Лабораторная работа 5. Файловые службы и общие сетевые файловые ресурсы в ОС Windows (SMB). Разрешения NTFS.

Теоретический материал.

Файловый сервер

Файловый сервер — это выделенный компьютер в сети, предназначенный для хранения файлов. К нему организован совместный доступ пользователей, которые могут скачивать, закачивать, изменять и удалять файлы.

Этот термин может означать как оборудование, так и программное обеспечение, необходимое для выполнения функций файлового сервера.

На файловом сервере каждому авторизованному пользователю предоставляется определенное пространство для хранения рабочих файлов. Другие пользователи могут также их открывать, читать и редактировать, в соответствии с их правами доступа. Эти права устанавливаются администратором файлового сервера. Он определяет, кто какие файлы и в каких папках может открывать и просматривать, а также (если это разрешено) редактировать, удалять или добавлять новые файлы.

Способы организации файловых серверов:

Компьютер пользователя. В самом простом варианте, если в корпоративной сети немного пользователей (порядка 10-15), то в качестве файлового сервера может быть использован любой компьютер пользователя в сети компании. Это, конечно, далеко не лучший вариант, поскольку при перезагрузке или выключении этого компьютера сеть оказывается без файлового сервера. Кроме того, пользовательские операционные системы мало подходят для работы в качестве сервера.

Сервер с установленной ОС (Windows Server или Unix), на котором системный администратор настраивает роль файлового сервера. Это самый дорогой вариант, но и самый универсальный, поскольку все настройки можно сделать точно в соответствии с требованиями.

Выделенный сервер без предустановленной ОС, например файловый сервер FreeNAS. Этот программный сервер предназначен только для системы файлового хранения. Такой метод дает возможность самостоятельно выбрать оборудование, но разворачивание займет больше времени.

Решение под ключ. Представляет собой сервер, на котором производителем или поставщиком предустановлена система с настроенным сервисом

хранения данных. Такой вариант удобен тем, что он требует не более 10 минут настройки для последующей работы. Это также недешевый вариант и имеющий некоторые ограничения, поскольку все настройки предусмотрены разработчиками.

Для организации работы с файловыми серверами, как правило, используются протоколы SMB, NFS, FTP, SFTP.

Протокол SMB

SMB (англ. Server Message Block) (Одна из версий называется CIFS (Common Internet File System)) — сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам, COM-портам и другим сетевым ресурсам, а также для межпроцессного взаимодействия. Протокол главным образом используется в операционных системах Microsoft Windows, где был известен как "Microsoft Windows Network" перед последующим внедрением Active Directory. Соответствующими службами в Windows являются LAN Manager Server (для серверного компонента) и LAN Manager Workstation (для клиентского компонента).

SMB может работать на верхнем слое сетевой сессии (или ниже) несколькими путями:

- Напрямую через TCP, порт 445;
- Через NetBIOS API, который в свою очередь может работать несколькими способами:
  - Через UDP, порты 137,138 и TCP, порты 137, 139;
  - С помощью устаревших протоколов, таких как NBF, IPX/SPX;

SMB "Межпроцессные коммуникации" (англ. Inter-process Communication, IPC) обеспечивает именованные каналы и является одним из первых межпроцессных механизмов, обычно доступных для программистов и предоставляющих средства аутентификации, когда клиент впервые подключается к серверу SMB.

Некоторые сервисы, которые работают по именованным каналам, такие как те, которые используют реализацию DCE/RPC через SMB от Microsoft, известную как MSRPC через SMB, также позволяют клиентским программам

MSRPC выполнять аутентификацию, которая переопределяет авторизацию, предоставляемую сервером SMB, но только в контексте клиентской программы MSRPC, что является дополнительной проверкой подлинности.

Samba — пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах по протоколу SMB/CIFS. Имеет клиентскую и серверную части. Является свободным программным обеспечением, выпущена под лицензией GPL.

Начиная с четвёртой версии, разработка которой велась почти 10 лет, Samba может выступать в роли контроллера домена и сервиса Active Directory, совместимого с реализацией Windows 2000, и способна обслуживать все поддерживаемые Microsoft версии Windows-клиентов, в том числе Windows 10.

Samba работает на большинстве Unix-подобных систем, таких как Linux, POSIX-совместимых Solaris и Mac OS X Server, на различных вариантах BSD; в OS/2 портирован Samba-клиент, являющийся плагином к виртуальной файловой системе NetDrive. Samba включена практически во все дистрибутивы Linux.

