# Методические рекомендации по администрированию локальных сетей под управлением операционной системы Microsoft Windows Server

Туманов Иван Анатольевич методист ГБУ ДПО "СПбЦОКОиИТ" <u>tumanov.i78@gmail.com</u>

Санкт-Петербург 2020г

#### Содержание:

- 1. Windows Server
- 2. Управление элементами Active Directory
- 3. Групповые политики
- 4. Профили пользователей
- 5. <u>Общий профиль в Windows 10</u>
- 6. <u>Делегирование полномочий в домене</u> <u>Active Directory</u>
- 7. Файловый сервер

# Windows Server

К содержанию

# Windows Server

Windows Server предназначена для организаций, в нее включены различные программные модули, в числе которых роли сервера, позволяющие выполнять следующие функции:

- Active Directory служба управления учетными записями пользователей, предназначенная для организации внутреннего контроллера домена.
- **DHCP** сетевой протокол динамического распределения хостов, позволяющий назначать автоматически IP-адреса всем компьютерам внутри локальной сети или домена. В домашних условиях эту функцию обычно выполняет роутер, но на предприятиях с большим количеством рабочих станций потребуется использовать различные дополнительные настройки этой службы.
- Файловый сервер, позволяющий хранить файлы с применением отказоустойчивых RAID-массивов, а также ограничивать доступ к определенной информации для некоторых рабочих станций или пользовательских профилей.
- Сервер обновлений устанавливает обновления на все компьютеры внутри домена по определенному расписанию.
- идр.

### Домен Windows

Домен Windows является формой компьютерной сети, в которой все учетные записи пользователей, компьютеры, принтеры и другие участники безопасности регистрируются в центральной базе данных, расположенной на одном или нескольких центральных компьютерах, называемых контроллеры домена.

Аутентификация происходит на контроллерах домена, т.е. централизовано. Каждый человек получает уникальную учетную запись пользователя, которой затем может быть назначен доступ к ресурсам в домене.

Начиная с Windows 2003, компонентом Windows, отвечающим за поддержание этой центральной базы данных является **Active Directory** или служба каталогов.

Роль контроллера домена настраивается только на серверных версиях OC Windows.

### Скачивание Windows Server

#### Скачать Windows Server 2019 для ЛВС





# Установка Windows Server 2019

	Операционная систе	ма	Архитектура	Дата измене
	Windows Server 2019	Standard Evaluation	x64	07.09.2019
	Windows Server 2019	Standard Evaluation (возможности ра	x64	07.09.2019
📃 Общие	Windows Server 2019	Datacenter Evaluation	x64	07.09.2019
Имя: WinServer2019 OC: Windows 2019 (64-bit)	Windows Server 2019	Datacenter Evaluation (возможности	x64	07.09.2019
🔳 Система		При установке лучше выд	елить боль	ше
Оперативная память: 1024 МБ Порядок загрузки: Гибкий, Жёстки Ускорение: VT-x/AM	диск, Оптический диск, й диск D-V. Nested Paging	ресурсов (особенно опера после установки и первичи	тивной пам ной настро	ияти), йки можно
Дисплей		уменьшить	•	
Видеопамять: Графический контроллер: Сервер удалённого дисплея: Запись:	128 МБ /BoxSVGA Зыключен Зыключена	Пароль администратора и можно использовать 1230	меет огран	ичения -
Носители           Контроллер: SATA           SATA порт 0:         WinServer20           SATA порт 1:         [Оптически	019.vdi (Обычный, 50,00 ГЕ й привод] Пусто	достаточно для выполнен сложности.	ия условий	ПО
Аудио Аудиодрайвер: Windows Di Аудиоконтроллер: Intel HD Au	rectSound dio	Первым делом устанавли VirtualBox, потом не забые	ваем драйв заем измен	зеры от ить имя
Сеть Адаптер 1: Intel PRO/1000 MT	Desktop (Внутренняя сеть,	OC, после рекомендуется блокировку экрана в вирту	отключить /альной ма	шине.

