedures for KMS and DNS issues (Типичные процедуры для устранения проблем с KMS и DNS).

Активация KMS: известные проблемы

Статья • 28.01.2023 • Чтение занимает 4 мин

Попробуйте воспользоваться виртуальным агентом.

Он помогает быстро выявлять и устранять распространенные проблемы, связанные с KMS и активацией MAK

В этой статье описываются распространенные вопросы и проблемы, которые могут возникнуть при активации с помощью службы управления ключами (KMS), а также рекомендации по их устранению.

> **Примечание**
>
> Если вы подозреваете, что ваша проблема связана с DNS, ознакомьтесь с разделом **Общие процедуры устранения неполадок с KMS и DNS**.

Следует ли выполнять резервное копирование данных узла KMS?

Для узлов KMS резервное копирование не требуется. Однако если вы используете инструмент для регулярной очистки журналов событий, то возможна утрата хронологии активации, хранящейся в журналах. Если вы используете журнал событий для трассировки или документирования активаций KMS, периодически экспортируйте журнал событий службы управления ключами из папки "Журналы приложений и служб" Просмотра событий.

Если вы используете System Center Operations Manager, то в базе данных хранилища данных System Center хранятся данные журнала событий для создания отчетов, поэтому нет необходимости в отдельном резервном копировании журналов событий.

Активирован ли клиентский компьютер KMS?

На клиентском компьютере KMS откройте панель управления **Система** и найдите сообщение **Активация Windows выполнена**. Кроме того, можно запустить Slmgr.vbs и указать параметр командной строки **/dli**.

Клиентский компьютер KMS не активируется

Проверьте, не достигнут ли порог активаций KMS. На главном компьютере KMS выполните Slmgr.vbs и укажите параметр командной строки **/dli**, чтобы узнать текущее число клиентов этого узла. Если к узлу KMS не подключены как минимум 25 клиентов, то клиентские компьютеры Windows 7 активировать невозможно. Для активации клиентов KMS на платформе Windows Server 2008 R2 требуется, чтобы у узла KMS было не менее 5 клиентов. Дополнительные сведения о требованиях к KMS см. в руководстве по планированию активации корпоративных лицензий.

На клиентском компьютере KMS в журнале событий приложений найдите идентификатор события 12289. Проверьте это событие на наличие следующих сведений.

- Код результата **0**? Все прочие коды означают ошибку.
- В событии указано правильное имя узла KMS?
- Указан правильный порт KMS?
- Доступен ли узел KMS?
- Если на клиенте работает брандмауэр стороннего производителя, необходимо ли настроить исходящий порт?

На главном компьютере KMS в журнале событий KMS найдите идентификатор события 12290. Проверьте это событие на наличие следующих сведений.

- Содержит ли журнал узла KMS запрос с клиентского компьютера? Убедитесь, что указано имя клиентского компьютера KMS. Убедитесь, что клиент и узел KMS могут обмениваться данными. Получил ли клиент ответ?
- Если в журнале не зарегистрировано событие клиента KMS, запрос не поступил на узел KMS или узлу KMS не удалось его обработать. Убедитесь, что маршрутизаторы не блокируют трафик через TCP-порт 1688 (если используется порт по умолчанию) и разрешена передача трафика с отслеживанием состояния в клиент KMS.

Что означает этот код ошибки?

За исключением событий KMS с идентификатором 12290, Windows регистрирует все события активации в журнале событий приложений под именем поставщика

событий Microsoft-Windows-Security-SPP. Windows регистрирует события KMS в журнале службы управления ключами, который хранится в папке "Приложения и службы". ИТ-специалисты могут запустить Slui.exe, чтобы отобразить описание большинства кодов ошибок, связанных с активацией. Общий синтаксис этой команды выглядит следующим образом.

```
cmd
```

```
slui.exe 0x2a ErrorCode
```

Например, если событие с идентификатором 12293 содержит код ошибки 0x8007267C, можно отобразить описание этой ошибки, выполнив следующую команду.

```
cmd
```

```
slui.exe 0x2a 0x8007267C
```

Дополнительные сведения о конкретных кодах ошибок и способах их устранения см. в разделе Устранение ошибок активации.

Клиенты не добавляются к счетчику KMS

Чтобы сбросить идентификатор клиентского компьютера (идентификатор CMID) и другие сведения об активации продукта, выполните команду **sysprep /generalize** или **slmgr /rearm**. В противном случае каждый клиентский компьютер выглядит одинаково и узел KMS не учитывает их как отдельные клиенты KMS.

Узлам KMS не удается создавать записи SRV

Служба доменных имен (DNS) может ограничивать доступ на запись или не поддерживает динамическую службу доменных имен (DDNS). В этом случае предоставьте узлу KMS доступ на запись к базе данных DNS или создайте запись ресурса (RR) службы (SRV) вручную. Дополнительные сведения о проблемах с KMS и DNS см. в статье Общие процедуры устранения неполадок с KMS и DNS.

Только первый узел KMS может создавать записи SRV

Если в организации имеется несколько узлов KMS, другие узлы могут не иметь возможности обновлять записи ресурсов SRV, пока не изменены разрешения по умолчанию для SRV. Дополнительные сведения о проблемах с KMS и DNS см. в статье Общие процедуры устранения неполадок с KMS и DNS.

Мной установлен ключ KMS на клиенте KMS

Ключи KMS должны устанавливаться только на узлах KMS, а не на клиентах KMS. Выполните команду **slmgr.vbs -ipk <SetupKey>** . Таблицы ключей, которые можно использовать для настройки компьютера в качестве клиента KMS, приведены в разделе Ключи установки клиента KMS. Эти ключи общеизвестны и зависят от выпуска. Обязательно удалите из DNS лишние записи ресурсов SRV и перезагрузите компьютеры.

Произошел сбой узла KMS

В случае сбоя узла KMS необходимо установить ключ узла KMS на новом узле, а затем активировать этот узел. Убедитесь, что для нового узла KMS в базе данных DNS имеется запись ресурса SRV. Если вы устанавливаете новый узел KMS, используя те же имя компьютера и IP-адрес, что и у неисправного узла KMS, то новый узел KMS может использовать запись SRV DNS неисправного узла. Если новый узел имеет другое имя компьютера, то можно вручную удалить запись ресурса SRV DNS неисправного узла или (если в DNS включена очистка) разрешить службе DNS удалить ее автоматически. Если сеть использует DDNS, то новый узел KMS автоматически создаст на DNS-сервере новую запись ресурса SRV. Затем, как только будет соблюден порог активации KMS, новый узел KMS начнет сбор запросов на возобновление работы клиентов и перейдет к их активации.

Если клиенты KMS используют автоматическое обнаружение, они автоматически выберут другой узел KMS, если исходный узел KMS не отвечает на запросы на возобновление. Если клиенты не используют автоматическое обнаружение, необходимо будет вручную обновить клиентские компьютеры KMS, назначенные узлу KMS, на котором произошел сбой. Для этого нужно выполнить команду **slmgr.vbs /skms**. Чтобы избежать этой ситуации, настройте на клиентах KMS автоматическое обнаружение. Для получения дополнительных сведений ознакомьтесь с руководством по развертыванию активации корпоративных лицензий.

Активация с помощью MAK: известные проблемы

Статья • 28.01.2023 • Чтение занимает 2 мин

Попробуйте воспользоваться виртуальным агентом.

Он помогает быстро выявлять и устранять распространенные проблемы, связанные с KMS и активацией MAK

В этой статье описаны распространенные проблемы, которые могут возникать при активации с помощью ключа многократной активации (MAK), и приведены рекомендации по их устранению.

Как узнать, активирован ли мой компьютер?

На компьютере откройте панель управления **Система** и найдите сообщение **Активация Windows выполнена**. Кроме того, можно запустить Slmgr.vbs и указать параметр командной строки **/dli**.

Компьютер не активируется через Интернет

Убедитесь, что необходимые порты не заблокированы в брандмауэре. Список портов приведен в руководстве по развертыванию активации корпоративных лицензий.

Сбой активации через Интернет и по телефону

Обратитесь в местный центр активации лицензий Майкрософт. Номера телефонов центров активации лицензий Майкрософт по всему миру приведены в разделе Телефонные номера центров активации лицензий Майкрософт. При обращении обязательно предоставьте данные соглашения о корпоративном лицензировании и подтверждение покупки.

Slmgr.vbs /ato возвращает код ошибки

Если Slmgr.vbs возвращает шестнадцатеричный код ошибки, получите соответствующее сообщение об ошибке, выполнив следующий сценарий.

```cmd
slui.exe 0x2a 0x <ErrorCode>
```

Дополнительные сведения о конкретных кодах ошибок и способах их устранения см. в разделе Устранение ошибок активации.

Рекомендации по устранению проблем с активацией, связанных с DNS.

Статья • 21.12.2022 • Чтение занимает 9 мин

Вы можете попробовать выполнить некоторые из этих инструкций, если выполняется одно или несколько из следующих условий.

- Для установки одной из следующих операционных систем используется корпоративный носитель и универсальный ключ многократной установки:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
  - Windows Server 2008
  - Windows 10
  - Windows 8.1
  - Windows 8
- Мастеру активации не удается подключиться к главному компьютеру KMS.

При попытке активировать клиентскую систему мастер активации использует DNS для размещения соответствующего компьютера, на котором работает программное обеспечение KMS. Если мастер запрашивает DNS и не находит запись DNS для главного компьютера узла KMS, он сообщает об ошибке.

Чтобы найти инструкции, соответствующие вашим условиям, просмотрите следующий список.