Разрешения NTFS

NTFS (аббревиатура от англ. new technology file system — «файловая система новой технологии») — стандартная файловая система для семейства операционных систем Windows NT фирмы Microsoft.

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 повышения надёжности файловой системы в NTFS используется система журналирования USN. Для NTFS размер кластера по умолчанию составляет от 512 байт до 64 КБ в зависимости от размера тома и версии ОС.

Основой системы безопасности операционных систем Windows служит файловая система NTFS, которая предполагает использование так называемых разрешений. Под разрешением NTFS понимается правило, связанное с объектом (файлом, папкой) и используемое для управления доступом пользователей к этому объекту. При этом под пользователем понимается не только пользователь-человек как таковой, но и программы, запущенные от его имени (под его учетной записью).

В NTFS, разрешения назначаемые папкам, отличаются от разрешений, назначаемых файлам. Причем в NTFS предусмотрен как стандартный набор разрешений (для общих случаев), так и специализированный набор - для «тонкой» настройки.

Стандартные разрешения

Особенность разрешений для папок заключается в том, что они определяют возможные действия как для самих папок, так и для содержащихся внутри них файлов и подпапок. Ниже в таблице показано, что это могут быть за разрешения.

Стандартные разрешения NTFS для папок:

Разрешение	**Допускаемые действия**
Чтение (Read)	Разрешается просматривать вложенные папки и файлы, а также их свойства: имя владельца, разрешения и атрибуты (такие как «только чтение», «скрытый», «архивный» и «системный»)
Запись (Write)	Разрешается создавать и размещать внутри папки новые файлы и подпапки, а также изменять атрибуты папки и просматривать ее свойства: владельца и разрешения
Список содержимого папки (List folder contents)	Дает право просматривать имена содержащихся в папке файлов и вложенных подпапок
Чтение и выполнение (Read&Execute)	Позволяет получить доступ к файлам в подпапках, даже если нет доступа к самой папке. Кроме того разрешает те же действия, что предусмотрены для разрешений «Чтение» и «Список содержимого папки»
Изменение (Modify)	Разрешает все действия, предусмотренные для разрешений «Чтение» и «Чтение и выполнение» + разрешает удаление папки
Полный доступ (Full control)	Предоставляет полный доступ к папке. Это значит, что допускаются все действия, предусмотренные всеми

	перечисленными выше разрешениями. Дополнительно позволяется становиться владельцем папки и изменять ее разрешения
Особые разрешения (Special Permission)	Задает набор специальных разрешений, отличающийся от стандартных. Перечислены ниже

Разрешения для файлов имеют те же названия, но смысл их несколько отличается.

Стандартные разрешения NTFS для файлов:

Разрешение	**Допускаемые действия**
Чтение (Read)	Разрешается чтение файла, а также просмотр его свойств: имя владельца, разрешений и атрибутов
Запись (Write)	Разрешается перезапись файла, изменение его атрибутов, а также просмотр его владельца и разрешений
Чтение и выполнение (Read&Execute)	То же что и «Чтение» + возможность запуска приложения (если файл исполняемый)
Изменение (Modify)	Допускает изменение и удаление файла + то, что предусмотрено разрешениями «Запись» и «Чтение и выполнение»
Полный доступ (Full control)	Предоставляет полный доступ к файлу. Это значит, что допускаются все действия, предусмотренные всеми перечисленными выше разрешениями. Дополнительно позволяется становиться владельцем файла и изменять его разрешения
Особые разрешения (Special Permission)	Задает набор специальных разрешений, отличающийся от стандартных. Перечислены ниже

Специальные разрешения

Если стандартные разрешения предназначены для общих случаев, для быстрого и удобного назначения прав доступа, то специализированные права доступа позволяют подойти к этому делу более ответственно.

При этом можно изменить стандартный набор разрешений так, как будет необходимо. Описание специализированных разрешений как для папок, так и для файлов показано в таблице ниже.