### Клиентские ОС в домене

Клиентом домена в семействе Microsoft Windows могут быть версии с названиями Business, Professional, Enterprise...

В версиях Ноте функционал доменной интеграции отсутствует.

Клиентом домена могут быть также OC Linux. Они могут использовать централизованную аутентификацию, но не управляются групповыми политиками.

Контроллер домена можно также развернуть на ОС Linux. Для этих целей используется свободное ПО SAMBA.

# Управление элементами Active Directory

К содержанию

### Способы управления Active Directory (AD)

Типичные задачи контроллера домена:

- 1. Управление пользователями и группами
- 2. Управление групповыми политиками домена
- 3. Управление ресурсами файлового сервера

Стандартно эти элементы доступны после установки роли контроллера домена на серверной версии Windows. Работать с ними можно на рабочем столе непосредственно или через удаленный рабочий стол.

Другой вариант - установить на рабочую станцию средства управления доменом. Это позволит управлять настройками AD пользователям, не имеющим прав администратора домена (а только эти пользователи могут удаленно подключаться к серверу без приобретения дополнительных лицензий терминального доступа).

В AD можно **делегировать** часть прав "не администраторам", так, например, можно позволить учителям сбрасывать пароли ученикам или включать\выключать их из группы, отвечающей за доступ к Интернет.

### Запуск оснастки управления пользователями AD



Выполнить "dsa.msc" или в меню "пуск":

V

### Средства управления доменом

Чтобы управлять AD с клиентского компьютера с Windows (7-10), необходимо установить компонент Microsoft Remote Server Administration Tools (RSAT).

Скачать нужную версию RSAT можно бесплатно с официального сайта <u>microsoft.ru</u> указав в поиске RSAT и выбрав файл для нужной версии Windows и разрядность.

Возможно управление AD в PowerShell - оболочке с интерфейсом командной строки.

Начиная с версии Windows 10 1809 RSAT включены в ОС, необходимо



# Подразделение (OU, Organizational Unit)

Организационное **подразделение** (OU) представляет собой контейнер в домене Active Directory, который может содержать различные объекты из того же самого домена AD: другие контейнеры, группы, аккаунты пользователей и компьютеров.

Две основные задачи OU, кроме хранения объектов Active Directory:

- 1. Делегирование управления и административных задач внутри домена другим администраторам и обычным пользователям без предоставления им прав администратора домена;
- **2.** Назначение групповых политик на все объекты (пользователей и компьютеры), которые находятся в данном подразделении (OU).

Подразделение	<ul> <li>Датіче Directory</li> <li>Файл Действие</li> <li>Файл Действие</li> <li>Файл Действие</li> <li>Пользователи и</li> <li>Сохраненные</li> <li>Сохраненные</li> <li>School.lan</li> <li>Вuilti</li> <li>Comi</li> <li>Domi</li> <li>Forei</li> <li>Mana</li> <li>Users</li> </ul>	- пользователи и компьютеры Вид Справка Вид Справка Вид Справка Мия волинотеры Компьютеры Запросы Делегирование управления Найти Сменить домен Сменить контроллер домена Повысить режим работы домена Хозяева операций	<mark>i (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)</mark>	Описание Default container for up Default container for do Default container for sec Default container for ma Default container for up
Новый объект - Подразделение Создать в: school.lan/	×	Создать Все задачи Вид Обновить Экспортировать список Свойства	> >	Компьютер Контакт Группа InetOrgPerson msDS-ShadowPrincipalContainer msImaging-PSPs Псевдоним очереди MSMQ
ТЕАСНЕПСЯ Защитить контейнер от случайного удаления ОК Отме	а Справка	Справка		Подразделение Принтер Пользователь Общая папка

# Группа 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 AD существует два типа групп:

- **1.** Группа безопасности этот тип группы используется для предоставления доступа к ресурсам, например, к сетевым каталогам.
- **2.** Группа распространения данный тип групп используется для создания групп почтовых рассылок, нельзя использовать для доступа к ресурсам домена.