- Если вам не удается установить узел KMS или использовать активацию KMS, попробуйте изменить ключ продукта на MAK.
- Если вам нужно установить и настроить узел KMS, попробуйте настроить узел KMS для активации клиентов.
- Если клиенту не удается определить существующий узел KMS, выполните следующие инструкции по устранению неполадок с конфигурациями маршрутизации. Процедуры перечислены по возрастанию сложности:
  - проверьте основное IP-подключение к DNS-серверу;
  - проверьте конфигурацию узла KMS;
  - определите тип проблемы с маршрутизацией;
  - проверьте конфигурацию DNS;

- создайте запись SRV KMS вручную;
- вручную назначьте узел KMS клиенту KMS;
- настройте узел KMS для публикации в нескольких доменах DNS.

Изменение ключа продукта на MAK

Если по какой-то причине вам не удается установить узел KMS или использовать активацию KMS, попробуйте изменить ключ продукта на MAK. Если вы скачали образы Windows с сайта Microsoft Developer Network (MSDN) или TechNet, номера SKU, перечисленные под носителем, обычно связаны с корпоративными лицензиями на носители, а предоставленный ключ продукта является ключом MAK.

Чтобы изменить ключ продукта на MAK, сделайте следующее:

1. Откройте окно командной строки с повышенными правами. Для этого нажмите клавиши Windows+X, щелкните правой кнопкой мыши элемент **Командная строка** и выберите **Запуск от имени администратора**. При появлении запроса на ввод или подтверждение пароля администратора введите пароль или подтвердите его.
2. В командной строке выполните следующую команду:

```cmd
slmgr -ipk xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

> ⓘ **Примечание**
>
> Заполнитель **xxxxx-xxxxx-xxxxx-xxxxx-xxxxx** представляет ключ продукта MAK.

Вернитесь к списку инструкций.

Настройка узла KMS для активации клиентов

Для активации клиентов KMS нужно настроить узел KMS. Если в вашей среде нет узлов KMS, установите и активируйте их с помощью соответствующего ключа узла KMS. Настроив компьютер в сети для размещения программного обеспечения KMS, опубликуйте параметры DNS.

Сведения о настройке узла KMS см. в разделах Активация с помощью службы управления ключами и Установка и настройка средства управления активацией

корпоративных лицензий.

Вернитесь к списку инструкций.

Проверка основного IP-подключения к DNS-серверу

Проверьте основное IP-подключение к DNS-серверу с помощью команды ping. Для этого выполните следующие действия как на клиенте KMS, на котором возникла ошибка, так и на узле KMS:

1. Откройте окно командной строки с повышенными правами.
2. В командной строке выполните следующую команду:

```cmd
ping <DNS_Server_IP_address>
```

> ⓘ **Примечание**
>
> Если выходные данные этой команды не содержат фразу Reply from, это указывает на проблему с сетью или DNS, которую необходимо устранить, прежде чем можно будет переходить к другим инструкциям, описанным в этой статье. Узнайте больше об устранении неполадок TCP/IP при сбое проверки связи с DNS-сервером в **расширенном руководстве по устранению неполадок с TCP/IP**.

Вернитесь к списку инструкций.

Проверка конфигурации узла KMS

Проверьте реестр сервера узла службы KMS, чтобы определить, выполняется ли его регистрация в DNS. По умолчанию сервер узла службы KMS динамически регистрирует запись SRV DNS каждые 24 часа.

> ⓘ **Важно!**
>
> Внимательно выполните действия, описанные в этом разделе. Неправильное изменение реестра может привести к серьезным проблемам. Перед

внесением изменений **создайте резервную копию реестра для его восстановления** в случае возникновения проблем.

Для проверки сделайте следующее:

1. Откройте редактор реестра. Для этого щелкните правой кнопкой мыши **Пуск**, выберите **Выполнить**, введите **regedit** и нажмите клавишу ВВОД.
2. Найдите подраздел **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** (ранее вместо **SoftwareProtectionPlatform** в Windows Server 2008 и Windows Vista было указано **SL**) и просмотрите значение записи **DisableDnsPublishing**. Эта запись может иметь следующие значения:

   - **0** или не определено (по умолчанию). Сервер узла KMS регистрирует запись SRV каждые 24 часа.
   - **1**. Сервер узла KMS не регистрирует записи SRV автоматически. Если ваша реализация не поддерживает динамические обновления, см. руководство по созданию записи SRV KMS вручную.

3. Если запись **DisableDnsPublishing** отсутствует, создайте ее (тип — DWORD). Если динамическая регистрация допускается, оставьте неопределенное значение или укажите **0**.

Вернитесь к списку инструкций.

Определение типа проблемы с маршрутизацией

Вы можете определить, связана ли проблема с разрешением имен или записью SRV, с помощью следующих команд.

1. На клиенте KMS откройте окно командной строки с повышенными правами.

2. В командной строке введите следующие команды:

```cmd
cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>:<port>
cscript \windows\system32\slmgr.vbs -ato
```

Примечание

В этой команде <KMS_FQDN> представляет полное доменное имя (FQDN) главного компьютера KMS, а <port> представляет TCP-порт, используемый KMS.

Если эти команды помогли устранить проблему, значит проблема была в записи SRV. Вы можете устранить ее с помощью одной из команд, описанных в инструкциях по назначению узла KMS клиенту KMS вручную.

3. Если проблема не устранена, выполните следующие команды:

```cmd
cscript \windows\system32\slmgr.vbs -skms <IP Address>:<port>
cscript \windows\system32\slmgr.vbs -ato
```

> ⓘ **Примечание**
>
> В этой команде <IP Address> представляет IP-адрес главного компьютера KMS, а <port> представляет TCP-порт, используемый KMS.

Если эти команды помогли устранить проблему, это указывает на возможную проблему с разрешением имен. Дополнительные сведения об устранении неполадок см. в инструкциях по проверке конфигурации DNS.

4. Если ни одна из этих команд не устраняет проблему, проверьте конфигурацию брандмауэра компьютера. Любой обмен данными для активации между клиентами KMS и узлом KMS, происходит с использованием TCP-порта 1688. Брандмауэры должны разрешать обмен данными через порт 1688 как на клиенте KMS, так и на узле KMS.

Вернитесь к списку инструкций.

Проверка конфигурации DNS

> ⓘ **Примечание**
>
> Если не указано иное, выполните следующие действия на клиенте KMS, где возникла соответствующая ошибка.

1. Откройте окно командной строки с повышенными правами.
2. В командной строке выполните следующую команду:

```
cmd
```

```
IPCONFIG /all
```

3. В результатах команды изучите следующие сведения:

   - назначенный IP-адрес клиентского компьютера KMS;
   - IP-адрес основного DNS-сервера, используемого клиентским компьютером KMS;
   - IP-адрес основного шлюза по умолчанию, используемого клиентским компьютером KMS;
   - список DNS-суффиксов, используемых клиентским компьютером KMS.

4. Убедитесь, что записи SRV узла KMS зарегистрированы в DNS. Для этого выполните следующие действия:
   a. Откройте окно командной строки с повышенными правами.
   b. В командной строке выполните следующую команду:

```
cmd
```

```
nslookup -type=all _vlmcs._tcp>kms.txt
```

   c. Откройте файл KMS.txt, созданный командой. Этот файл должен содержать одну или несколько записей, которые выглядят примерно так:

```
```

```
_vlmcs._tcp.contoso.com SRV service location:
priority = 0
weight = 0
port = 1688 svr hostname = kms-server.contoso.com
```

> ⓘ **Примечание**
>
> В этой записи contoso.com представляет домен узла KMS.

   i. Проверьте IP-адрес, имя узла, порт и домен узла KMS.
   ii. Если эти записи **_vlmcs** существуют и содержат ожидаемые имена узла KMS, перейдите к инструкциям по назначению узла KMS клиенту KMS вручную.

> ⓘ **Примечание**

> Если команда **nslookup** находит узел KMS, это не значит, что клиент DNS может найти узел KMS. Если команда **nslookup** находит узел KMS, но активация с помощью узла KMS по-прежнему не удается, проверьте другие параметры DNS, включая основной суффикс DNS и список суффиксов DNS.

5. Убедитесь, что список включает суффикс домена DNS, связанный с узлом KMS. В противном случае перейдите к инструкциям по настройке узла KMS для публикации в нескольких доменах DNS.

Вернитесь к списку инструкций.

Создание записи SRV KMS вручную

Чтобы вручную создать запись SRV для узла KMS, использующего DNS-сервер Майкрософт, сделайте следующее:

1. Откройте на DNS-сервере диспетчер DNS. Чтобы открыть диспетчер DNS, щелкните **Пуск**, **Администрирование** и **Служба DNS**.
2. Выберите DNS-сервер, на котором необходимо создать запись ресурса SRV.
3. В дереве консоли разверните узел **Зоны прямого просмотра**, щелкните правой кнопкой мыши домен и выберите **Другие новые записи**.
4. Прокрутите список вниз, выберите **Расположение службы (запись SRV)** и щелкните **Создать запись**.
5. Введите следующие сведения:

   - служба — **_VLMCS**;
   - протокол — **_TCP**;
   - номер порта — **1688**;
   - узел, на котором размещена служба — ***FQDN узла KMS*** .

6. По окончании щелкните **ОК** и **Готово**.

Чтобы вручную создать запись SRV для узла KMS, использующего совместимый с BIND 9.x DNS-сервер, следуйте инструкциям по настройке этого DNS-сервера и предоставьте следующие сведения для записи SRV:

- имя — **_vlmcs._TCP**;
- тип — **SRV**;
- приоритет — **0**;
- вес — **0**;
- порт — **1688**;
- имя узла — ***FQDN или преобразованное имя узла KMS*** .

> ⓘ **Примечание**
>
> KMS не использует значения **приоритета** или **веса**. Но запись должна содержать их.

Чтобы включить для совместимого с BIND 9.x DNS-сервера поддержку автоматической публикации KMS, включите для него обновление записей ресурсов с узлов KMS. Например, добавьте следующую строку в определение зоны в файле Named.conf или Named.conf.local:

```
cmd

allow-update { any; };
```

Назначение узла KMS клиенту KMS вручную

По умолчанию клиенты KMS используют процесс автоматического обнаружения. При этом клиент KMS запрашивает у DNS список серверов, которые опубликовали записи SRV `_vlmcs` в зоне членства клиента. DNS возвращает список узлов KMS в случайном порядке. Клиент выбирает узел KMS и пытается открыть на нем сеанс. Если попытка удается, клиент кэширует имя узла KMS и попытается использовать его для следующей попытки продления. В случае сбоя клиент случайным образом выбирает другой узел KMS. Мы настоятельно рекомендуем использовать процесс автоматического обнаружения.

Но вы также можете назначить узел KMS определенному клиенту KMS. Для этого выполните следующие действия.

1. На клиенте KMS откройте окно командной строки с повышенными правами.
2. В зависимости от реализации выполните одно из следующих действий:

   - Чтобы назначить узел KMS с помощью FQDN, выполните следующую команду:

     ```
     cmd

     cscript \windows\system32\slmgr.vbs -skms <KMS_FQDN>:<port>
     ```

   - Чтобы назначить узел KMS с помощью IPv4, выполните следующую команду:

     ```
     cmd
     ```

```
cscript \windows\system32\slmgr.vbs -skms <IPv4Address>:<port>
```

- Чтобы назначить узел KMS с помощью IPv6, выполните следующую команду:

```
cmd
cscript \windows\system32\slmgr.vbs -skms <IPv6Address>:<port>
```

- Чтобы назначить узел KMS с помощью NetBIOS, выполните следующую команду:

```
cmd
cscript \windows\system32\slmgr.vbs -skms <NETBIOSName>:<port>
```

- Чтобы вернуться к автоматическому обнаружению на клиенте KMS, выполните следующую команду:

```
cmd
cscript \windows\system32\slmgr.vbs -ckms
```

> ⓘ **Примечание**
>
> В этих командах используются следующие заполнители:
> - **KMS_FQDN>>** — полное доменное имя (FQDN) главного компьютера KMS;
> - **>IPv4Address** — IP-адрес версии 4 главного компьютера KMS;
> - **>IPv6Address** — IP-адрес версии 6 главного компьютера KMS;
> - **>NETBIOSName** — имя NetBIOS главного компьютера KMS;
> - **port>** — TCP-порт, используемый KMS.

Настройка узла KMS для публикации в нескольких доменах DNS

> ⓘ **Важно!**
>
> Внимательно выполните действия, описанные в этом разделе. Неправильное изменение реестра может привести к серьезным проблемам. Перед

внесением изменений **создайте резервную копию реестра для его восстановления** в случае возникновения проблем.

Как описано в инструкциях по назначению узла KMS клиенту KMS вручную, клиенты KMS обычно используют процесс автоматического обнаружения для обнаружения узлов KMS. Для этого необходимо, чтобы записи SRV `_vlmcs` были доступными в зоне DNS клиентского компьютера KMS. Зона DNS соответствует либо основному DNS-суффиксу компьютера, либо одному из следующих компонентов:

- для компьютеров, присоединенных к домену, — домену компьютера, назначенному системой DNS (например, DNS AD DS);
- для компьютеров, входящих в рабочую группу — домену компьютера, назначенному протоколом DHCP. Это доменное имя определяется параметром с кодом, имеющим значение 15, как определено в RFC 2132.

По умолчанию узел KMS регистрирует свои записи SRV в зоне DNS, которая соответствует домену главного компьютера KMS. Например, предположим, что узел KMS присоединяется к домену contoso.com. В этом сценарии узел KMS регистрирует свою запись SRV `_vlmcs` в зоне DNS contoso.com. Таким образом, запись идентифицирует службу как `_VLMCS._TCP.CONTOSO.COM`.

Если узел и клиенты KMS используют разные зоны DNS, вам нужно включить для узла KMS автоматическую публикацию записей SRV в нескольких доменах DNS. Для этого выполните следующие действия:

1. На узле KMS откройте редактор реестра.
2. Найдите и выберите подраздел **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform** (ранее вместо **SoftwareProtectionPlatform** в Windows Server 2008 и Windows Vista было указано **SL**).
3. В разделе **Сведения** щелкните правой кнопкой мыши пустую область, а затем выберите **Создать** и **Мультистроковый параметр**.
4. В качестве имени новой записи введите **DnsDomainPublishList**.
5. Щелкните правой кнопкой мыши новую запись **DnsDomainPublishList** и выберите **Изменить**.
6. В диалоговом окне **Редактирование мультистроки** введите в отдельную строку каждый суффикс домена DNS, который KMS публикует, и щелкните **OK**.

> ⓘ **Примечание**

В Windows Server 2008 R2 формат для **DnsDomainPublishList** отличается. Сведения см. в техническом справочнике по активации корпоративных лицензий.

7. С помощью средства администрирования служб перезапустите службу защиты программного обеспечения (ранее называлась службой лицензирования программного обеспечения в Windows Server 2008 и Windows Vista). Эта операция создает записи SRV.
8. Убедитесь, что клиент KMS может связаться с настроенным узлом KMS, используя стандартную процедуру. Убедитесь, что клиент KMS правильно определяет узел KMS как по имени, так и по IP-адресу. Если какая-либо из этих проверок завершится неудачей, изучите эту проблему с сопоставителем клиентов DNS.
9. Чтобы очистить все ранее кэшированные имена узлов KMS на клиенте KMS, откройте окно командной строки с повышенными правами на клиенте KMS и выполните следующую команду:

```cmd
cscript C:\Windows\System32\slmgr.vbs -ckms
```

Перестроение файла Tokens.dat

Статья • 28.01.2023 • Чтение занимает 2 мин

При устранении неполадок, связанных с активацией Windows, может потребоваться перестроить файл Tokens.dat. В данной статье подробно описано, как это сделать.

Разрешение

Чтобы перестроить файл Tokens.dat, выполните следующие действия.

1. Откройте окно командной строки с повышенными привилегиями. **Для Windows 10**
   a. Откройте меню **Пуск** и введите **cmd**.
   b. В списке результатов щелкните правой кнопкой мыши **Командная строка**, а затем выберите **Запуск от имени администратора**.

   Для Windows 8.1
   a. Проведите пальцем от правого края экрана, а затем коснитесь **Найти**. Если вы используете мышь, наведите указатель мыши на правый нижний угол экрана, а затем выберите **Найти**.
   b. В поле поиска введите **cmd**.
   c. Проведите пальцем по отображенному значку **Командная строка** или щелкните его правой кнопкой мыши.
   d. Коснитесь или щелкните **Запуск от имени администратора**.

   Для Windows 7
   a. Откройте меню **Пуск** и введите **cmd**.
   b. В результатах поиска щелкните правой кнопкой мыши файл **cmd.exe** и выберите **Запуск от имени администратора**.

2. Введите набор команд, подходящих для вашей операционной системы.

   Для Windows 10, Windows Server 2016 и более поздних версий Windows последовательно введите следующие команды.

   cmd

   ```
   net stop sppsvc
   cd %Systemdrive%\Windows\System32\spp\store\2.0\
   ren tokens.dat tokens.bar
   net start sppsvc
   cscript.exe %windir%\system32\slmgr.vbs /rilc
   ```

Для Windows 8.1, Windows Server 2012 и Windows Server 2012 R2 последовательно введите следующие команды.

```
cmd

net stop sppsvc
cd %Systemdrive%\Windows\System32\spp\store\
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

Для Windows 7, Windows Server 2008 и Windows Server 2008 R2 последовательно введите следующие команды.

```
cmd

net stop sppsvc
cd
%Systemdrive%\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Mi
crosoft\SoftwareProtectionPlatform
ren tokens.dat tokens.bar
net start sppsvc
cscript.exe %windir%\system32\slmgr.vbs /rilc
```

3. Перезагрузите компьютер.

Дополнительные сведения

После перестроения файла Tokens.dat необходимо переустановить ключ продукта с помощью одного из следующих методов.

- В той же командной строке с повышенными привилегиями введите приведенную ниже команду и нажмите клавишу ВВОД.

```
cmd

cscript.exe %windir%\system32\slmgr.vbs /ipk <Product key>
```

> ⓘ **Важно!**
>
> Не используйте параметр **/upk** для удаления ключа продукта. Чтобы установить ключ продукта вместо имеющегося ключа продукта, используйте параметр **/ipk**.

- Щелкните правой кнопкой мыши **Мой компьютер**, выберите **Свойства**, а затем выберите **Изменить ключ продукта**.

Дополнительные сведения о ключах установки клиента KMS см. в разделе Ключи установки клиента KMS.

Пример: Устранение неполадок клиентов активации на основе Active Directory (ADBA), которые не активируются

Статья • 29.09.2022 • Чтение занимает 6 мин

> **Примечание**
>
> Эта статья была первоначально опубликована в блоге TechNet 26 марта 2018 года.

Всем привет. Меня зовут Майк Каммер, и я уже два года участвую в проекте Platforms PFE корпорации Майкрософт. Недавно я помог клиенту развернуть Windows Server 2016 в своей среде. Мы также использовали эту возможность, чтобы перенести их методику активации с сервера KMS на активацию на основе Active Directory.

