## История развития семейства Windows Server, развитие семейства. Область применения ОС.

Полное развитие:

Windows 1.0 -> Windows 2.0 -> Windows 3.0 -> Windows 3.1 -> Windows 3.11 for Workgroups (первая сетевая ОС) -> Разработка с IBM (разругались) -> Windows NT 3.1 -> Windows 95 -> Windows 4.0 (Workstation и Server) -> Windows 98 -> Windows Millenium Edition -> Windows 2000 (AD, NTFS 3 и др) -> Windows Server 2003 (.Net Framework, сертификат С2) -> Windows XP -> Windows Server 2003 -> Windows Vista (Ready Boost, UAC, EFS, Bitlocker) -> Windows Server 2008 (NTFS3, Hyper-V2) -> Windows 7 -> Windows 8 -> Windows 8.1 -> Windows Server 2012 (Hyper-V, Storage Spaces, NTFS4) -> Windows 10 -> Windows Server 2016 (переработано хранение, синхронизация, виртуализация, кластеризация) -> Windows Server 2019 (подсистема Linux, гибридное облако) -> Windows 11 -> Windows Server 2022 (Windows Containers, AzureArc, 48 Тб ОЗУ)

Развитие Windows Server:

Windows 4.0 Server -> Windows Server 2003 -> Windows Server 2008 (NTFS3, Hyper-V2) -> Windows Server 2012 (Hyper-V, Storage Spaces, NTFS4) -> Windows Server 2016 (переработано хранение, синхронизация, виртуализация, кластеризация) -> Windows Server 2019 (подсистема Linux, гибридное облако) -> Windows Server 2022 (Windows Containers, AzureArc, 48 Тб ОЗУ)

Область применения:

* Enterprise (AD)
* Работа сервисов от MS (MS SQL, SharePooint, Exchange)
* Виртуализация (Hyper-V3)
* Организация сетей хранения данных
* Построение гибридных облаков
* Интеграции в Azure

## Архитектура ОС, новшества в архитектуре ОС на примере Windows Server 2012-2016

Всё семейство Windows, начиная с Windows NT 3.1, идет от ядра Windows NT.

Архитектура: является гибридной архитектурой, пользовательский интерфейс вшит в ядро, ACL, искусственная регуляризация кол-ва подключений, хранения конфигов в реестре, имеет различные механизмы для взаимодействия с различными устройствами.

Также ядро Windows NT имеет только 2 уровня – компоненты режима ядра, на котором программы и компоненты имеет неограниченный доступ к системной памяти и внешним устройствам, и компоненты режима пользователя, где есть ограничения на доступ к системным ресурсам.

Режим пользователя

Режим пользователя состоит из подсистем, которые передают запросы ввода\вывода соответствующему драйверу режима ядра посредством менеджера ввода-вывода. Уровень пользователя состоит из двух подсистем — подсистема окружения (Environment) и интегральная подсистема (Integral).

Подсистема окружения разработана для запуска приложений, написанных для разных типов операционных систем. Ни одна из подсистем окружения не имеет прямого доступа к аппаратной части компьютера. Доступ к ресурсам памяти происходит посредством Менеджера виртуальной памяти, который работает в режиме ядра. Также приложения запускаются с меньшим приоритетом, чем процессы режима ядра.

Подсистема окружения состоит из следующих подсистем — подсистема Win32, подсистема OS/2 и подсистема POSIX. Подсистема окружения Win32 запускает 32-разрядные Windows-приложения. Она содержит консоль и поддержку текстового окна, обработку ошибок для всех других подсистем окружения. Поддерживает VDM (Virtual DOS Machine), которая позволяет запускать 16-разрядные DOS и Windows- (Win16) приложения. VDM запускается в своем собственном адресном пространстве и эмулирует систему MS-DOS, запущенную на компьютере с процессором Intel 80486. Программы Win16 запускаются в режиме Win16 VDM. Каждая программа запускается в одном процессе с использованием одного адресного пространства, но для каждой программы используется свой отдельный поток. Однако Windows NT позволяет запускать Win16-программы в отдельных Win16 VDM-процессах, реализуя вытесняющую многозадачность. Процесс подсистемы окружения Win32 — csrss.exe также включает в себя функциональность менеджера окон, то есть обрабатывает входящие события, такие, как нажатие клавиш клавиатуры и мыши, и передает их на обработку соответствующим приложениям. Каждое приложение само производит перерисовку окон в ответ на эти сообщения.

