Новые возможности Windows Server 2025

- Применяется к: ☑ Windows Server 2025

В этой статье описываются некоторые новейшие разработки в Windows Server 2025, которые могут похвастаться расширенными функциями, которые повышают безопасность, производительность и гибкость. Благодаря более быстрым возможностям хранения и возможности интеграции с гибридными облачными средами управление инфраструктурой теперь упрощается. Windows Server 2025 основывается на сильном фундаменте своего предшественника и представляет ряд инновационных улучшений для адаптации к вашим потребностям.

Возможности рабочего стола и обновление

Ознакомьтесь с параметрами обновления и возможностями рабочего стола.

Локальное обновление с Windows Server 2012 R2

Windows Server 2025 позволяет обновлять до четырех версий одновременно. Вы можете выполнить обновление непосредственно до Windows Server 2025 с Windows Server 2012 R2 и более поздних версий.

Оболочка рабочего стола

При первом входе оболочка рабочего стола соответствует стилю и внешнему виду Windows 11.

Bluetooth

Теперь вы можете подключать мыши, клавиатуры, гарнитуры, звуковые устройства и многое другое через Bluetooth в Windows Server 2025.

DTrace

Windows Server 2025 поставляется с `dtrace` в качестве собственного средства. DTrace — это программа командной строки, которая позволяет пользователям отслеживать и устранять неполадки производительности системы в режиме реального времени. С помощью DTrace можно динамически инструментировать код ядра и пространства пользователя без необходимости изменять сам код. Это универсальное средство поддерживает ряд методов сбора и анализа данных, таких как агрегаты, гистограммы и трассировка событий на уровне пользователя. Дополнительные сведения см. в разделе DTrace для справки по командной строке и DTrace в Windows для получения информации о других возможностях.

Электронная почта и учетные записи

Теперь можно добавить следующие типы учетных записей в параметры Windows в разделе "Учетные записи **">учетные записи электронной почты &** для Windows Server 2025:

- Microsoft Entra ID
- Microsoft account
- Рабочая или учебная учетная запись

Присоединение к домену по-прежнему требуется для большинства ситуаций.

Центр отзывов

Чтобы отправить отзыв или сообщить о проблемах, возникающих при использовании Windows Server 2025, используйте Центр отзывов Windows. Включите снимки экрана или записи процесса, вызвавшего проблему, чтобы помочь нам понять вашу ситуацию и поделиться предложениями по улучшению возможностей Windows. Дополнительные сведения см. в статье "Обзор Центра отзывов".

Сжатие файлов

Windows Server 2025 имеет новую функцию сжатия. Чтобы сжать элемент, щелкните правой кнопкой мыши и выберите **Сжатие до**. Эта функция поддерживает **ZIP-**, **7z**и **форматы сжатия TAR** с определенными методами сжатия для каждого из них.

Закрепленные приложения

Закрепление наиболее часто используемых приложений теперь доступно в меню **"Пуск"** и может быть настроено в соответствии с вашими потребностями. Приложения, закрепленные по умолчанию, в настоящий момент следующие:

- Настройка Azure Arc
- Центр отзывов
- File Explorer
- Microsoft Edge
- Диспетчер серверов
- Settings
- Terminal
- Windows PowerShell

Диспетчер задач

Windows Server 2025 использует современное приложение «Диспетчер задач» с материалом Mica, соответствующим стилю Windows 11.

Wi-Fi

Теперь проще включить беспроводные возможности, так как функция беспроводной локальной сети теперь устанавливается по умолчанию. Служба беспроводной связи

настроена на ручной запуск. Чтобы включить его, запустите `net start wlansvc` в командной строке, терминале Windows или PowerShell.

Терминал Windows

В Windows Server 2025 доступен Терминал Windows — мощное и эффективное многофункциональное приложение для пользователей командной строки. Найдите **Терминал** в строке поиска.

WinGet

WinGet устанавливается по умолчанию, который является средством диспетчера пакетов Windows командной строки, предоставляющим комплексные решения диспетчера пакетов для установки приложений на устройствах Windows. Дополнительные сведения см. в статье Использование средства WinGet для установкиприложений и управления ими.

Расширенная многоуровневая безопасность

Сведения о безопасности в Windows 2025.

Hotpatch (предварительная версия)

Hotpatch теперь доступен для компьютеров Windows Server 2025, подключенных к Azure Arc после включения Hotpatch на портале Azure Arc. Вы можете использовать Hotpatch для применения обновлений безопасности ОС без перезапуска компьютера. Чтобы узнать больше, см. Hotpatch.

> **Внимание**
>
> Hotpatch с поддержкой Azure Arc в настоящее время находится в предварительной версии. Юридические условия, применимые к функциям Azure, которые находятся в состоянии бета-версии, предварительной версии или иным образом еще не выпущены в общедоступной версии, см. на странице **Дополнительные условия использования предварительных версий в Microsoft Azure**.

Защита учетных данных

Начиная с Windows Server 2025, Credential Guard теперь включен по умолчанию на устройствах, отвечающих требованиям. Дополнительные сведения о Credential Guard см. в разделе "Настройка Credential Guard".

Доменные службы Active Directory

Последние усовершенствования служб домен Active Directory (AD DS) и упрощенных доменных служб Active Directory (AD LDS) представляют ряд новых функций и возможностей, направленных на оптимизацию возможностей управления доменами:

- **Опциональная функция размера страницы базы данных 32k**: Active Directory использует базу данных расширяемого хранилища (ESE) с момента внедрения в Windows 2000, которая использует размер страницы базы данных 8k. Решение архитектуры 8k привело к ограничениям в Active Directory, которые описаны в максимальных ограничениях Active Directory: масштабируемость. Примером этого ограничения является один объект Active Directory записи, который не может превышать 8k-байт. Переход к формату страницы базы данных 32k обеспечивает огромное улучшение областей, затронутых устаревшими ограничениями. Многозначные атрибуты теперь могут содержать около 3200 значений, что увеличивается на 2,6.