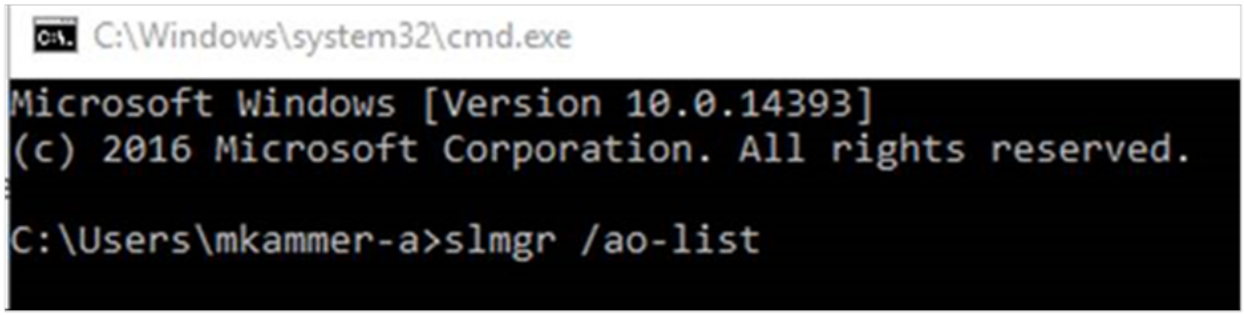
Следуя правильной процедуре внесения любых изменений, мы начали миграцию в тестовой среде клиента. Мы начали развертывание, следуя инструкциям, приведенным в этой отличной записи блога Чарити Шелборн: Active Directory-Based Activation vs. Key Management Services (Активация на основе Active Directory и службы управления ключами). Контроллеры домена в нашей тестовой среде работали под управлением Windows Server 2012 R2, поэтому нам не нужно было подготавливать лес. Мы установили роль на контроллере домена Windows Server 2012 R2 и выбрали активацию на основе Active Directory в качестве метода активации корпоративных лицензий. Мы установили ключ KMS и присвоили ему имя "KMS AD Activation (** LAB)". Мы довольно точно следовали инструкциям в записи блога.

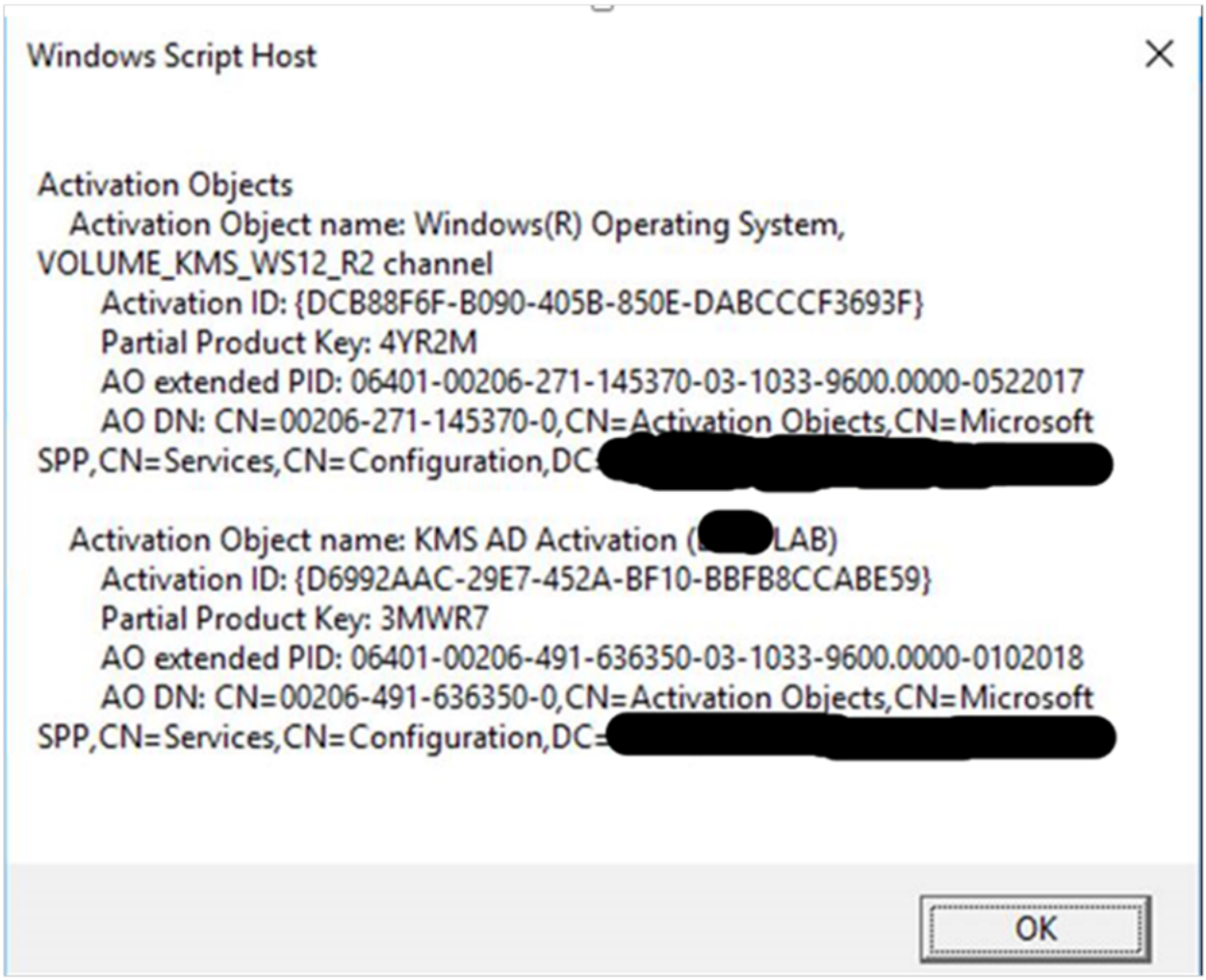
Сначала мы создали четыре виртуальных машины: две под управлением Windows 2016 Standard и две под управлением Windows 2016 Datacenter. На этом этапе все шло замечательно и все было довольны. Мы создали физический сервер под управлением Windows 2016 Standard, и он правильно активировался. Тут и сказочке конец.

Ха-ха! Шучу! Все было не так просто. На самом деле установка и настройка были очень простыми, так что эта часть была простой и понятной. Я вернулся в офисе в понедельник, и оказалось, что все виртуальные машины, которые я создал неделей

раньше, не активированы. Эй! Это же не правильно. Я вернулся к физическому компьютеру, и он был в порядке. Я отправился к клиенту, чтобы обсудить, что произошло. Конечно, первым вопросом был: "Что изменилось за выходные?" И, как обычно, в ответ я услышал: "Ничего". На этот раз действительно ничего не изменилось, и нам пришлось выяснить, что же происходило.

Я подошел к одному из проблемных серверов, открыл командную строку и проверил выходные данные команды **slmgr /ao-list**. Параметр **/ao-list** отображает все объекты активации в Active Directory.