Для каждого типа группы существует три области действия:

- 1. Локальная в домене используется для управления разрешениями доступа к ресурсам (файлам, папкам и другим типам ресурсам) только того домена, где она была создана.
- **2.** 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.
- **3.** Универсальная группа рекомендуется использовать в лесах из множества доменов.

Так как обычно в школах нет леса и почтовых доменов, то достаточно создавать все группы с настройками по умолчанию как глобальные группы безопасности.

	Имя группы (пред-Windows 2000)	:
<ul> <li>Аctive Directory - пользователи и компьютеры</li> <li>Файл Действие Вид Справка</li> <li>Файл Действие Вид Справка</li> <li>Пользователи и компьютеры</li> <li>Пользователи и компьютеры</li> <li>Сохраненные запросы</li> <li>School.lan</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal:</li> <li>Managed Service Accour</li> <li>Users</li> </ul>	teachers Область действия группы Локальная в домене Глобальная Универсальная	Тип группы (© Группа безопасности () Группа распространения ОК Отмена
Делегирование управления Переместить Найти Создать Все задачи	Компьютер Контакт	
Вид	Группа	

Новый объект - Группа

Имя группы:

teachers

Создать в: school.lan/TEACHERS

Х

Пользо	рвате	лР Г	Новый объект	Пользователь		×		
			Score Core	адать в: school.la	n/TEACHERS			
📃 Active Directory - г Файл Действие В <del>ф</del> 🔿 📷 4	пользователи и Вид Справка 📋   🗙 🕎	компьютер	Имя: Фамилия: Полное имя:	teacher teacher	Инициалы:			
<ul> <li>Пользователи и ко</li> <li>Сохраненные з</li> <li>school.lan</li> <li>Builtin</li> </ul>	апросы	1мя teachers	Имя входа пол teacher Имя входа пол	пьзователя: пьзователя (пред-V	@school Jan Vindows 2000):	Новый объект - Пользо	ватель school Jan/TEACHERS	>
<ul> <li>Computers</li> <li>Domain Cor</li> <li>ForeignSecu</li> <li>Managed Se</li> <li>Users</li> </ul>	ntrollers irityPrincipal: irvice Accour				< Назад Далее >	Пароль: Подтверждение:	•••••	
TEACHEDE	Делегировани Переместить Найти	е управлени	я			Пребовать смены па Запретить смену па Срок действия паро Отключить учетную	ароля при следующем входе в систему роля пользователем ля не ограничен запись	
	Создать Все задачи Вид		>	Компьютер Контакт Группа			(Hasan Danee )	Отнена
< Создание нового	Вырезать Удалить Переименоват Обновить Экспортирова	ть список		InetOrgPerson msDS-Shadov msImaging-P Псевдоним о Подразделен Принтер	n vPrincipalContainer SPs ичереди MSMQ ие		Тазай	Umena
	Свойства			Пользовател	b			

### Добавление пользователя в группу

14	Ture	0	Выбор: "Г	руппы"	×
	Тип	Описание	Выберите	тип объекта:	
teacher	Копироват	гь	"Группы"	или "Встроенные субъекты безопасности"	Типы объектов
and teachers	Добавить	в группу	В следуюц school.lan	цем месте:	Размещение
			Введите и teachers	мена выбираемых объектов (примеры):	2 Проверить имена
Свойства: teacher			? ×	тельно	3 ОК Отмена
Профиль слу Общие Адрес Член групп Входя Член групп:	жо удаленных рабочи Учетная запись Пр ящие звонки Среда	х столов С офиль Телефоны Ор Сеансы Удаленное у	ОМ+ оганизация правление		
Имя	Папка доменных о	служб Active Directory			
teachers	school.lan/TEACH	ERS			
Добавить	Удалить				

# Групповые политики

К содержанию

### Групповые политики

**Групповая политика** (Group Policy Object, GPO) - механизм, позволяющий изменять различные параметры, связанные с операционной системой, пользователями и различными приложениями в графическом режиме при помощи **редактора** групповых политик.