  Вы можете установить новые контроллеры домена (DCs) с базой данных на 32 тысячи страниц, использующей 64-разрядные идентификаторы длинных значений (LIDs), и работать в 8k-страничном режиме для совместимости с предыдущими версиями. Обновленный контроллер домена продолжает использовать текущий формат базы данных и 8 кб страниц. Переход к базе данных на 32 тыс. страниц осуществляется для всего леса и требует, чтобы все контроллеры домена в лесу имели базу данных, поддерживающую 32 тыс. страниц.

- **обновления схемы Active Directory**: вводятся три новых файла базы данных журнала, расширяющие схему Active Directory: `sch89.ldf`, `sch90.ldf`и `sch91.ldf`. Обновления эквивалентной схемы AD LDS находятся в `MS-ADAM-Upgrade3.ldf`. Дополнительные сведения о предыдущих обновлениях схемы см. в обновлениях схемы Windows Server Active Directory.
- **восстановление объектов Active Directory**: администраторы предприятия теперь могут восстановить объекты с отсутствующими основными атрибутами `SamAccountType` и `ObjectCategory`. Администраторы предприятия могут обнулить атрибут `LastLogonTimeStamp` у объекта, установив его на текущее время. Эти операции выполняются с помощью новой функции модификации RootDSE, применяемой на затронутом объекте с именем `fixupObjectState`.
- **Поддержка аудита привязки канала**: Теперь вы можете включить события 3074 и 3075 для привязки канала протокола Легкого Доступа к Каталогу (LDAP). Если политика привязки канала изменяется на более безопасный параметр, администратор может определить устройства в этой среде, которые не поддерживают или не могут осуществить привязку канала. Эти события аудита также доступны в Windows Server 2022 и более поздних версиях через KB4520412.
- **улучшения алгоритма определения местоположения контроллера домена**: Алгоритм обнаружения контроллера домена предоставляет новую функциональность с улучшением сопоставления коротких доменных имен в стиле NetBIOS с доменными именами в стиле DNS. Дополнительные сведения см. в статье Поиск контроллеров домена в Windows и Windows Server.

  Примечание.

  Windows не использует почтовые слоты во время операций обнаружения контроллеров домена, так как корпорация Майкрософт объявила об устаревании WINS и почтовых слотов для этих устаревших технологий.

- **Функциональные уровни леса и домена**: новый функциональный уровень используется для общей поддерживаемости и требуется для новой функции размера страницы базы данных 32k. Новый функциональный уровень сопоставляется со значением `DomainLevel 10` и `ForestLevel 10` для установок без

присмотра. Корпорация Майкрософт не планирует модернизировать функциональные уровни для Windows Server 2019 и Windows Server 2022. Чтобы выполнить неактивное повышение и понижение контроллера домена, см. синтаксис файла ответов DCPROMO для неактивного повышения и понижения уровня контроллеров домена.

API DsGetDcName также поддерживает новый флаг `DS_DIRECTORY_SERVICE_13_REQUIRED`, который позволяет находить контроллеры домена, работающие под управлением Windows Server 2025. Дополнительные сведения о функциональных уровнях см. в следующих статьях:

- уровни функциональности AD DS
- повышение уровня функциональности домена
- Повышение функционального уровня леса

Примечание.

Новые леса Active Directory и наборы конфигураций AD LDS должны иметь функциональный уровень Windows Server 2016 или выше. Для продвижения реплики Active Directory или AD LDS требуется, чтобы существующий домен или набор конфигурации уже работал с функциональным уровнем Windows Server 2016 или более поздней версии.

Корпорация Майкрософт рекомендует всем клиентам начать планирование обновления серверов Active Directory и AD LDS до Windows Server 2022 в рамках подготовки к следующему выпуску.

- **Улучшенные алгоритмы поиска имен/SID**: Переадресация поиска имен и SID с использованием локального органа безопасности (LSA) между учётными записями компьютеров больше не использует устаревший безопасный канал Netlogon. Вместо этого используются аутентификация Kerberos и алгоритм определения контроллера домена. Для обеспечения совместимости с устаревшими операционными системами можно использовать безопасный канал Netlogon в качестве резервного варианта.
- **Улучшенная безопасность конфиденциальных атрибутов**: Контроллеры домена и экземпляры AD LDS разрешают выполнение операций добавления, поиска и изменения с использованием LDAP, связанных с конфиденциальными атрибутами, только при зашифрованном соединении.
- **улучшенная безопасность паролей учетных записей компьютера по умолчанию**: Active Directory теперь использует пароли учетных записей компьютера по умолчанию, которые создаются случайным образом. Контроллеры домена Windows 2025 блокируют установку паролей учетных записей компьютеров на значение по умолчанию, равное имени учетной записи компьютера.

  Чтобы управлять этим поведением, включите параметр объекта групповой политики (GPO) **Контроллер домена: отказать в установке пароля учетной записи компьютера по умолчанию**, расположенный в *Конфигурация компьютера\Параметры Windows\Параметры безопасности\Локальные политики\Параметры безопасности*.

  Служебные программы, такие как Центр администрирования Active Directory (ADAC), пользователи и компьютеры Active Directory (ADUC), `net`

`computer`и `dsmod` также учитывают это новое поведение. AdAC и ADUC больше не позволяют создавать учетную запись до Windows 2000.