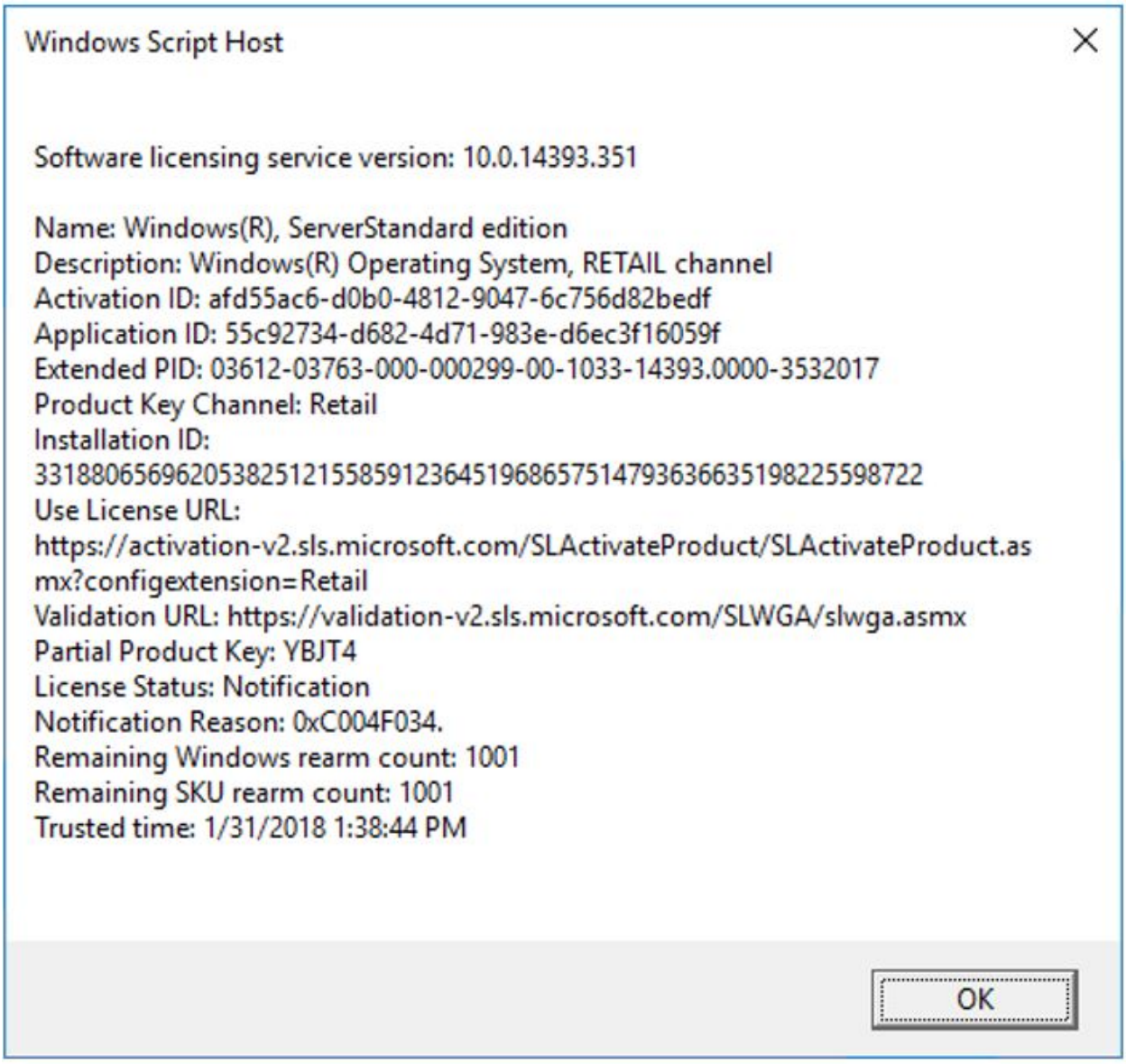




Результаты показывают, что имеются два объекта активации: один для Windows Server 2012 R2 и один для недавно созданного ключа KMS AD Activation (** LAB), который является лицензией на Windows Server 2016. Это подтверждает, что

конфигурация Active Directory правильно настроена для активации клиентов KMS для Windows.

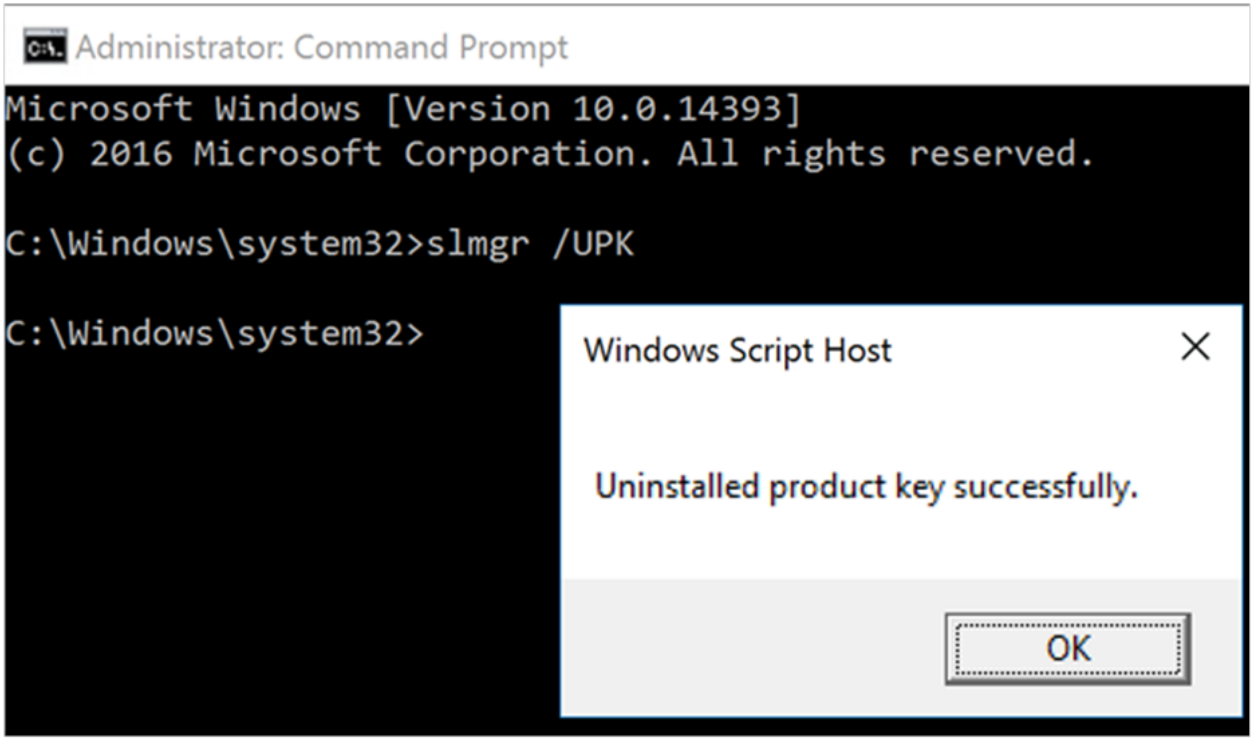
Зная, что команда **slmgr** — мой надежный помощник для активации лицензий, я продолжил использовать ее с разными параметрами. Я пробовал параметр **/dlv**, который отображает подробные сведения о лицензиях. Все выглядело хорошо. Я использовал версию Windows Server 2016 Standard и были указаны идентификатор активации, идентификатор установки, URL-адрес проверки и даже частичный ключ продукта.



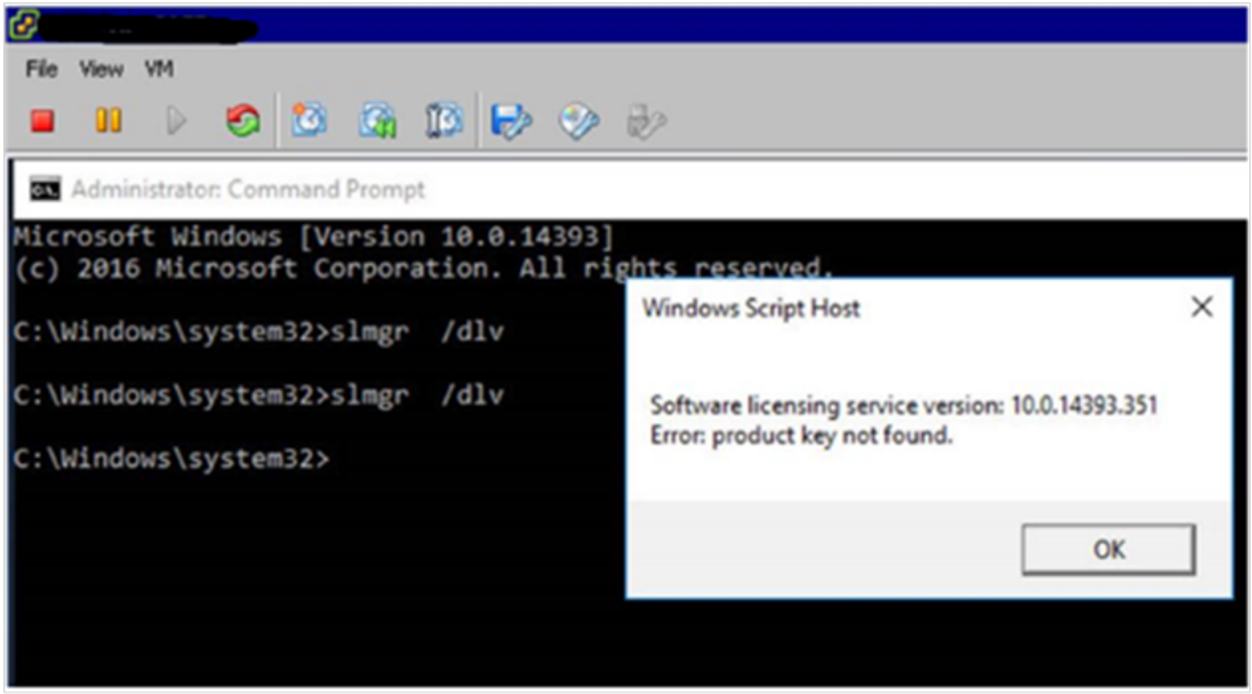
Кто-нибудь заметил, что я пропустил на этом этапе? Мы вернемся к этому, когда я расскажу о других своих действиях по устранению неполадок, но достаточно сказать, что ответ находится на этом снимке экрана.

Теперь я думал, что по какой-то причине ключ поврежден, поэтому я использовал параметр **/upk**, который удаляет текущий ключ. Хотя ключ действительно удаляется, это далеко не лучший способ. Перезагрузка сервера перед получением нового ключа может оставить сервер в неработоспособном состоянии. Я

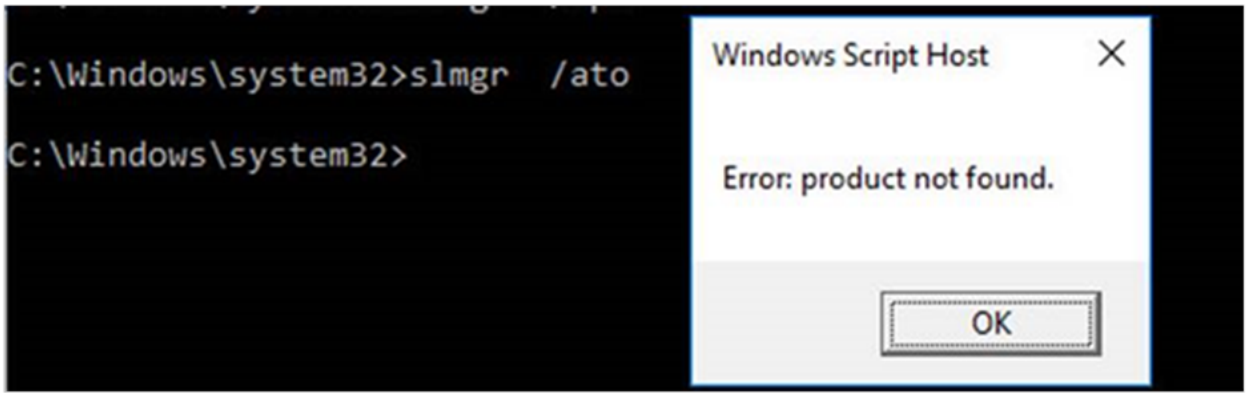
обнаружил, что параметр **/ipk** (что я сделаю позже при устранении неполадок) перезаписывает существующий ключ и является намного более безопасным путем. Учитесь на моих промахах!