Подсистема окружения OS/2 поддерживает неграфические 16-разрядные приложения операционной системы OS/2 и эмулирует систему OS/2 2.1.x.

Подсистема окружения POSIX поддерживает приложения, написанные в соответствии со стандартом POSIX.1.

Интегрированная подсистема (Integral subsystem) следит за некоторыми функциями операционной системы от имени подсистемы окружения. Состоит из подсистемы безопасности, службы рабочей станции и службы сервера. Служба безопасности обращается с маркерами доступа, разрешает или запрещает доступ к учётной записи пользователя, обрабатывает запросы авторизации и инициирует процесс входа пользователя в систему. Служба Рабочая станция обеспечивает доступ компьютера к сети — является API для сетевого редиректора (ПО, эмулирующее доступ к удаленной файловой системе как к локальной). Служба Сервер позволяет компьютеру предоставлять сетевые сервисы.

Режим ядра

Режим ядра Windows NT имеет полный доступ к аппаратной части компьютера и системным ресурсам. Работает в защищенной области памяти. Управляет памятью и взаимодействием с аппаратной частью. Предотвращает доступ к критическим областям памяти со стороны приложений и служб пользовательского режима. Для выполнения подобных операций процесс пользовательского режима должен попросить режим ядра выполнить её от своего имени.

Архитектура x86 поддерживает 4 уровня привилегий — от 0 до 3, но используются только 0-й и 3-й уровень. Режим пользователя использует уровень 3, а режим ядра — 0. Это было сделано для возможности переноса на платформу RISC, которая использует только два уровня привилегий. Режим ядра состоит из исполнительных служб, которые представляют собой различные модули, выполняющие определённые задачи, драйвера ядра, само ядро и уровень аппаратных абстракций HAL.

Исполнительная подсистема

Работает с вводом/выводом, менеджером объектов, управлением над процессами и безопасностью. Неофициально делится на несколько подсистем — менеджер кэша, менеджер конфигурации, менеджер ввода/вывода, вызов локальных процедур, менеджер памяти, монитор безопасности. Системные службы, то есть системные вызовы, реализованы на этом уровне, за исключением нескольких вызовов, которые вызывают непосредственно ядро для большей производительности. В данном контексте термин «служба» относится к вызываемым подпрограммам, или набору вызываемых подпрограмм. Они отличаются от служб, выполняемых в режиме пользователя, которые в какой-то мере являются аналогом демонов в UNIX-подобных системах.

Менеджер объектов

Это исполнительная подсистема, к которой обращаются все остальные модули исполнительной подсистемы, в частности, системные вызовы, когда им необходимо получить доступ к ресурсам Windows NT. Менеджер объектов служит для уменьшения дублирования объектов, что может привести к ошибкам в работе системы. Для менеджера объектов каждый ресурс системы является объектом — будь то физический ресурс типа периферийного устройства, файловой системы, или логический ресурс — файл и др. Каждый объект имеет свою структуру, или тип объекта.

Создание объекта делится на две стадии — создание и вставка. Создание — создается пустой объект и резервируются необходимые ресурсы, например, имя в пространстве имен. Если создание пустого объекта произошло успешно, то подсистема, ответственная за создание объекта, заполняет его. Если инициализация успешна, то подсистема заставляет менеджер объектов произвести вставку объекта — то есть сделать его доступным по своему имени или дескриптору.

Windows Server 2012

Основные усовершенствования:

* Новый пользовательский интерфейс Modern UI.
* 2300 новых командлетов Windows PowerShell.
* Усовершенствованный Диспетчер задач.
* Теперь Server Core стал рекомендуемым вариантом установки, а переключение между режимами с классическим рабочим столом и режимом Server Core может быть выполнено без переустановки сервера.
* Новая роль IPAM (IP Address Management) для управления и аудита адресным пространством IP4 и IP6.
* Усовершенствования в службе Active Directory.
* Новая версия Hyper-V 3.0. Новая файловая система ReFS (Resilient File System).
* Новая версия IIS 8.0 (Internet Information Services).

Storage Spaces

Одним из нововведений новой Windows Server 2012 является новая разработка корпорации — Storage Spaces, которая предлагает возможность системным администраторам, работающим с этой ОС, управлять большим числом систем хранения данных, подключенными через интерфейс SAS. Интересно, что благодаря Storage Spaces нет необходимости использовать дополнительное программное обеспечение.