- **поддержка протокола Kerberos PKINIT для криптографической гибкости**: криптография открытого ключа Kerberos для начальной проверки подлинности в Kerberos (PKINIT) обновляется, чтобы обеспечить криптографическую гибкость, поддерживая дополнительные алгоритмы и удаляя жестко закодированные алгоритмы.
- **изменения в Kerberos для алгоритмов, используемых для предоставления билетов**: Центр распределения Kerberos больше не будет выдавать билеты на предоставление доступа с использованием шифрования RC4, такого как RC4-HMAC(NT).
- **Изменения в Kerberos для конфигурации поддерживаемого типа шифрования:** Kerberos больше не учитывает устаревший ключ реестра REG_DWORD, найденный в пути `SupportedEncryptionTypes`, Microsoft рекомендует использовать групповую политику. Дополнительные сведения о параметрах групповой политики см. в статье " Безопасность сети": настройка типов шифрования, разрешенных для Kerberos.
- **параметр групповой политики диспетчера локальной сети**: параметр групповой политики **сетевой безопасности. Не сохраняйте хэш-значение LAN Manager при следующем изменении пароля** больше не присутствует и не применяется к новым версиям Windows.
- **Шифрование LDAP по умолчанию**: для всех новых развертываний Active Directory требуется подпись LDAP (печать) по умолчанию для всех подключений клиента LDAP после привязки простой проверки подлинности и уровня безопасности (SASL). Дополнительные сведения о поведении при подписывании см. в разделе Подпись LDAP для доменных служб Active Directory.
- **поддержка LDAP для Transport Layer Security (TLS) 1.3**: LDAP использует последнюю реализацию SCHANNEL и поддерживает протокол TLS 1.3 для подключений LDAP по TLS. Использование TLS 1.3 устраняет устаревшие алгоритмы шифрования и повышает безопасность более ранних версий. TLS 1.3 стремится зашифровать как можно большую часть рукопожатия. Дополнительные сведения см. в статьях "Протоколы" в протоколах TLS/SSL (Schannel SSP) и наборах шифров TLS в Windows Server 2022.
- **Процедура изменения пароля в удалённом вызове (RPC) устаревшего Диспетчера учётных записей безопасности (SAM)**: безопасные протоколы, такие как Kerberos, являются предпочтительным способом для изменения паролей пользователей домена. По умолчанию на контроллерах домена (DC) новейший метод изменения пароля SAM RPC SamrUnicodeChangePasswordUser4 с использованием стандарта шифрования AES (Advanced Encryption Standard) принимается при удаленном вызове. Следующие устаревшие методы SAM RPC блокируются по умолчанию при удаленном вызове:
  - SamrChangePasswordUser
  - SamrOemChangePasswordUser2
  - SamrUnicodeChangePasswordUser2

  Для пользователей домена, являющихся членами группы защищенных пользователей и локальных учетных записей на компьютерах-членах домена, все изменения удаленного пароля через устаревший интерфейс SAM RPC блокируются по умолчанию, включая .

Чтобы управлять этим поведением, используйте следующий параметр групповой политики:

Конфигурация компьютера>Административные шаблоны>Система>Security Account Manager>Настройка политики методов RPC для изменения пароля SAM

- **поддержка**неоднородного доступа к памяти (NUMA): AD DS теперь использует аппаратное обеспечение с поддержкой NUMA с помощью ЦП во всех группах процессоров. Ранее Active Directory использовал только ЦП в группе 0. Active Directory может расшириться за пределами 64 ядер.
- **счетчики производительности**: теперь доступны мониторинг и устранение неполадок производительности следующих счетчиков:
  - Для указателя контроллера домена : доступны счетчики, относящиеся к клиентам и контроллерам домена.
  - **Поиски LSA**: поиск по именам и SID через `LsaLookupNames`, `LsaLookupSids`и эквивалентные API. Эти счетчики доступны как на клиентских, так и на серверных версиях.
  - клиент **LDAP**: доступен в Windows Server 2022 и более поздних версиях через обновление KB 5029250.
- **порядок приоритета репликации**: Теперь администраторы могут увеличить системно вычисляемый приоритет репликации с определенным партнером репликации для определенного контекста именования. Эта функция обеспечивает большую гибкость при настройке порядка репликации для решения конкретных сценариев.

Управляемая учетная запись делегированного обслуживания

Этот новый тип учетной записи позволяет перенести учетную запись службы на делегированную управляемую учетную запись службы (dMSA). Этот тип учетной записи поставляется с управляемыми и полностью случайными ключами, чтобы обеспечить минимальные изменения приложения при отключении паролей исходной учетной записи службы. Дополнительные сведения см. в разделе Обзор делегированных управляемых учетных записей служб.

Решение для паролей локальных администраторов Windows

Решение для локального администратора Windows (LAPS) помогает организациям управлять паролями локального администратора на компьютерах, присоединенных к домену. Он автоматически создает уникальные пароли для учетной записи локального администратора каждого компьютера. Затем он хранит их безопасно в Active Directory и регулярно обновляет их. Автоматически созданные пароли помогают повысить безопасность. Они снижают риск доступа злоумышленников к конфиденциальным системам с помощью скомпрометированных или легко угадываемых паролей.

Некоторые функции, новые для Microsoft LAPS, представляют следующие улучшения:

- **Новое автоматическое управление учетными записями**: IT-администраторы теперь могут с легкостью создавать локальную управляемую учетную запись. С помощью этой функции можно настроить имя учетной записи и включить или

отключить учетную запись. Вы даже можете случайно использовать имя учетной записи для повышения безопасности. Обновление также включает улучшенную интеграцию с существующими политиками управления локальными учетными записями от Корпорации Майкрософт. Дополнительные сведения об этой функции см. в режимах управления учетными записями Windows LAPS.

- **Обнаружение отката изображения**: Windows LAPS теперь определяет, когда происходит откат изображения. Если откат происходит, пароль, хранящийся в Active Directory, может больше не совпадать с паролем, хранящимся локально на устройстве. Откаты могут привести к *повреждённому состоянию*. В этом случае ИТ-администратор не может войти на устройство с помощью сохраненного пароля Windows LAPS.

  Для решения этой проблемы добавлена новая функция, которая включает атрибут Active Directory с именем `msLAPS-CurrentPasswordVersion`. Этот атрибут содержит случайный глобальный уникальный идентификатор (GUID), написанный Windows LAPS каждый раз, когда новый пароль сохраняется в Active Directory и сохраняется локально. Во время каждого цикла обработки идентификатор GUID, хранящийся в `msLAPS-CurrentPasswordVersion`, запрашивается и сравнивается с локально сохраняемой копией. Если они отличаются, пароль немедленно сменяется.

  Чтобы включить эту функцию, запустите последнюю версию командлета `Update-LapsADSchema`. Windows LAPS распознает новый атрибут и начинает использовать его. Если вы не запускаете обновленную версию командлета `Update-LapsADSchema`, Windows LAPS регистрирует событие предупреждения 10108 в журнале событий, но продолжает работать нормально во всех остальных отношениях.

  Параметры политики не используются для включения или настройки этой функции. Функция всегда включена после добавления нового атрибута схемы.