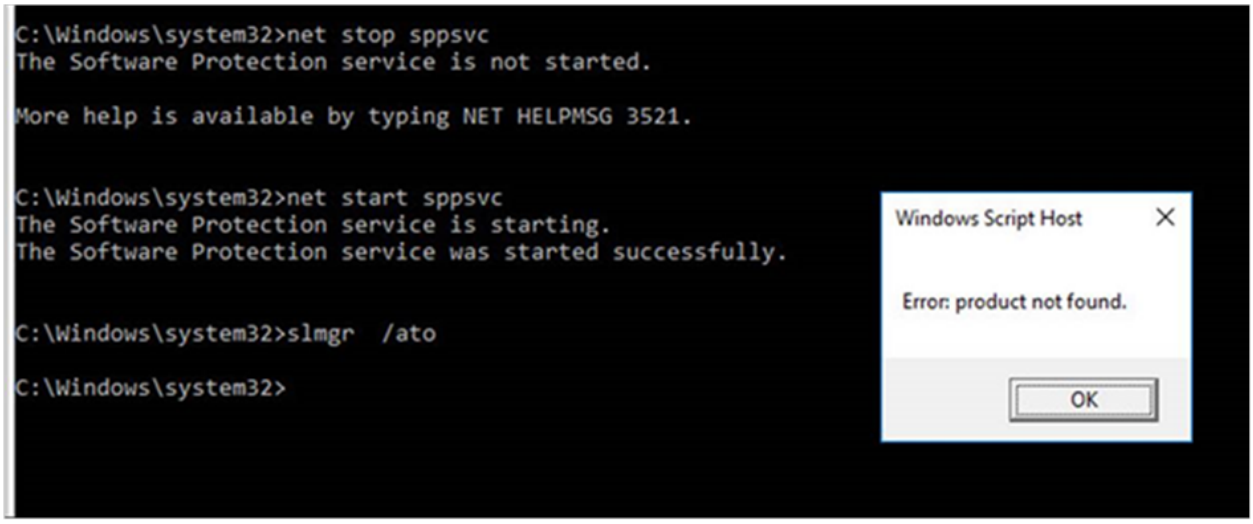
Я выполнил команду с параметром **/dlv**, чтобы просмотреть подробные сведения о лицензиях. К сожалению, ничего полезного я не узнал, а просто увидел ошибку "ключ продукта не найден". Ну конечно, ключа нет, ведь я только что удалил его!



Я понял, что вероятность успеха невелика, но пытался использовать параметр **/ato**, который должен активировать Windows на известных серверах KMS (или Active Directory, что тоже возможно). И опять ошибка "продукт не найден".

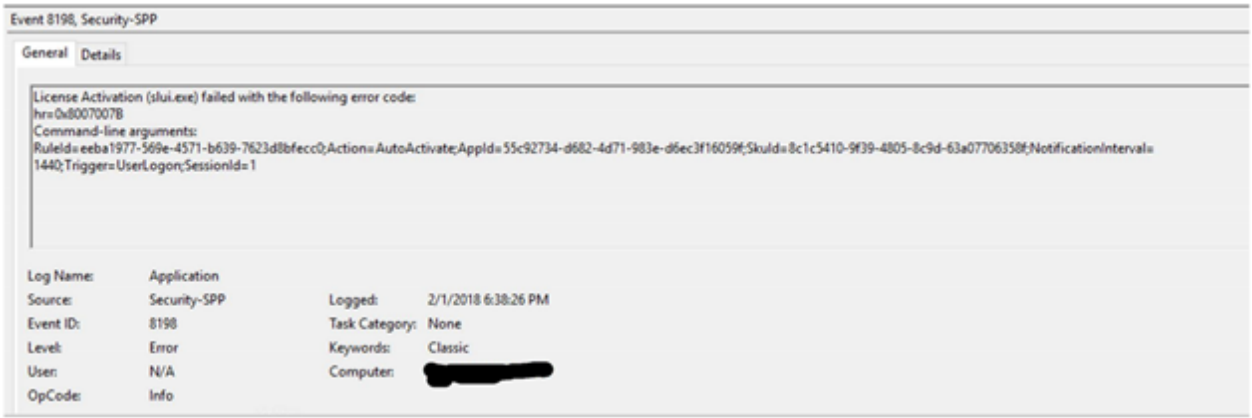


Моей следующей мыслью было, что иногда помогает остановка и запуск службы, поэтому я испробовал это. Мне нужно было остановить и запустить службу платформы защиты программного обеспечения Майкрософт (службу SPPSvc). В командной строке с правами администратора я использовал проверенные команды **net stop** и **net start**. Сначала я было решил, что служба не работает и проблема именно в этом.



Но нет. После запуска службы и попытки повторной активации Windows я по-прежнему получал сообщение об ошибке "продукт не найден".

Затем я просмотрел журнал событий приложений на одном из проблемных серверов. Я обнаружил ошибку, связанную с активацией лицензии, событие с идентификатором 8198 и кодом 0x8007007B.



При поиске этого кода я нашел статью, в которой написано, что мой код ошибки указывает на неправильный синтаксис имени файла, имени каталога или метки тома. Почитав методы, описанные в статье, я понял, что они не очень подходят для моего случая. Когда я выполнил команду **nslookup -type=all _vlmcs._tcp**, я нашел имеющийся сервер KMS (в среде все еще было много компьютеров под управлением Windows 7 и Windows Server 2008, поэтому он был необходим), а также пять контроллеров домена. Это означает, что неполадка не связана с DNS, и проблемы возникли где-то еще.

```
nslookup -type=all _vlmcs._tcp>kms.txt

Server:  labdns1.CONTOSO.COM
Address:  10.10.14.11

_vlmcs._tcp.CONTOSO.COM    SRV service location:
          priority       = 0
          weight         = 0
          port           = 1688
          svr hostname   = labKMS.CONTOSO.COM

_tcp.CONTOSO.COM   nameserver = labDC2.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = remDC1.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = labDC4.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = labDC1.CONTOSO.COM
_tcp.CONTOSO.COM   nameserver = labDC3.CONTOSO.COM
labKMS.CONTOSO.COM  internet address = 10.10.14.100
labDC1.CONTOSO.COM   internet address = 10.10.14.26
remDC1.CONTOSO.COM   internet address = 10.10.20.88
labDC4.CONTOSO.COM   internet address = 10.10.14.27
labDC3.CONTOSO.COM   internet address = 10.10.14.34
labDC2.CONTOSO.COM   internet address = 10.10.14.44
```

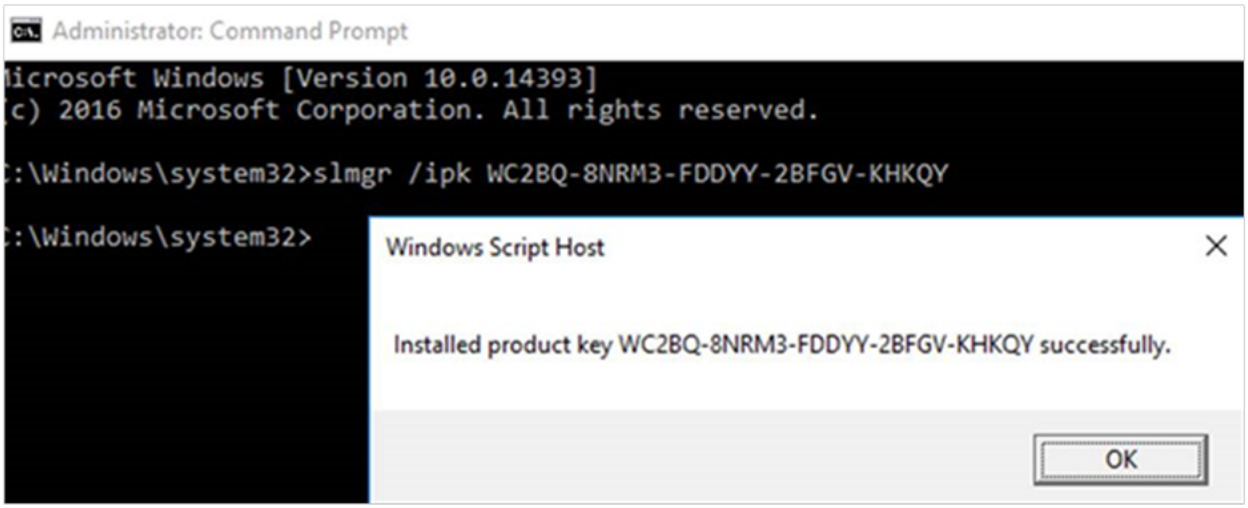
Итак, я знал, что DNS в порядке. Служба Active Directory правильно настроена в качестве источника активации с помощью KMS. Мой физический сервер активирован правильно. Возможно, проблема связана только с виртуальными машинами? Интересное примечание: в тот момент мой клиент говорит мне, что кто-то в другом отделе также решил создать более десятка виртуальных машин Windows Server 2016. Итак, я полагаю, что теперь у меня есть еще десяток серверов, которые не активируются. Но нет! Эти серверы активировались без проблем.