На конференции Microsoft Build было показано объединение 16 жёстких дисков в единый пул. Интересная особенность такого объединения дисков как возможность разделения содержимого этого пула дисков на многочисленные виртуальные диски. Схожая возможность демонстрировалась несколькими годами ранее на презентации новой версии файловой системы ReFS (Resilient File System).

Безопасность

В новой серверной ОС будет добавлена служба Dynamic Access Control. Работа данной службы направлена на улучшение централизованной защиты на уровне доменов файлов, а также на обеспечение безопасности папок поверх всех имеющихся разрешений файлов.

Windows Server 2016

* Механизм обновления ОС хостов кластера без его остановки (Cluster Operating System Rolling Upgrade) — это происходит через создание смешанного кластера Windows Server 2012 R2 и Windows Server vNext.
* Синхронная репликация хранилищ на уровне блоков с поддержкой географически распределенных кластеров.
* Виртуальный сетевой контроллер (software-defined networking stack) для одновременного управления физическими и виртуальными сетями.
* Новый формат файлов конфигурации виртуальных машин (.VMCX и .VMRS), с более высокой степенью защиты от сбоев на уровне хранилища. Также можно будет обновлять версии конфигурационных файлов.
* Можно создавать снэпшоты прямо из гостевой ОС.
* Полноценный Storage Quality of Service (QoS) — возможность динамического отслеживания производительности хранилищ и горячая миграция виртуальных машин при превышении этими хранилищами пороговых значений (IOPS).
* Изменения в самом Hyper-V: использование альтернативных аккаунтов (хранение нескольких учётных данных одного человека, возможность использования по времени), возможность управления предыдущими версиями Hyper-V в корпоративной инфраструктуре, обновление и улучшение протокола удалённого управления, возможность безопасной загрузки гостевых операционных систем Linux
* Возможность обновления Integration Services через Windows Update.
* «Горячее» добавление сетевых карт и оперативной памяти.
* Поддержка OpenGL и OpenCL для Remote Desktop.
* Возможности публикации приложений.
* Совместимость с режимом Connected Standby.
* Windows Defender: Windows Server Antimalware теперь установлена и включена по умолчанию без графического интерфейса
* IIS 10: Добавлена поддержка протокола HTTP/2
* Windows PowerShell 5.0
* Убран Telnet сервер.

## Основные компоненты и службы Windows Server

## Файловые системы NTFS

NTFS поддерживает хранение метаданных. С целью улучшения производительности, надёжности и эффективности использования дискового пространства для хранения информации о файлах в NTFS используются специализированные структуры данных. Информация о файлах хранится в главной файловой таблице — Master File Table (MFT). NTFS поддерживает разграничение доступа к данным для различных пользователей и групп пользователей (списки контроля доступа — англ. access control lists, ACL), а также позволяет назначать дисковые квоты (ограничения на максимальный объём дискового пространства, занимаемый файлами тех или иных пользователей). Для NTFS размер кластера по умолчанию составляет от 512 байт до 2 МБ в зависимости от размера тома и версии ОС.

Диск NTFS условно делится на две части. Первые 12% диска отводятся под MFT-зону - пространство, в которое растет метафайл MFT. Запись каких-либо данных в эту область невозможна. MFT-зона всегда держится пустой – это делается для того, чтобы самый главный, служебный файл (MFT) не фрагментировался при своем росте. Остальные 88% диска представляют собой обычное пространство для хранения файлов.

Безопасность на основе списка управления доступом (ACL) для файлов и папок. NTFS позволяет устанавливать разрешения для файла или папки, указывать группы и пользователей, чей доступ требуется ограничить или разрешить, и выбрать тип доступа.

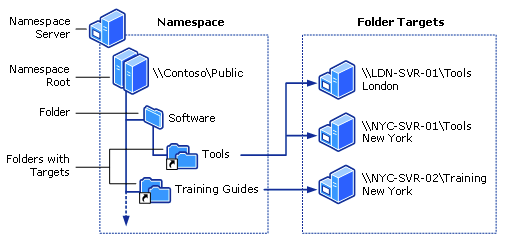
Поддержка шифрования диска BitLocker. Шифрование диска BitLocker обеспечивает дополнительную безопасность важных системных сведений и других данных, хранящихся на томах NTFS. Начиная с Windows Server 2012 R2 и Windows 8.1, BitLocker поддерживает шифрование устройств на компьютерах с архитектурой x86 и x64 с доверенным платформенным модулем, который поддерживает режим ожидания с подключением (ранее доступный только на устройствах Windows RT). Шифрование устройств помогает защитить данные на компьютерах под управлением Windows и помогает предотвратить доступ пользователей-злоумышленников к системным файлам, которые они используют для обнаружения пароля, или к диску путем физического удаления его с компьютера и установки в другой компьютер.