Большинство настроек Windows возможны через реестр, редактор GPO это фактически и делает, но наглядным способом.

GPO представляет собой файлы в определенном формате, связанные (назначенные) определенным объектам.

Групповые политики подразделяются на:

- локальные (выполнить gpedit.msc)
- доменне (выполнить gpmc.msc)

### Структура групповых политик



Групповая политика делится на две категории:

- Конфигурация компьютера. Политики этой категории применяются ко всему компьютеру независимо от пользователя. Например, если вы хотите применить политику надежности пароля для всех пользователей на компьютере или в домене, измените соответствующую политику в этой категории.
- Конфигурация пользователя. Политики этой категории применяются к
   пользователям, а не ко всему компьютеру, независимо от того, с какого компьютера пользователь входит в систему. Это, например, ограничения на доступ к
   отдельному ПО или скрипты при входе в систему.

#### Групповые политики в домене

В домене групповая GPO является объектом, который можно связать с сайтом, доменом и подразделением (в том числе с вложенными (дочерними) подразделениями).

В случае наличия нескольких групповых политик сразу, порядок применения будет следующий:

- 1. Локальная групповая политика.
- 2. Групповая политика сайта.
- 3. Групповая политика домена.
- 4. Групповая политика верхнего подразделения.
- 5. Групповая политика дочернего подразделения.

Это надо учитывать и, при необходимости, отключать наследование GPO.

## Политика сложности паролей в домене

🚈   🌛 📕 🗢   Администрирован	Г → Администрирование Управление			Для этого надо изменить уже
Файл Главная Поделиться	Вид	Средства работы с	ярлыками	
$\leftrightarrow$ $\rightarrow$ $\checkmark$ $\bigstar$ 🦓 « Система и	безопасност	ть > Администриро	ование	умолчанию политику домена.
<ul> <li>Быстрый доступ</li> <li>Рабочий стол</li> <li>Загрузки</li> <li>Документы</li> </ul>	Имя * 3 * 2 *	я Модуль Active Direc Монитор брандмау Монитор ресурсов Оптимизация диско	tory для Window эра Защитника 18	
📰 Изображения 🔛 Ул System32 🎰 🖷	правление груг айл Действие	пповой политикой е Вид Окно Справ 🕢 🔽 📷	ка	
<ul> <li>Этот компьютер</li> <li>Видео</li> </ul>	равление груп Лес: school.la	пповой поли school.li	а <b>п</b> Связанные объек:	ты групповой политики Наспедование групповой политики Делен
> 🗎 Документы	Домены Зі school.	l.lan	Порядок ссылок	Объект групповой политики Принудительный
> 👆 Загрузки 🔷	Сайты В Моделиро	ование групг	1	Default Domain Policy Изменить
> 📰 Изображения	<b>D</b>	Системный монито	р	
> 🧊 Музыка	100 m	Службы Microsoft A	zure	
> Объемные объекты > Рабочий стол		Службы компонент Службы	OB	
> 🏪 Локальный диск (С:)		Средство проверки	памяти Window	
		лиравление группо	Бой политикой	

### Политика сложности паролей в домене

Нужно привести параметры доменной групповой политики в вид, как на рис.

Политики из категории "Конфигурация компьютера" применяются только при загрузке ПК (поэтому лучше перезагрузить сервер).

Политики из категории "Конфигурация пользователя" применяются при логине ПК (достаточно "выйти и зайти").



# Создание объектов GPO

Чтобы не забивать настройками общую доменную политику, часто лучше создать несколько отдельных политик для определенных подразделений.