Специальные разрешения NTFS для файлов и папок:

Разрешение	**Описание**
Обзор папок / Выполнение файлов	Для папок. Разрешение «Обзор папок» позволяет или запрещает перемещение по структуре папок в поисках других файлов или папок. Причем это допускается даже в тех случаях, когда пользователь не обладает разрешением на доступ к просматриваемым папкам. Для разрешения «Обзор папок» имеется одно ограничение: оно действительно только в том случае, если группа или пользователь не обладает правом «Обход перекрестной проверки», устанавливаемым в оснастке «Групповая политика». (По умолчанию правом «Обход перекрестной проверки» наделена группа «Все»). Для файлов. Разрешение «Выполнение файлов» позволяет или запрещает запуск программ. Обратите внимание, что разрешение «Обзор папок» для папки не означает автоматическую установку разрешения «Выполнение файлов» для всех файлов, размещенных в этой папке
Содержание папки / Чтение данных	Для папок. Разрешение «Содержание папки» позволяет или запрещает просмотр имен файлов и подпапок, содержащихся в папке. Это разрешение относится только к содержимому данной папки и не означает, что имя самой этой папки также должно включаться в список. Для файлов. Разрешение «Чтение данных» позволяет или запрещает чтение данных из файла
Чтение атрибутов	Разрешает или запрещает просмотр таких атрибутов файла или папки, как «Только чтение» и «Скрытый»
Чтение дополнительных атрибутов	Разрешает или запрещает просмотр дополнительных атрибутов файла или папки. Дополнительные атрибуты определяются программами и могут различаться для разных программ
Создание файлов / Запись данных	Для папок. Разрешение «Создание файлов» позволяет или запрещает создание файлов в папке (применимо только к папкам). Для файлов. Разрешение «Запись данных» позволяет или запрещает внесение изменений в файл и запись поверх имеющегося содержимого
Создание папок / Дозапись данных	Для папок. Разрешение «Создание папок» позволяет или запрещает создание папок внутри папки (применимо только к папкам).

	Для файлов. Разрешение «Дозапись данных» позволяет или запрещает внесение данных в конец файла, но не изменение, удаление или замену имеющихся данных (применимо только к файлам)
Запись атрибутов	Разрешает или запрещает смену таких атрибутов файла или папки, как «Только чтение» и «Скрытый». При этом разрешение «Запись атрибутов» не подразумевает права на создание или удаление файлов или папок: разрешается только вносить изменения в их атрибуты
Запись дополнительных атрибутов	Разрешает или запрещает смену дополнительных атрибутов файла или папки. Дополнительные атрибуты определяются программами и могут различаться для разных программ. Разрешение «Запись дополнительных атрибутов» не подразумевает права на создание или удаление файлов или папок: разрешается только вносить изменения в их атрибуты
Удаление	Разрешает или запрещает удаление файла или папки. Если для файла или папки отсутствует разрешение «Удаление», то объект все же можно удалить при наличии разрешения «Удаление подпапок и файлов» для родительской папки
Удаление подпапок и файлов	Это разрешение применяется только к папкам. Оно позволяет или запрещает удаление подпапок и файлов внутри папки даже в тех случаях, когда отсутствует разрешение «Удаление»
Чтение разрешений	Разрешает или запрещает чтение разрешений на доступ к файлу или папке (т.е. разрешений «Полный доступ», «Чтение» и «Запись»)
Смена разрешений	Разрешает или запрещает смену разрешений на доступ к файлу или папке (таких как «Полный доступ», «Чтение» и «Запись»)
Смена владельца	Разрешает или запрещает вступать во владение файлом или папкой. Привилегия владельца состоит в том, что он всегда может изменять разрешения на доступ к файлу или папке, независимо от любых разрешений, защищающих этот файл или папку
Синхронизация	При одновременном доступе к одним и тем же папкам (файлам) данное разрешение позволяет или запрещает ожидание различными потоками файлов или папок и синхронизацию их с другими потоками. Это разрешение применимо только к программам, выполняемым в многопоточном режиме с несколькими процессами

Разрешения для файлов и папок

Ниже, в таблице показано, какие особые разрешения входят в какие стандартные разрешения. Например, можно увидеть, что в стандартное разрешение «Полный доступ» входят все специальные разрешения, а в стандартное разрешение «Изменение» - все, кроме «Удаление подпапок и файлов», «Смена разрешений» и «Смена владельца».

В таблице также можно увидеть, что стандартные разрешения «Список содержимого папки» и «Чтение и выполнение» включают в себя одинаковый перечень особых разрешений. Тем не менее разница все-таки есть, а заключается она в том, что наследуются эти разрешения по разному. Так, разрешение «Список содержимого папки» наследуется только папками и отображается только при просмотре разрешений на доступ к папкам. Файлами это разрешение не наследуется.

Что касается разрешения «Чтение и выполнение», то оно наследуется как папками, так и файлами. Отображается оно также при просмотре разрешений на доступ как к папкам, так и к файлам.