NTFS использует файл журнала и сведения о контрольных точках для восстановления согласованности файловой системы при перезагрузке компьютера после сбоя системы. После ошибки поврежденного сектора NTFS динамически изменяет конфигурацию кластера, содержащего поврежденный сектор, выделяет новый кластер для данных, отмечает исходный кластер как поврежденный и больше не использует старый кластер. Например, после сбоя сервера NTFS может восстановить данные путем воспроизведения файлов журнала.

NTFS непрерывно отслеживает и исправляет временные проблемы повреждения в фоновом режиме, не переводя том в автономный режим (эта функция, введенная в Windows Server 2008, известна как NTFS с самовосстановлением). При значительных проблемах с повреждением программа Chkdsk в Windows Server 2012 и более поздних версиях сканирует и анализирует диск, пока том подключен, ограничивая время автономной работы временем, необходимым для восстановления целостности данных в томе. Когда NTFS используется с CSV, простои не требуются.

## Файловые службы DFS

Пространства имен DFS (распределенная файловая система) — это служба ролей в Windows Server, которая позволяет группировать общие папки, расположенные на разных серверах, в одно или несколько логически структурированных пространств имен. Это делает возможным предоставлять пользователям виртуальное представление общих папок, где один путь ведет к файлам, расположенным на нескольких серверах.



Далее приведено описание элементов, из которых состоит пространство имен DFS:

* Сервер пространства имен. Сервер пространства имен, содержащий пространство имен. Сервер пространства имен может быть рядовым сервером или контроллером домена.
* Корень пространства имен. Корень пространства имен является отправной точкой пространства имен. На предыдущем рисунке имя корневого каталога — Public, а путь к пространству имен — \\Contoso\Public. Этот тип пространства имен является доменным пространством имен, потому что оно начинается с имени домена (например, Contoso) и его метаданные хранятся в доменных службах Active Directory (AD DS). Несмотря на то, что на предыдущем рисунке показан один сервер пространства имен, доменное пространство имен можно размещать на нескольких серверах пространства имен, чтобы повысить доступность пространства имен.
* Папка. Папки без конечных объектов-папок образуют структуру и иерархию в пространстве имен, а папки с целевыми объектами-папками предоставляют пользователям фактическое содержимое. Когда пользователи просматривают папку, содержащую конечные объекты-папки в пространстве имен, клиентский компьютер получает направление, которое прозрачно перенаправляет клиентский компьютер к одному из конечных объектов папки.
* Конечные объекты-папки. Конечный объект-папка — это путь UNC к общей папке или к другому пространству имен, которое связано с папкой в пространстве имен. Конечный объект-папка — это место, в котором хранятся данные и содержимое. На предыдущем рисунке у папки с именем Tools есть два конечных объекта-папки — в Лондоне и в Нью-Йорке — а папка с именем Training Guides имеет один конечный объект-папку в Нью-Йорке. Пользователь, который переходит в папку \\Contoso\Public\Software\Tools, прозрачно перенаправляется в общую папку \\LDN-SVR-01\Tools или \\NYC-SVR-01\Tools в зависимости от того, на каком сайте находится пользователь в данный момент.

## Сетевая служба SMB

SMB (сокр. от англ. Server Message Block) — сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия. В настоящее время SMB связан главным образом с операционными системами Microsoft Windows, где используется для реализации «Сети Microsoft Windows» и «Совместного использования файлов и принтеров».

Принцип работы

SMB — это протокол, основанный на технологии клиент-сервер, который предоставляет клиентским приложениям простой способ для чтения и записи файлов, а также запроса служб у серверных программ в различных типах сетевого окружения. Серверы предоставляют файловые системы и другие ресурсы (принтеры, почтовые сегменты, именованные каналы и т. д.) для общего доступа в сети. Клиентские компьютеры могут иметь у себя свои носители информации, но также имеют доступ к ресурсам, предоставленным сервером для общего пользования.