- **новые пароли**: ИТ-администраторы теперь могут использовать новую функцию в Windows LAPS, которая позволяет создавать менее сложные пароли. Примером является парольная фраза, например **EatYummyCaramelCandy**. Эта фраза проще читать, запоминать и вводить по сравнению с традиционным паролем, например **V3r_b4tim#963?**.

  С помощью этой новой функции можно настроить параметр политики `PasswordComplexity`, чтобы выбрать один из трех различных списков слов для парольной фразы. Все списки включены в Windows и не требуют отдельной загрузки. Новый параметр политики с именем `PassphraseLength` определяет количество слов, используемых в парольной фразе.

  При создании парольной фразы указанное число слов выбирается случайным образом из выбранного списка слов и объединяется. Первая буква каждого слова заглавная, чтобы повысить удобочитаемость. Эта функция также полностью поддерживает резервное копирование паролей в Active Directory или Идентификатор Microsoft Entra.

  Списки слов, используемые в трех новых настройках парольных фраз `PasswordComplexity`, взяты из статьи Electronic Frontier Foundation Глубокое погружение: Новые списки слов EFF для случайных парольных фраз. Списки слов Windows LAPS для паролей лицензированы в соответствии с лицензией CC-BY-3.0 и доступны для скачивания.

Примечание.

Windows LAPS не позволяет настраивать встроенные списки слов или использовать настроенные клиентом списки слов.

- **словарь паролей с улучшенной читаемостью**: Windows LAPS вводит новый параметр `PasswordComplexity`, который позволяет ИТ-администраторам создавать менее сложные пароли. Эту функцию можно использовать для настройки LAPS для использования всех четырех категорий символов (прописных букв, строчных букв, чисел и специальных символов), таких как существующий параметр сложности `4`. При новом параметре `5`более сложные символы исключаются для повышения удобочитаемости паролей и минимизации путаницы. Например, числовые **1** и буква **I** никогда не используются с новой настройкой.

  Если `PasswordComplexity` настроено на `5`, в набор символов словаря паролей по умолчанию вносятся следующие изменения:

  - **не используйте:** буквы **I**, **O**, **Q**, **l**, **o**
  - **не используйте:** числа **0**, **1**
  - **не используйте:** специальные символы **„**, **.**, **&**, **{**, **}**, **[**, **]**, **(**, **)**, **;**
  - **Использовать:** специальные символы **:**, **=**, **?**, *****

  Оснастка ADUC (через консоль управления Майкрософт) теперь включает улучшенную вкладку Windows LAPS. Пароль Windows LAPS теперь отображается в новом шрифте, который повышает его удобочитаемость при отображении в виде обычного текста.

- **Поддержка действий после аутентификации для завершения отдельных процессов**: новый параметр добавлен в параметр **действий после аутентификации** (PAA) в настройках групповой политики `Reset the password, sign out the managed account, and terminate any remaining processes`, который расположен в **Конфигурация компьютера**>**Административные шаблоны**>**Система**>**LAPS**>**Действия после аутентификации**.

  Этот новый параметр является расширением предыдущего параметра `Reset the password and log off the managed account`. После настройки PAA уведомляет, а затем завершает любые интерактивные сеансы входа. Он перечисляет и завершает все процессы, которые по-прежнему выполняются под локальной учетной записью, управляемой Windows LAPS. Завершение происходит без предварительного уведомления.

  Расширение логирования событий во время выполнения PAA предоставляет более глубокое понимание работы.

Дополнительные сведения о Windows LAPS см. в статье "Что такое Windows LAPS?".

OpenSSH

В более ранних версиях Windows Server средство подключения OpenSSH требовало ручной установки перед использованием. Компонент на стороне сервера OpenSSH устанавливается по умолчанию в Windows Server 2025. Пользовательский интерфейс

диспетчер сервера также включает одношаговый параметр в **разделе "Удаленный SSH-доступ"**, который включает или отключает `sshd.exe` службу. Кроме того, вы можете добавить пользователей в **группу пользователей OpenSSH** , чтобы разрешить или ограничить доступ к устройствам. Дополнительные сведения см. в обзоре OpenSSH для Windows.

Базовый уровень безопасности

Реализуя настраиваемую базовую линию безопасности, вы можете установить меры безопасности с самого начала для роли устройства или виртуальной машины на основе рекомендуемого уровня безопасности. Этот базовый план оснащен более чем 350 предварительно настроенными параметрами безопасности Windows. Параметры можно использовать для применения и обеспечения соблюдения определенных параметров безопасности, которые соответствуют рекомендациям, рекомендуемыми корпорацией Майкрософт и отраслевыми стандартами. Чтобы узнать больше, см. информацию в обзоре OSConfig.

Анклавы безопасности на основе виртуализации

Анклав безопасности на основе виртуализации (VBS) — это доверенная среда выполнения на основе программного обеспечения в адресном пространстве ведущего приложения. Анклавы VBS используют базовую технологию VBS для изоляции конфиденциальной части приложения в безопасной секции памяти. Анклава VBS обеспечивают изоляцию конфиденциальных рабочих нагрузок как от ведущего приложения, так и остальной части системы.

Анклавы VBS позволяют приложениям защищать свои секреты, устраняя необходимость доверия администраторам и усиливая защиту от вредоносных злоумышленников. Дополнительные сведения см. в справочнике по анклавам VBS Win32 .

Защита ключей безопасности на основе виртуализации

Защита ключей VBS позволяет разработчикам Windows защитить криптографические ключи с помощью VBS. VBS использует возможность расширения виртуализации ЦП для создания изолированной среды выполнения за пределами обычной ОС.

При использовании ключи VBS изолируются в рамках защищенного процесса. Операции с ключами могут выполняться без раскрытия данных закрытого ключа за пределами данного пространства. В неактивном состоянии ключ TPM шифрует данные закрытого ключа, что связывает ключи VBS с устройством. Ключи, защищенные таким образом, нельзя сбрасывать из памяти процесса или экспортировать в обычный текст с компьютера пользователя.

Защита ключей VBS помогает предотвратить эксфильтрационные атаки любого злоумышленника с правами администратора. Для использования защиты ключей необходимо включить VBS. Сведения о том, как включить VBS, см. в разделе Включение целостности памяти.