📓 Управление групповой поли	тикой			
🔜 Файл Действие Вид Ок	но Сг	равка		
🗢 🔿 🖄 📰	0			
📓 Управление групповой поли	TEAC	HERS		
<ul> <li>Домены</li> </ul>	Связа	инные объекты групповой поли	тики	Наследование групповой пол
<ul> <li>school.lan</li> <li>Default Domain</li> <li>Domain Contro</li> <li>TEACHERS</li> </ul>	\$ \$	Порядок ссылок	Объе	ект групповой политики
> 📑 Объекты г	Создат	ь объект групповой политики	и в эт	ом домене и связать его
<ul> <li>&gt; Фильтры \</li> <li>&gt; 🧊 Начальны</li> <li>&gt; 👔 Сайты</li> <li>🙀 Моделирование</li> </ul>	Связат Блокир Обнов	ь существующий объект груг оовать наследование ление групповой политики	пово	ой политики
🖳 Результаты групг	Мастер	моделирования групповой	поли	тики

# Профили пользователей

К содержанию

### Профиль пользователя

Профиль пользователя Windows – это набор файлов и папок, которые закреплены за конкретной учетной записью. В профиле пользователя Windows находятся файлы, содержащие информацию об индивидуальных настройках операционной системы, о ярлыках программ и файлов, размещенных в меню Пуск, на панели задач или Рабочем столе.



### Типы профилей

Профили подразделяются на:

- локальные (привязаны к локальному ПК)
- перемещаемые (за счет хранения в сети, синхронизируются и копируются пользователю при входе на любую доменную машину)

Перемещаемые профили могут быть также:

- общими (едиными для нескольких пользователей)
- обязательными (не сохраняющими изменения)

В домене при большом количестве однотипных пользователей удобно создать один перемещаемый общий обязательный профиль, тогда не надо "переживать" за изменение внешнего вида рабочего стола учениками.

Персональные данные хранятся на индивидуальных сетевых каталогах.

Документация на сайте microsoft.

#### Подготовка каталогов на сервере



# Перемещаемый профиль в AD

Указываем в AD путь к профилю.	Файл Главная Поделиться Вид
После первого входа пользователя	← → → ↑ 📙 « Локальный диск (C:) → SRV → PROFILES
на рабочую станцию на сервере появится каталог с его профилем.	<ul> <li>Вагрузки</li> <li>Ж № Имя</li> <li>Документы</li> <li>Ж № Цеасher.V6</li> <li>В Изображения</li> </ul>
Файл Действие Вид Справка	Профиль доступен
Пользователи и компьютеры Сохраненные запросы School.lan Builtin	только данному пользователю.
<ul> <li>Schoollan</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal:</li> <li>Managed Service Accour</li> <li>Users</li> <li>TEACHERS</li> <li>TEACHERS</li> <li>TEACHERS</li> <li>Ceoйcтва: teacher</li> <li>Член групп Входящие звонки Ср Профиль служб удаленных раб Общие Адрес Учетная запись</li> <li>Профиль пользователя</li> <li>Путь к профилю: \wserver\p Сценарий входа:</li> <li>Домашняя папка</li> <li>Подключить: </li> </ul>	<ul> <li>? ×</li> <li>При входе он будет</li> <li>подгружаться, при</li> <li>выходе - выгружаться</li> <li>на сервер.</li> <li>На локальных</li> <li>машинах будут</li> <li>оставаться копии</li> <li>профиля для</li> <li>ускорения загрузки.</li> </ul>

# Обязательный профиль



Разрешения на каталог с обязательным профилем можно сделать так:

Эле	менты р	азрешений:	
	Тип	Субъект	Доступ
92	Разр	СИСТЕМА	Полный доступ
2	Разр	teacher (teacher@school.lan)	Чтение и выполнение
82	Разр	Администраторы (SCHOOL\	Полный доступ

## Управление обязательным профилем

При необходимости внесения изменений в профиль, можно переименовать MAN в DAT, настроить разрешения пользователю на "полный доступ", войти пользователем, внести изменения, выйти и переименовать обратно, выставив разрешения "на чтение"..