В этой связи следует отметить, что пользователи, которым разрешен полный доступ к папке, могут удалять любые файлы в этой папке, независимо от установленных для них разрешений.

Вхождение специальных разрешений в стандартные разрешения.

Особые разрешения	Стандартные разрешения					
	Полный доступ	Изменение	Чтение и выполнение	Список содержимого папки (только для папок)	Чтение	Запись
Обзор папок/ Выполнение файлов	X	X	X	X		
Содержание папки/ Чтение данных	X	X	X	X	X	
Чтение атрибутов	X	X	X	X	X	
Чтение дополнительных	X	X	X	X	X	

атрибутов						
Создание файлов/ Запись данных	X	X				X
Создание папок/ Дозапись данных	X	X				X
Запись атрибутов	X	X				X
Запись дополнительных атрибутов	X	X				X
Удаление подпапок и файлов	X					
Удаление	X	X				
Чтение разрешений	X	X	X	X	X	X
Смена разрешений	X					
Смена владельца	X					
Синхронизация	X	X	X	X	X	X

Группы Active Directory

Группа Active Directory – это совокупность объектов в Active Directory. В группу могут входить пользователи, компьютеры, другие группы и другие объекты AD. Администратор управляет группой как одним объектом. В Active Directory существует 7 типов групп: две группы с тремя областями действий в каждой и локальная группа безопасности.

В AD существует два типа групп:

- **Группа безопасности** – этот тип группы используется для предоставления доступа к ресурсам. Например, вы хотите предоставить определенной группе доступ к файлам в сетевой папке. Для этого нужно создать группу безопасности.
- **Группа распространения** – данный тип групп используется для создания групп почтовых рассылок (как правило используется при установке Microsoft Exchange Server). Письмо, отправленное на такую

группу, дойдет всем пользователям группы. Это тип группы нельзя использовать для предоставления доступа к ресурсам домена.

Для каждого типа группы существует три области действия:

- **Локальная в домене** — используется для управления разрешениями доступа к ресурсам (файлам, папкам и другим типам ресурсам) только того домена, где она была создана. Локальную группу нельзя использовать в других доменах (однако в локальную группу могут входить пользователи другого домена). Локальная группа может входить в другую локальную группу, но не может входить в глобальную.
- **Глобальная группа** – данная группа может использоваться для предоставления доступа к ресурсам другого домена. В эту группу можно добавить только учетные записи из того же домена, в котором создана группа. Глобальная группа может входить в другие глобальные и локальные группы.
- **Универсальная группа** — рекомендуется использовать в лесах из множества доменов. С помощью нее можно определять роли и управлять ресурсами, которые распределены на нескольких доменах. В том случае, если в вашей сети имеется много филиалов, связанных медленными WAN каналами, желательно использовать универсальные группы только для редко изменяющихся групп. Т.к. изменение универсальной группы вызывает необходимость репликации глобального каталога во всем предприятии.

Отдельно выделяют **локальные группы**. Эти группы создаются в локальной базе данных диспетчера безопасности учетных записей (SAM) только одного компьютера. В отличии от доменных групп, локальные группы работают даже в случае недоступности контролеров домена.

AGDLP

AGDLP (сокращение от «**a**ccount, **g**lobal, **d**omain **l**ocal, **p**ermission» или «учетная запись, глобальная, локальная в домене, разрешение») кратко резюмирует рекомендации Microsoft по реализации управления доступом на основе ролей (RBAC) с использованием вложенных групп в домене Active Directory (AD): учетные записи пользователей и компьютеров являются членами глобальных групп, которые входят в локальные группы в домене,

которым в свою очередь присваиваются разрешения на ресурсы или назначаются права доступа.

Стратегия **AGDLP** как правило применяется в структурах с одним доменом AD. Для нескольких доменов или лесов рекомендуется использовать стратегию **AGUDLP** (сокращение от «**a**ccount, **g**lobal, **u**niversal, **d**omain **l**ocal, **p**ermission»).

Список источников:

1. https://itelon.ru/blog/faylovyy-server/
2. https://ru.bmstu.wiki/SMB_(Server_Message_Block)
3. https://ru.wikipedia.org/wiki/Samba
4. https://ru.wikipedia.org/wiki/NTFS
5. https://winnote.ru/security/93-razresheniya-ntfs.html
6. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc732880(v=ws.11)
7. https://vmblog.ru/tipy-grupp-active-directory-kak-sozdat-novuyu/
8. https://en.wikipedia.org/wiki/AGDLP