Защищенное подключение

В следующих разделах рассматривается безопасность подключений.

Безопасное управление сертификатами

Поиск или получение сертификатов в Windows теперь поддерживает хэши SHA-256, как описано в функциях CertFindCertificateInStore и CertGetCertificateContextProperty. Проверка подлинности сервера TLS более безопасна в Windows и теперь требует минимальной длины ключа RSA 2048 бит. Дополнительные сведения см. в статье аутентификация сервера TLS: отказ от использования сертификатов RSA с низкой степенью защиты.

SMB по QUIC

Функция SMB на сервере QUIC , которая доступна только в Windows Server Azure Edition, теперь доступна как в windows Server Standard, так и в версиях Центра обработки данных Windows Server. SMB через QUIC использует преимущества протокола QUIC, обеспечивая низкую задержку и зашифрованные подключения через Интернет.

Политика активации SMB через QUIC

Администраторы могут отключить клиент SMB по протоколу QUIC с помощью групповой политики и PowerShell. Чтобы отключить SMB через QUIC с помощью групповой политики, установите политику **Включить SMB через QUIC** в следующих путях в состояние **Отключено**:

- *конфигурация компьютера\Административные шаблоны\Network\Lanman Workstation*
- *конфигурация компьютера\Административные шаблоны\Network\Lanman Server*

Чтобы отключить SMB через QUIC с помощью PowerShell, выполните следующую команду в командной строке PowerShell с повышенными привилегиями:

```
PowerShell
Set-SmbClientConfiguration -EnableSMBQUIC $false
```

Аудит подписывания и шифрования SMB

Администраторы могут включить аудит сервера SMB и клиента для поддержки подписывания и шифрования SMB. Если клиент или сервер, отличный от Майкрософт, не поддерживает шифрование SMB или подпись, его можно обнаружить. Если устройство или программное обеспечение, отличное от Майкрософт, поддерживает SMB 3.1.1, но не поддерживает подписывание SMB, оно нарушает требование протокола целостности проверки подлинности SMB 3.1.1.

Параметры аудита подписи и шифрования SMB можно настроить с помощью групповой политики или PowerShell. Эти политики можно изменить в следующих путях групповой политики:

- *Конфигурация компьютера\Административные шаблоны\Network\Lanman Server\Audit client не поддерживает шифрование*
- *Конфигурация компьютера\Административные шаблоны\Network\Lanman Server\Audit client не поддерживает подпись*
- *Конфигурация компьютера\Административные шаблоны\Network\Lanman Workstation\Audit Server не поддерживает шифрование*
- *Конфигурация компьютера\Административные шаблоны\Network\Lanman Workstation\Audit Server не поддерживает подпись*

Чтобы выполнить эти изменения с помощью PowerShell, выполните следующие команды в командной строке с повышенными привилегиями, где `$true` включает и `$false` отключает следующие параметры:

PowerShell

```
Set-SmbServerConfiguration -AuditClientDoesNotSupportEncryption $true
Set-SmbServerConfiguration -AuditClientDoesNotSupportSigning $true

Set-SmbClientConfiguration -AuditServerDoesNotSupportEncryption $true
Set-SmbClientConfiguration -AuditServerDoesNotSupportSigning $true
```

Журналы событий для этих изменений хранятся в средствах просмотра событий по следующим путям с указанным идентификатором события.

Path	**Идентификатор событ**
Журналы приложений и служб\Microsoft\Windows\SMBClient\Audit	31998 31999
Журналы приложений и служб\Microsoft\Windows\SMBServer\Audit	3021 3022

Аудит SMB через QUIC

Аудит подключения клиента SMB через QUIC регистрирует события в журнале событий для включения транспорта QUIC в Просмотр событий. Эти журналы хранятся по следующим путям с их определённым идентификатором события (Event ID).

Path	**Идентификатор собы**
Журналы приложений и служб\Microsoft\Windows\SMBClient\Connectivity	30832
Журналы приложений и служб\Microsoft\Windows\SMBServer\Connectivity	1913

Управление доступом клиента SMB через QUIC

Windows Server 2025 включает управление доступом клиентов для SMB через QUIC. SMB через QUIC — это альтернатива TCP и RDMA, которая обеспечивает безопасное подключение к пограничным файловым серверам через ненадежные сети. Управление доступом к клиенту вводит дополнительные элементы управления, чтобы ограничить доступ к данным с помощью сертификатов. Дополнительные сведения см. в статье о работе управления доступом клиентов.

Альтернативные порты SMB

Клиент SMB можно использовать для подключения к альтернативным портам TCP, QUIC и RDMA вместо их значений по умолчанию IANA/IETF: 445 для TCP, 443 для QUIC и 5445 для RDMA. Можно настроить альтернативные порты с помощью групповой политики или PowerShell. Ранее сервер SMB в Windows назначил входящий трафик для использования зарегистрированного через IANA порта TCP/445, а tcp-клиент SMB допускает только исходящие подключения к тому же TCP-порту. Теперь SMB через QUIC позволяет использовать альтернативные порты SMB, если порты UDP/443, требуемые QUIC, доступны как для серверов, так и для клиентских устройств. Дополнительные сведения см. в разделе "Настройка альтернативных портов SMB".

Усиление защиты правил брандмауэра SMB

Ранее при создании общей папки правила брандмауэра SMB были автоматически настроены для включения группы **общего доступа к файлам и принтерам** для соответствующих профилей брандмауэра. Теперь создание общей папки SMB в Windows приводит к автоматической настройке новой группы **Ограниченного общего доступа к файлам и принтерам**, которая больше не разрешает входящие порты NetBIOS 137-139. Дополнительные сведения см. в разделе "Обновленные правила брандмауэра".

Шифрование SMB

Принудительное шифрование SMB включено для всех исходящих клиентских подключений SMB. С помощью этого обновления администраторы могут установить требование, чтобы все конечные серверы поддерживали SMB 3.x и шифрование. Если сервер не имеет этих возможностей, клиент не может установить подключение.