Клиенты соединяются с сервером, используя протоколы TCP/IP (а, точнее, NetBIOS через TCP/IP), NetBEUI или IPX/SPX. После того, как соединение установлено, клиенты могут посылать команды серверу (эти команды называются SMB-команды или SMBs), который даёт им доступ к ресурсам, позволяет открывать, читать файлы, писать в файлы и вообще выполнять весь перечень действий, которые можно выполнять с файловой системой. Однако в случае использования SMB эти действия совершаются через сеть.

Как было сказано выше, SMB работает, используя различные протоколы. В сетевой модели OSI протокол SMB используется как протокол Application/Presentation уровня и зависит от низкоуровневых транспортных протоколов. SMB может использоваться через TCP/IP, NetBEUI и IPX/SPX. Если TCP/IP или NetBEUI будут заняты, то будет использоваться NetBIOS API. SMB также может посылаться через протокол DECnet. Digital (ныне Compaq) сделала это специально для своего продукта PATHWORKS. NetBIOS в случае использования через TCP/IP имеет различные названия. Microsoft называет его в некоторых случаях NBT, а в некоторых NetBT. Также встречается название RFCNB.

С начала существования SMB было разработано множество различных вариантов протокола для обработки всё возрастающей сложности компьютерной среды, в которой он использовался. Договорились, что реальный вариант протокола, который будет использоваться клиентом и сервером, будет определяться командой negprot (negotiate protocol). Этот SMB обязан посылаться первым до установления соединения. Первым вариантом протокола был Core Protocol, известный как SMB-реализация PC NETWORK PROGRAM 1.0. Он должным образом поддерживает весь набор основных операций, который включает в себя:

* присоединение к файловым и принтерным ресурсам и отсоединение от них;
* открытие и закрытие файлов;
* открытие и закрытие принтерных файлов;
* чтение и запись файлов;
* создание и удаление файлов и каталогов;
* поиск каталогов;
* получение и установление атрибутов файла;
* блокировка и разблокировка файлов.

Аутентификация Microsoft SMB Protocol

Модель механизма защиты, которая используется в Microsoft SMB Protocol, в основном идентична модели любого другого варианта SMB-протокола. Она состоит из двух уровней защиты: user-level (пользовательский уровень) и share-level (уровень совместно используемого ресурса). Под share (опубликованный ресурс) понимается файл, каталог, принтер, любая услуга, которая может быть доступна клиентам по сети.

Аутентификация на уровне user-level означает, что клиент, который пытается получить доступ к ресурсу на сервере, должен иметь username (имя пользователя) и password (пароль). Если данная аутентификация прошла успешно, клиент имеет доступ ко всем доступным ресурсам сервера, кроме тех, что с share-level-защитой. Этот уровень защиты даёт возможность системным администраторам конкретно указывать, какие пользователи и группы пользователей имеют доступ к определённым данным. Он используется в Windows NT, Windows 2000, Windows XP.

Аутентификация на уровне share-level означает, что доступ к ресурсу контролируется паролем, установленным конкретно на этот ресурс. В отличие от user-level, этот уровень защиты не требует имя пользователя для аутентификации и не устанавливается никакая уникальность текущего пользователя. Этот уровень используется в Windows NT, Windows 2000 и Windows XP для обеспечения дополнительного уровня контроля защиты сверх user-level. Операционные системы Windows 95, Windows 98 и Windows ME реализуют защиту только этого уровня.

В обоих этих уровнях защиты используется шифрование. Пароль зашифровывается, прежде чем отправляется на сервер. Типы шифрования NTLM, NTLMv2 и старые версии LAN Manager (LM) поддерживаются протоколом. Оба метода шифрования используют аутентификацию типа отклик-отзыв, в которой сервер посылает клиенту случайную сгенерированную строку, а клиент возвращает в качестве отзыва обработанную строку, которая доказывает, что клиент имеет достаточный мандат для доступа к данным.

Безопасность

На протяжении всего срока эксплуатации эталонной реализации протокола от Microsoft специалистами по информационной безопасности выявлялись уязвимости, позволяющие успешно провести сетевую атаку на удалённый узел. Организация атаки на незащищённые серверы SMB является одной из наиболее привлекательных среди злоумышленников. Так, например, с помощью использования уязвимостей протокола SMB были осуществлены взлом серверов Sony Pictures Entertainment и распространение вредоносного ПО DoublePulsar, WannaCry (уязвимость EternalBlue) и Petya.