Что же, я снова взялся за команду **slmgr**, чтобы узнать, как активировать этих монстров. На этот раз я собирался использовать параметр **/ipk**, который позволит установить ключ продукта. Я перешел на этот сайт, чтобы получить соответствующие ключи для версии Windows Server 2016 Standard. Некоторые из моих серверов работают под управлением версии Datacenter, но мне нужно было сначала исправить этот сервер.

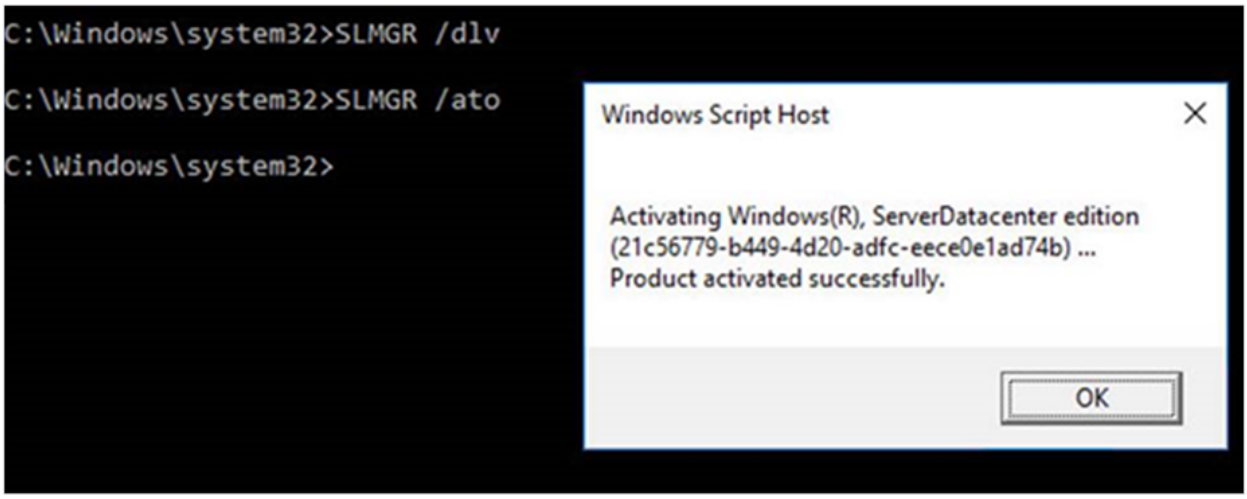
Windows Server 2016

Operating system edition	KMS Client Setup Key
Windows Server 2016 Datacenter	CB7KF-BWN84-R7R2Y-793K2-8XDDG
Windows Server 2016 Standard	WC2BQ-8NRM3-FDDYY-2BFGV-KHKQY
Windows Server 2016 Essentials	JCKRF-N37P4-C2D82-9YXRT-4M63B

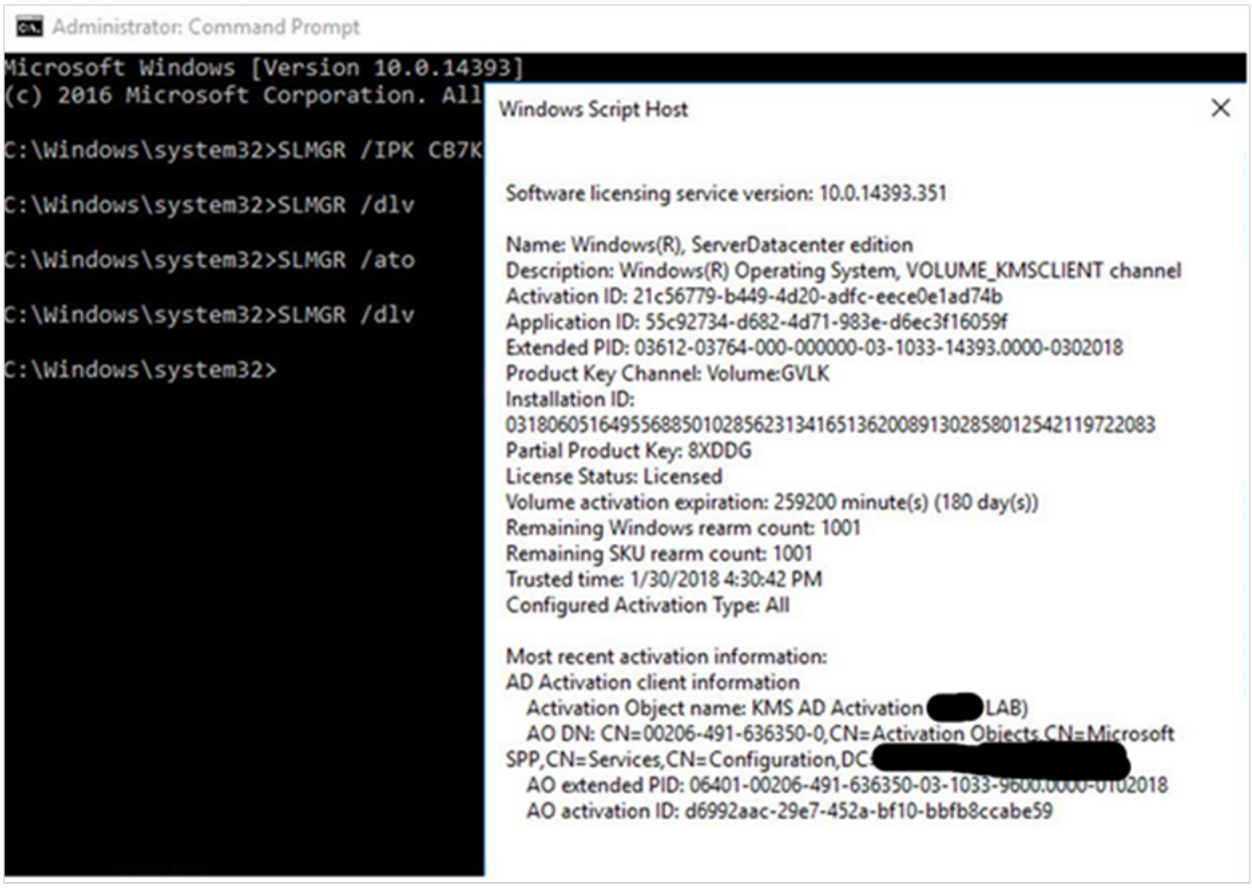
Я использовал параметр **/ipk** для установки ключа продукта, выбрав ключ Windows Server 2016 Standard.



Здесь я записал только результаты для версии Datacenter, но они такие же. Для принудительной активации я использовал параметр **/ato**. Мы получаем чудесное сообщение о том, что продукт был успешно активирован!

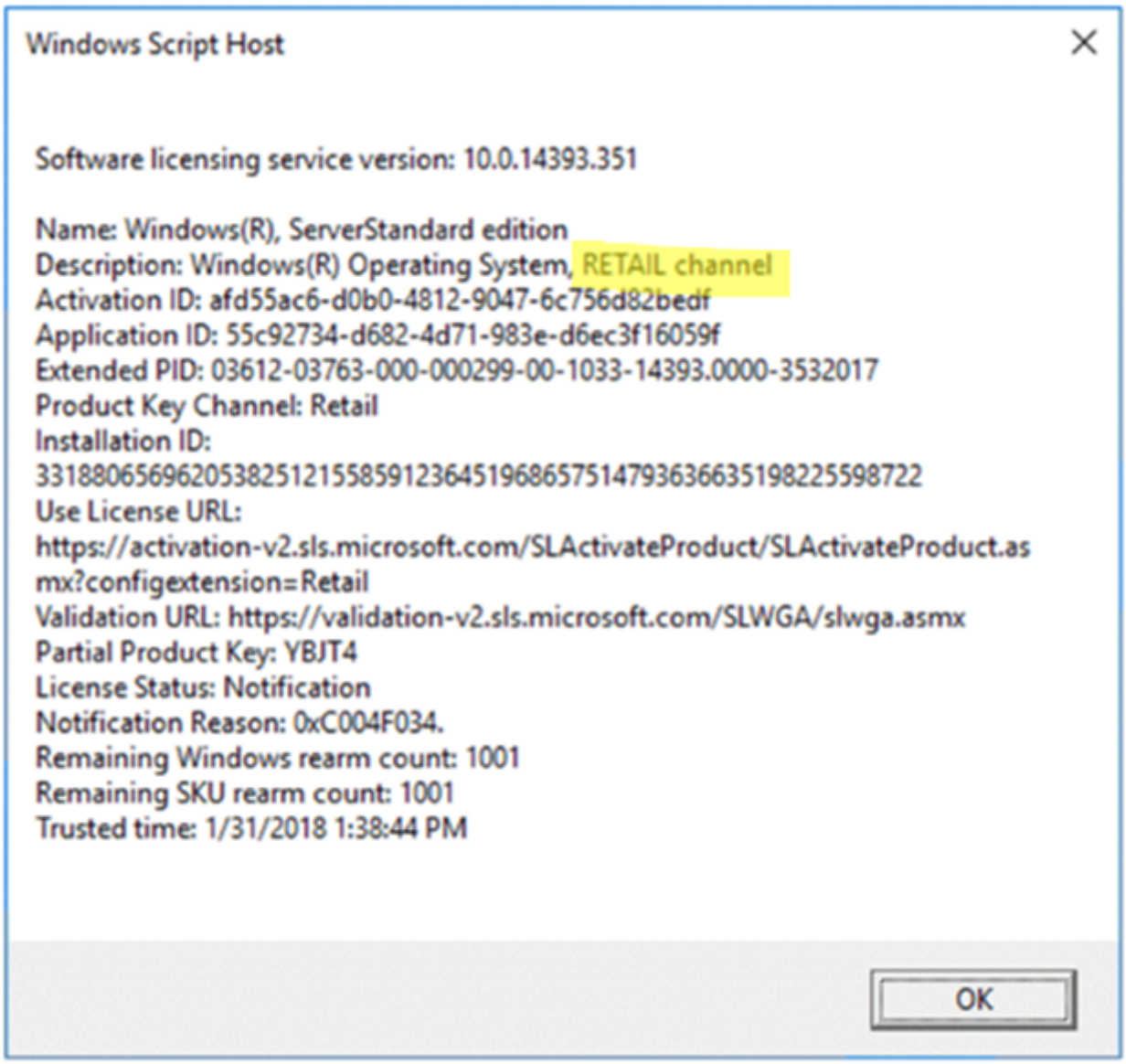


Еще раз воспользовавшись параметром **/dlv**, можно было увидеть, что мы выполнили активацию с помощью Active Directory.