Ограничение скорости проверки подлинности SMB

Ограничение скорости проверки подлинности SMB ограничивает количество попыток проверки подлинности в течение определенного периода времени. Ограничитель скорости аутентификации SMB помогает бороться с атаками грубой силы. Служба для сервера SMB использует ограничитель скорости проверки для осуществления задержки между каждой неудачной попыткой проверки подлинности NTLM или PKU2U. Служба включена по умолчанию. Дополнительные сведения см. в статье о том, как работает ограничение скорости проверки подлинности SMB.

Отключите SMB NTLM

Начиная с Windows Server 2025 клиент SMB поддерживает блокировку NTLM для удаленных исходящих подключений. Ранее механизм ведения переговоров Windows Simple and Protected GSSAPI (SPNEGO) вел переговоры, используя Kerberos, NTLM и другие механизмы с целевым сервером для определения поддерживаемого пакета безопасности. Дополнительные сведения см. в разделе "Блокировать подключения NTLM" в SMB.

Управление диалектом SMB

Теперь вы можете управлять диалектами SMB в Windows. При конфигурировании сервер SMB определяет, какие диалекты SMB 2 и SMB 3 он согласовывает по сравнению с прежним поведением, и выбирает только самый высокий диалект.

Подписывание SMB

Подписывание SMB теперь требуется по умолчанию для всех исходящих подключений SMB. Ранее это было необходимо только при подключении к общим папкам с именем **SYSVOL** и **NETLOGON** на контроллерах домена Active Directory. Дополнительные сведения см. в статье Как работает подпись.

Удалённый мейлслот

Протокол Remote Mailslot отключен по умолчанию для SMB и для использования протокола DC Locator в сочетании с Active Directory. Remote Mailslot может быть удален в более позднем выпуске. Дополнительные сведения см. в статье Функции, удаленные или не разработанные в Windows Server.

Усиление защиты служб маршрутизации и удаленного доступа

По умолчанию новые установки служб маршрутизации и удаленного доступа (RRAS) не принимают VPN-подключения на основе PPTP и L2TP. При необходимости эти протоколы можно включить. VPN-подключения на основе SSTP и IKEv2 по-прежнему принимаются без каких-либо изменений.

Существующие конфигурации сохраняют их поведение. Например, если вы запускаете Windows Server 2019 и принимаете подключения PPTP и L2TP, а также выполняете обновление до Windows Server 2025 с помощью обновления на месте, подключения на основе L2TP и PPTP по-прежнему принимаются. Это изменение не влияет на клиентские операционные системы Windows. Дополнительные сведения о повторной активации PPTP и L2TP см. в статье Настройка протоколов VPN.

Изменение протокола ключей по умолчанию IPsec

Модули ключей по умолчанию были изменены на IKEv1 и IKEv2 для подключений IPsec, прошедших проверку подлинности с помощью сертификатов компьютера. Для других методов проверки подлинности по умолчанию остается authIP и IKEv1. Это относится к клиентам Windows Server 2025 и Windows 11 24H2. На пути реестра `HKLM:\SYSTEM\CurrentControlSet\Services\MpsSvc\Parameters`, запись `IpsecRestoreLegacyKeyMod` со значением **0** использует новую последовательность: IKEv2 и IKEv1. Значение **1** использует предыдущую последовательность, AuthIP и IKEv1. Чтобы вернуться к предыдущему поведению, добавьте следующий раздел реестра в системы, использующие новую последовательность ключевого протокола по умолчанию. Чтобы изменения вступили в силу, требуется перезагрузка.

PowerShell

```
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\MpsSvc\Parameters" -
Name "IpsecRestoreLegacyKeyMod" -PropertyType "DWORD" -Value 1
```

Hyper-V, AI и производительность

В следующих разделах рассматриваются Hyper-V, ИИ и производительность.

Ускорение сети (предварительная версия)

Ускоренная сеть (AccelNet) упрощает управление одно корневой виртуализацией ввода-вывода (SR-IOV) для виртуальных машин, размещенных на кластерах Windows Server 2025. Эта функция использует высокопроизводительный канал передачи данных SR-IOV для уменьшения задержки, дрожания и использования центрального процессора. AccelNet также включает уровень управления, который обрабатывает проверку готовности, конфигурацию узла и параметры производительности виртуальной машины. Дополнительные сведения см. в Ускоренная сетевая функция (предварительная версия).

Совместимость динамического процессора

Режим совместимости динамического процессора обновляется, чтобы воспользоваться преимуществами новых возможностей процессора в кластеризованной среде. Совместимость динамического процессора использует максимальное количество функций процессора, доступных на всех серверах в кластере. Режим повышает производительность по сравнению с предыдущей версией совместимости процессора.

Вы также можете использовать динамическую совместимость процессора для сохранения состояния между узлами виртуализации, использующих разные поколения процессоров. Теперь режим совместимости процессора предоставляет расширенные динамические возможности на процессорах, способных переводить адреса второго уровня. Дополнительные сведения об обновленном режиме совместимости см. в разделе "Совместимость процессора" для Hyper-V виртуальных машин.

Диспетчер Hyper-V

При создании новой виртуальной машины с помощью диспетчера Hyper-V, поколение 2 теперь устанавливается в качестве параметра по умолчанию в мастере создания виртуальных машин.

Управляемое гипервизором постраничное преобразование

Принудительная трансляция страниц с гипервизором (HVPT) — это улучшение безопасности для гарантии целостности линейных трансляций адресов. HVPT защищает критически важные системные данные от атак write-what-where, где злоумышленник записывает произвольное значение в произвольное расположение, часто в результате переполнения буфера. HVPT защищает таблицы страниц, которые управляют критически важными системными данными. HVPT включает всё, что уже находится под защитой целостности кода с использованием гипервизора (HVCI). HVPT включен по умолчанию, где доступна поддержка оборудования. HVPT не включен, если Windows Server работает в качестве гостя на виртуальной машине.

Секционирование GPU

Физическое устройство GPU можно совместно использовать с несколькими виртуальными машинами с помощью секционирования GPU. Вместо выделения всего GPU на одну виртуальную машину секционирование GPU (GPU-P) назначает выделенные доли GPU каждой виртуальной машине. При Hyper-V GPU-P высокой доступности виртуальная машина GPU-P автоматически включается на другом узле кластера при незапланированном простое.