## Архитектура безопасности Windows Server, управление пользователями и группами.

В целом безопасность в Windows Server осуществляется за счет AD.

Управление пользователями и группами можно осуществить через консоль «пользователи и компьютеры Active Directory». Также мы можем создавать, изменять групповые политики, которые применяются в зоне действия контейнера, котором они находятся.

AD обладает гибким механизмом назначения прав на основе ACL.

## Управление сервисами Windows Server

Управление сервисами (также как и ролями и компонентами) происходит в диспетчере серверов. Во вкладке «управление» мы можем добавить и убрать роль и компонент для сервера, не только для локального, но и для другого сервера в домене.

## Развертывание ПО через групповые политики.

Для развертывания ПО в групповой политике лучше создавать отдельные GPO и привязывать к отдельным контейнерам, чтобы упростить повторное разворачивание ПО или обновление.

Для того, чтобы развернуть ПО необходимо создать GPO объект. Далее зайти в Политики, Конфигурация программ, Установка программ. После чего создать пакет. Установочный файл необходимо разместить в какой-нибудь общей папке.

Можно разворачивать для отдельных пользователей, так и для компьютера.

## Назначение и примеры использования WSUS.

Компонент Windows Server Update Services устанавливается в диспетчере серверов через вкладку «управление».

## Контроль доступа к ресурсам.  ACL. Мандатный доступ.

ACL (Access Control List) – список контроля доступа, который состоит из ACE.

ACE состоит из SID, маски разрешений и маски запретов.

Эффективные права – объединение множеств прямо и косвенно назначенных разрешений за вычетом объединения множеств прямо и косвенно назначенных запретов.

Мандатный доступ – модель контроля и управления доступом, основанная на мандатной модели управления доступом, при которой объекты классифицируются по уровням секретности, а субъектам выдается мандат доступа определенного уровня.

Секретность объекта не может быть понижена.

Чтение объекта с более высоким уровнем секретности невозможна.

## Схемы безопасности в сетях. Одноранговые, централизованные и распределенные системы.

Идентификация – установление личности субъекта

Аутентификация – подтверждение подлинности субъекта

Авторизация – проверка прав доступа субъекта к ресурсам

Одноранговые – на каждом узле своя система безопасности и ресурсы, необходима дополнительная аутентификация.

Централизованные – на каждом узле своя система безопасности, выступающая клиентом централизованной система безопасности, нет необходимости дополнительной аутентификации.

Распределенные – на каждом уровне своя система безопасности, выступающая клиентом распределенной система безопасности, нет необходимости дополнительной аутентификации.

## Службы каталогов на примере Active Directory.

Каталог – иерархическая структура, в которой хранятся сведения об объектах в сети. Служба каталогов предоставляет методы для хранения данных каталога и предоставления доступа к этим данным сетевым пользователям и администраторам.

Проблемы, которые решает AD:

* Множественная аутентификация
* Управление учетными записями
* Масштабирование систем аутентификации и авторизации

Особенности AD:

* Централизованный репозиторий данных
* Распределенная архитектура
* Средство авторизации и аутентификации
* Средство управления субъектно-объектных отношений
* Система хранения данных
* Логическая структура в виде дерева
* Два типа объектов: контейнеры и листья
* Логическая структура из DNS

Изображение выглядит как текст

Автоматически созданное описание

Хозяин схемы (на лес) – следит за целостностью схемы

Хозяин именования доменов (на лес) – поддерживает уникальность имен для создаваемых доменов. Добавление и удаление доменов в пределах леса. Создание shortcut. Переименование.

Хозяин идентификаторов – выдает другим контроллерам пачки по 500 SID

Эмулятор PDC – репликация изменение паролей, сервер точного времени в домене, защищает административные группы от изменения. Работа с групповыми политиками.

Хозяин инфраструктуры – отвечает на вопрос, какие пользователи из других доменов содержатся в нашем домене. Хранит некий фантомный объект. Отвечает за перемещение пользователей между доменами. Поддерживает идентификаторы удаляемых или перемещаемых объектов на время репликации изменений между контроллерами домена.

Узнать, где роли: Get-ADDomainController или netdom query fsmo

Переместить роли: Move-ADDirectoryServerOperationMasterRole -Identity куда -OperationMaterRole ид или имя роли