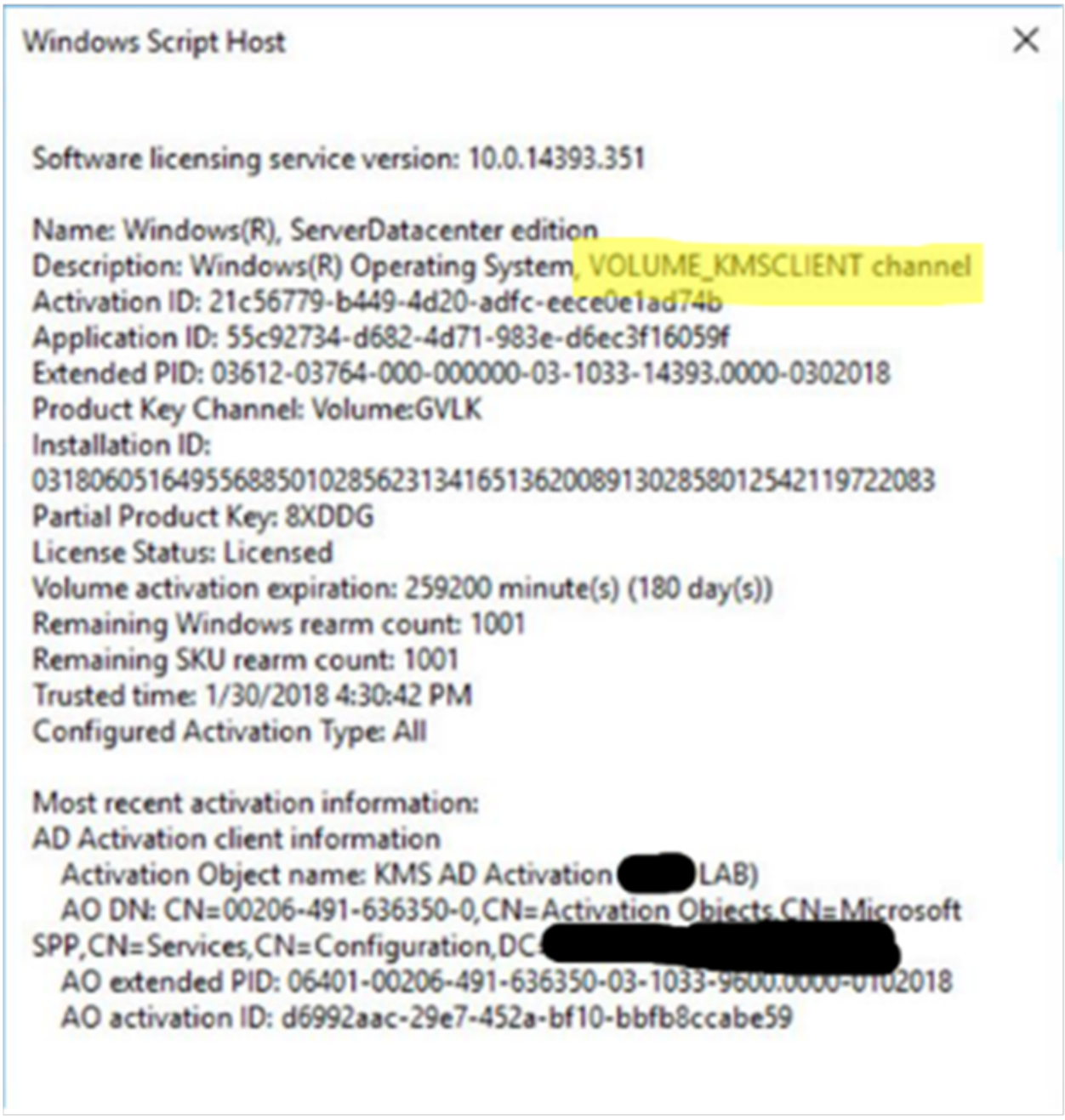


Итак, что же пошло не так? Почему мне пришлось удалить установленный ключ и добавить эти универсальные ключи, чтобы обеспечить правильную активацию этих компьютеров? Почему десяток (или около того) других компьютеров был активирован без каких-либо проблем? Как я уже говорил, я пропустил кое-что важное на начальных этапах изучения проблемы. Я был в сильном недоумении, поэтому обратился к Чарити из первоначальной записи блога, чтобы узнать, сможет ли она помочь. Она сразу же обнаружила проблему и помогла мне понять, что я упустил с самого начала.

Ключ был в описании в выходных данных команды с параметром **/dlv**. Описание содержало следующее: Windows® Operating System, RETAIL Channel. Я видел это и решил, что канал RETAIL означал, что лицензия была приобретена и имела допустимый ключ.



Если взглянуть на выходные данные команды с параметром **/dlv**, выполненной на правильно активированном сервере, можно заметить, что в описании уже указан канал VOLUME_KMSCLIENT. Это дает нам понять, что это действительно корпоративная лицензия.



Что же означает канал RETAIL? Это означает, что носителем, использованным для установки операционной системы, был ISO-файл с сайта MSDN. Я вернулся к клиенту и спросил, существует ли вероятность того, что в сети есть второй ISO-файл Windows Server 2016. Оказалось, что да, в сети есть другой ISO-файл, который использовался для создания десятка других компьютеров. Они сравнили эти два ISO-файла — и, разумеется, образ, который мне предоставили для создания виртуальных серверов, оказался ISO-файлом MSDN. Они удалили этот ISO-файл MSDN из сети, и теперь все наши серверы были активированы и можно было не беспокоиться о сбое активации в будущих сборках.

Надеюсь, эта история была полезна и вы можете сэкономить немного своего времени.

Майк

Состояние выпуска Windows

Официальные сведения о выпусках Windows и вехах обслуживания, а также ресурсы, средства и новости об известных проблемах и средствах защиты, которые помогут вам спланировать следующее обновление. Нужны последние обновления работоспособности выпуска Windows? Подпишитесь @WindowsUpdate на Twitter.

GET STARTED
Как получить обновление Windows 11...

WHAT'S NEW
Новые возможности для Windows...

GET STARTED
Как получить обновление Windows 10...

REFERENCE
Просмотрите блог о летнем & часовом...

REFERENCE
Сведения о выпуске Windows 11

OVERVIEW
Общее представление о...

Центр сообщений

- Take action: April 2023 security update available for all supported versions of Windows
- Reminder: End of servicing for Windows 10 version 21H2 (Editions: Home, Pro, Pro Education and Pro for Workstations)
- Take action: Review Windows Autopatch Tenant Management for potential action required to prevent inactive status

See more >

Windows 11 версии 22H2

- Known issues
- Resolved issues
- Release notes
- Windows 11 release information
- How to get Windows 11, version 22H2

Windows 10 версии 22H2

- Known issues
- Resolved issues
- Release notes
- Windows 10 release information

Windows 11 версии 21H2

- Known issues
- Resolved issues
- Release notes
- Windows 11 release information

How to get Windows 10, version 22H2

How to get Windows 11

Windows 10 версии 21H2

- Known issues
- Resolved issues
- Release notes
- Windows 10 release information
- How to get Windows 10, version 21H2

Windows Server 2022

- Known issues
- Resolved issues
- Release notes
- Windows Server release information
- What's new in Windows Server 2022

Windows 10 версии 20H2

- Known issues
- Resolved issues
- Release notes
- Windows 10 release information

Дополнительные версии

См. сведения об известных и разрешенных проблемах для других поддерживаемых версий Windows и Windows Server.

- Known issues: earlier versions

Есть вопросы? Присоединяйтесь к часам работы!

Получите настраиваемые рекомендации, советы и ответы на свои вопросы.

Отправить отзыв

Поделитесь своими идеями о существующих функций или идеями для новых с помощью центра отзывов.

Справка

Ресурсы, которые помогут вам устранить распространенные проблемы и получить поддержку от...

Windows Server — условия лицензии

Статья • 29.09.2022 • Чтение занимает 2 мин

ознакомьтесь с нашими условиями лицензии, относящимися к серверу Windows.

- Дополнительное программное обеспечение для Windows Server 2016
- Окончание срока действия Windows Server Technical Preview
- Windows Server 2016 условия лицензионного соглашения на техническую версию
- Условия лицензионного соглашения на использование программного обеспечения корпорации Майкрософт — Майкрософт. WINDOWSSERVER. системинсигхтс
- Условия лицензионного соглашения на использование программного обеспечения корпорации Майкрософт — Майкрософт. WINDOWSSERVER. СИСТЕМИНСИГХТС. РЕЧЬ
- условия лицензии Windows Admin Center