Динамическая миграция GPU-P предоставляет решение для перемещения виртуальной машины (для запланированного простоя или балансировки нагрузки) с GPU-P на другой узел независимо от того, является ли он автономным или кластеризованным. Дополнительные сведения о секционирования GPU см. в разделе "Секционирование GPU".

Сетевая ATC

Сетевой ATC упрощает развертывание и управление сетевыми конфигурациями для кластеров Windows Server 2025. Сетевой ATC использует подход, основанный на намерениях, где пользователи указывают свои намерения, например, управление, вычисления или хранилище для сетевого адаптера. Развертывание автоматизировано на основе предполагаемой конфигурации.

Этот подход сокращает время, сложность и ошибки, связанные с развертыванием сетей узлов. Это обеспечивает согласованность конфигурации в кластере, а также устраняет смещение конфигурации. Дополнительные сведения см. в разделе "Развертывание сетевых ресурсов с использованием Network ATC".

Scalability

В Windows Server 2025 Hyper-V теперь поддерживает до 4 петабайт памяти и 2048 логических процессоров на узел. Это увеличение позволяет повысить масштабируемость и производительность виртуализированных рабочих нагрузок.

Windows Server 2025 также поддерживает до 240 ТБ памяти и 2048 виртуальных процессоров для виртуальных машин поколения 2, обеспечивая повышенную гибкость для выполнения больших рабочих нагрузок. Дополнительные сведения см. в разделе "Планирование масштабируемости Hyper-V" в Windows Server.

Кластеры рабочей группы

Hyper-V кластеры рабочей группы — это особый тип отказоустойчивого кластера Windows Server, где узлы кластера Hyper-V не являются членами домена Active Directory с возможностью динамической миграции виртуальных машин в кластере рабочей группы.

Storage

В следующих разделах описываются обновления хранилища.

Поддержка клонирования блоков

Теперь Dev Drive поддерживает клонирование блоков, начиная с Windows 11 24H2 и Windows Server 2025. Поскольку Dev Drive использует формат устойчивой файловой системы (ReFS), поддержка клонирования блоков обеспечивает значительные преимущества в производительности при копировании файлов. С помощью клонирования блоков файловая система может скопировать диапазон байтов файлов для приложения как операцию с метаданными с низкой стоимостью, вместо выполнения дорогостоящих операций чтения и записи в базовые физические данные.

Результатом является быстрое завершение копирования файлов, сокращение операций ввода-вывода в базовое хранилище и повышение емкости хранилища, позволяя нескольким файлам совместно использовать одни и те же логические кластеры. Дополнительные сведения см. в разделе "Блокировка клонирования" в ReFS.

Диск разработки

Dev Drive — это том хранилища, предназначенный для повышения производительности ключевых рабочих нагрузок разработчика. Dev Drive использует технологию ReFS и включает определенные оптимизации файловой системы, чтобы обеспечить более широкий контроль над параметрами тома хранилища и безопасностью. Теперь администраторы могут назначать доверие, настраивать параметры антивирусной программы и осуществлять административный контроль над подключенными фильтрами. Дополнительные сведения см. в статье "Настройка диска разработки" в Windows 11.

NVMe

NVMe — это новый стандарт для быстрых твердотельных дисков. Производительность хранилища NVMe оптимизирована в Windows Server 2025. Результатом является повышение производительности с увеличением операций ввода-вывода в секунду и снижением использования ЦП.

Сжатие реплики хранилища

Сжатие реплики хранилища уменьшает объем данных, передаваемых по сети во время репликации. Дополнительные сведения о сжатии в Storage Replica см. в разделе ОбзорStorage Replica.

Расширенный журнал репликации хранилища

Улучшенный журнал реплики хранилища помогает в реализации журнала для устранения затрат на производительность, связанных с абстракциями файловой системы. Улучшена производительность блочной репликации. Чтобы узнать больше, см. Расширенный журнал реплики хранилища.

Дедупликация и сжатие в собственном хранилище ReFS

Дедупликация и сжатие в собственном хранилище ReFS — это методы оптимизации эффективности хранения для статических и активных рабочих нагрузок, таких как файловые серверы или виртуальные рабочие столы. Дополнительные сведения о

дедупликации и сжатии ReFS см. в статье Оптимизация хранилища с помощью дедупликации и сжатия ReFS в локальной Azure.

Тонко выделенные тома

Тома с тонким выделением ресурсов с использованием Storage Spaces Direct — это способ эффективного распределения ресурсов хранилища и предотвращения дорогостоящего перераспределения путем выделения из пула только когда это необходимо в кластере. Вы также можете преобразовать тома с фиксированным распределением в тома с тонким распределением. Преобразование из фиксированных в тонкие подготовленные тома возвращает любое неиспользуемое хранилище обратно в пул для использования других томов. Чтобы узнать больше о тонких томах с динамическим выделением, см. Тонкое выделение памяти.

Блок сообщений сервера

Блок сообщений сервера (SMB) является одним из наиболее широко используемых протоколов в сети. SMB предоставляет надежный способ совместного использования файлов и других ресурсов между устройствами в сети. Windows Server 2025 включает поддержку сжатия SMB для стандартного алгоритма сжатия LZ4 в отрасли. LZ4 в дополнение к уже существующей поддержки SMB для XPRESS (LZ77), XPRESS Huffman (LZ77+Huffman), LZNT1 и PATTERN_V1.

Azure Arc и гибридная среда

В следующих разделах рассматриваются конфигурации Azure Arc и гибридные конфигурации.

Упрощенная настройка Azure Arc

Настройка Azure Arc — это функция по запросу, поэтому она устанавливается по умолчанию. Удобный интерфейс мастера и значок области задач помогают упростить процесс добавления серверов в Azure Arc. Azure Arc расширяет возможности платформы Azure, чтобы создавать приложения и службы, которые могут работать в различных средах. Эти среды включают центры обработки данных, пограничные и многооблачные среды и обеспечивают повышенную гибкость. Дополнительные сведения см. в статье "Подключение компьютеров Windows Server к Azure с помощью программы установки Azure Arc".

Лицензирование с оплатой по факту использования

Вариант лицензирования подписки с оплатой по мере использования Azure Arc является альтернативой обычному постоянному лицензированию для Windows Server 2025. С помощью варианта оплаты по мере использования можно развернуть устройство Windows Server, лицензировать его и оплатить только столько, сколько вы используете. Эта функция упрощается с помощью Azure Arc и оплачивается через подписку Azure. Дополнительные сведения см. в статье лицензирование Azure Arc по мере использования.

Управление Windows Server, поддерживаемое Azure Arc

Управление Windows Server, осуществляемое с помощью Azure Arc, предоставляет новые преимущества клиентам, имеющим лицензии Windows Server с активной подпиской Software Assurance или действующие подписочные лицензии на Windows Server. Windows Server 2025 имеет следующие ключевые преимущества:

- **Windows Admin Center в Azure Arc**: интегрирует Azure Arc с Windows Admin Center, что позволяет управлять экземплярами Windows Server через портал Azure Arc. Эта интеграция обеспечивает единый интерфейс управления для экземпляров Windows Server, работающих локально, в облаке или на периферии.
- **Удаленная техническая поддержка**: предоставление клиентам профессиональной поддержки, возможности предоставления доступа по принципу "точно в срок" (JIT-доступ) с подробными расшифровками выполнения и правами на отзыв.
- **Оценка лучших практик**: Сбор и анализ данных сервера выявляют проблемы и предоставляют рекомендации по их устранению, а также способствуют улучшению производительности.
- **конфигурации Azure Site Recovery**. Конфигурация Azure Site Recovery обеспечивает бесперебойность бизнес-процессов и обеспечивает репликацию и устойчивость данных для критически важных рабочих нагрузок.

Дополнительные сведения об управлении Windows Server, включенном Azure Arc и доступных преимуществах, см. в статье "Управление Windows Server" с поддержкой Azure Arc.

Программно-определяемая сеть

Программно-определяемые сети (SDN) — это подход к сетям, который сетевые администраторы могут использовать для управления сетевыми службами через абстрагирование низкоуровневых функций. SDN позволяет разделить плоскость управления сетью, которая управляет сетью с плоскости данных, которая обрабатывает трафик. Это разделение позволяет повысить гибкость и программируемость в управлении сетями. SDN предоставляет следующие преимущества в Windows Server 2025:

- **Сетевой контроллер**: Эта контрольная плоскость для SDN теперь размещается непосредственно в виде служб отказоустойчивого кластера на физических узловых компьютерах. Использование роли кластера устраняет необходимость развертывания виртуальных машин, что упрощает развертывание и управление и экономит ресурсы.
- **Сегментация на основе тегов**. Администраторы могут использовать пользовательские теги служб для ассоциации групп безопасности сети и виртуальных машин для управления доступом. Вместо указания диапазонов IP-адресов администраторы теперь могут использовать простые самообъясняющиеся метки, чтобы обозначать виртуальные машины рабочей нагрузки и применять политики безопасности на основе этих меток. Теги упрощают процесс управления безопасностью сети и устраняют необходимость запоминать и перетипировать диапазоны IP-адресов. Дополнительные сведения см. в статье "Настройка групп безопасности сети с тегами в Windows Admin Center".
- **Политики сети по умолчанию в Windows Server 2025**: эти политики предлагают варианты защиты, похожие на Azure, для сетевых групп безопасности (НСБ) при развертывании рабочих процессов через Центр администрирования Windows.

Политика по умолчанию запрещает весь входящий доступ, позволяя выборочно открывать известные входящие порты, разрешая полный исходящий доступ с виртуальных машин рабочей нагрузки. Политики сети по умолчанию гарантируют, что виртуальные машины рабочей нагрузки защищены с точки создания. Дополнительные сведения см. в статье "Использование политик доступа к сети по умолчанию" на виртуальных машинах в локальной среде Azure.

- **SDN Multisite**: эта функция обеспечивает естественное соединение уровня 2 и уровня 3 между приложениями в двух локациях без дополнительных компонентов. С помощью multisite SDN приложения могут легко перемещаться без необходимости перенастройки приложения или сетей. Она также предлагает унифицированное управление политиками сети для рабочих нагрузок, чтобы не нужно обновлять политики при переходе виртуальной машины рабочей нагрузки из одного расположения в другое. Дополнительные сведения см. в статье "Что такое SDN Multisite?".
- **улучшенная производительность шлюзов уровня 3 SDN**: шлюзы уровня 3 обеспечивают более высокую пропускную способность и сокращают циклы ЦП. Эти улучшения включены по умолчанию. Пользователи автоматически испытывают более высокую производительность при настройке подключения уровня 3 шлюза SDN с помощью PowerShell или Windows Admin Center.

Переносимость контейнеров Windows

Переносимость является важным аспектом управления контейнерами и имеет возможность упростить обновления, применяя повышенную гибкость и совместимость контейнеров в Windows.

Переносимость — это функция Windows Server, которую пользователи могут использовать для перемещения образов контейнеров и связанных с ними данных между разными узлами или средами без каких-либо изменений. Пользователи могут создать образ контейнера на одном узле, а затем развернуть его на другом узле, не беспокоясь о проблемах совместимости. Чтобы узнать больше, см. Переносимость для контейнеров.

Программа предварительной оценки Windows Server

Программа предварительной оценки Windows Server предоставляет ранний доступ к последним выпускам ОС Windows для сообщества энтузиастов. В качестве члена вы являетесь одним из первых, чтобы попробовать новые идеи и концепции, которые корпорация Майкрософт разрабатывает. После регистрации в качестве участника вы можете участвовать в различных каналах выпуска. Перейдите к разделу **Пуск**>**Параметры**>**Центр обновления Windows**>**Программа Windows Insider**.

Связанный контент

обсуждения Инсайдерского сообщества Windows Server

Дополнительные ресурсы

Документация

- **Требования к оборудованию для Windows Server**
  Проверьте минимальные требования к оборудованию ЦП, памяти (ОЗУ), хранилища и сети, необходимые для установки и запуска Windows Server.
- **Сравнение выпусков Windows Server**
  Узнайте о различиях между выпусками Windows Server Standard, Datacenter, Datacenter: Azure Edition и Annual Channel для контейнеров.
- **Новые возможности Windows Server 2019**
  В этой статье описаны некоторые новые функции Windows Server 2019.