Так как из "загрузок" и "рабочего стола" всё будет удаляться, пользователям надо привыкнуть...

Для сохранения файлов можно в профиле настроить ярлыки на локальные или сетевые каталоги с доступом пользователю на чтение или перенаправить на такие расположения некоторые каталоги из профиля (например, "документы").



### Неудобства перемещаемого профиля

- Если не делать профиль обязательным, то, по опыту, пользователи хранят очень много данных на рабочем столе и в загрузках (загрузки, фильмы, например), что сильно замедляет вход-выход из системы из-за синхронизации с сервером. Начинаются жалобы + "забивается" сеть.
- 2. Т.к. на ПК остаются локальные копии, то несколько перемещаемых профилей могут "съесть" все пространство на диске "С".
- 3. Настройки групповой политики по удалению локальных кэшированных профилей не всегда срабатывают корректно, иногда приходится это делать вручную.
- 4. Если профиль обязательный, то можно сделать его общим сразу для всех пользователей.

# Удаление копий профилей в групповых

#### ΠΟΠΝΤΝΚΑΧ



Надо в групповых политиках включить следующий параметр (действует после перезагрузки клиентов):

	пе проверять сооственность пользователя перемещаем	пе задана
	Удалять кэшированные копии перемещаемых профилей	Включена
Политики ОС	Domension and the second second	Lie en en en en
Помощь при ошибке «Отказано в,	:= Отключить идентификатор ооъявлении	не задана
📔 Поставщик теневых копий файлов	🗄 Не выполнять принудительной выгрузки реестра пользо	Не задана
📔 Профили пользователей	📔 Отключить обнаружение медленного сетевого подключ	Не задана

# Общий профиль в Windows 10

К содержанию

# Создание общего обязательного профиля

Этапность:

- 1. Настройка профиля на тестовой машине
- 2. Перенос профиля в "профиль по умолчанию"
- 3. Копирование профиля "по умолчанию" на сервер
- 4. Назначение профиля как перемещаемого

В Windows 10 процедура не самая явная, в ранних версиях п1 и 2 не было..

### Настройка профиля на тестовой машине

Входим на тестовую машину под администратором и настраиваем внешний вид на свой вкус. На самом деле неважно, после можно будет донастроить.



## Перенос профиля в "профиль по умолчанию"

1. Создаём файл unattend.xml следующего содержания ("amd64" поменять на "x86", если версия 32 бита) и сохраняем на диск С:

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
<settings pass="specialize">
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<CopyProfile>true</CopyProfile>
</component>
</component>
</settings>
</unattend>
```

Параметр CopyProfile указывает, что программа Sysprep (утилита системной подготовки Microsoft Windows к развертыванию) копирует папку профиля пользователя, выполнившего вход в настоящее время, в профиль пользователя по умолчанию.

#### 2. Запускаем команду

C:\Windows\System32\Sysprep\sysprep.exe /oobe /reboot /generalize /unattend:c:\unattend.xml

# Ошибки sysprep

В случае ошибки sysprep указывает файл, где указаны проблемы с запуском.

В случае Windows 10 LTSC 1809, используемой в данном курсе, ошибка вызвана наличием пакета локализации (русификации). Для дальнейшей работы в данной версии его придется удалить (потом поставим обратно).

Штатными средствами подобный пакет не удалить. Придется использовать средства PowerShell ("продвинутая" командная строка Windows).

Запускаем PowerShell (можно в поиске) и выполняем команду:

Get-AppxPackage Microsoft.LanguageExperiencePackru-RU | Remove-AppxPackage

Если всё верно, то Windows станет "английским", зато sysprep запустится и отработает.

Sysprep возвращает образ ОС в начальное состояние, сбрасывает имя ПК, отключает от домена и т.п., поэтому лучше делать на свежеустановленном образе в виртуальной машине.

# Копирование профиля "по умолчанию" на сервер

- Заходим на клиентскую машину под администратором.
- Копируем "Профиль по умолчанию" на сервер.

– 🤿 👻 Т 🔜 У Панелі	»У Иг	мя компью	тера		Оборудование
	Дополни	тельно	Защита	системы	Удаленный доступ
Панель управления — домашняя страница	Необходил перечисле	мо иметь п енных парал	рава админи метров.	стратора дл	я изменения большинст
Диспетчер устройств	Быстрод	ействие			
Настройка удаленного доступа	Визуальн виртуаль	ные эффект ной памяти	ты, использо 1	вание проце	ессора, оперативной и
Защита системы					Параметры
Дополнительные параметри	Профили	пользоват	елей		
CHCTEMBI	Парамет	ры рабочег	о стола, отн	осящиеся ко	входу в систему
					Параметры
В профилях поль иные данные, отн Для одного поль: различные проф профиль.	зователей храня юсящиеся к уче зователя на разн или или исполь	ятся парам етным запі ных компь ізовать оди	етры рабоч исям пользо ютерах мож ин перемеш	него стола и ователей. кно создать јаемый	я информация Параметры
В профилях поль иные данные, отн Для одного поль: различные проф профиль. Профили, хранящиеся на	зователей храня юсящиеся к уче зователя на разн или или исполь этом компьютер Размер	атся парам етным запи ных компь зовать оди ре: Тип	етры рабоч исям пользо ютерах мож ин перемеш	иего стола и ователей. кно создать јаемый	я информация Параметры ременные среды
В профилях поль иные данные, отн Для одного полы различные проф профиль. Профили, хранящиеся на Имя SCHOOL\teacher	зователей храня юсящиеся к уче зователя на разн или или исполь этом компьютер Размер 1 76 МБ	атся парам етным запи ных компь зовать оди ре: Тип Перем	етры рабоч исям пользо ютерах мож ин перемеш Состоя	иего стола и ователей. кно создать јаемый Изм 20.0	я информация Параметры ременные среды
В профилях поль иные данные, отн Для одного полы различные проф профиль. Профили, хранящиеся на Имя SCHOOL\teacher SCHOOL\Aдминистратор	зователей храня юсящиеся к уче зователя на разн или или исполь этом компьютер Размер 1,76 МБ 2.66 МБ	атся парам етным запи ных компь зовать оди ре: Тип Перем Локаль	етры рабоч исям пользе ютерах мож ин перемещ Состоя Перем Локаль	его стола и ователей. сно создать аемый Изм 20.0 21.0	я информация Параметры ременные среды мена Применя
В профилях поль иные данные, отн Для одного полы различные проф профиль. Профили, хранящиеся на SCHOOL\teacher SCHOOL\teacher SCHOOL\Aдминистратор WIN10-0\ladmin	зователей храня носящиеся к уче зователя на разн или или исполь этом компьютер Размер 1,76 МБ 2,66 МБ 58,5 МБ	атся парам етным запи ных компь зовать оди ре: Тип Перем Локаль Локаль	етры рабоч исям пользо ютерах мож ин перемеш Состоя Перем Локаль Локаль	иего стола и ователей. кно создать (аемый Изм 20.0 21.0	я информация Параметры ременные среды мена Примен
В профилях поль иные данные, отн Для одного полы различные проф профиль. Профили, хранящиеся на Имя SCHOOL\teacher SCHOOL\teacher SCHOOL\Aдминистратор WIN10-0\ladmin	зователей хранз юсящиеся к уче зователя на разн или или исполь этом компьюте Размер 1,76 МБ 2,66 МБ 58,5 МБ 1,52 МБ	атся парам етным запи ных компь зовать оди ре: Тип Перем Локаль Локаль	етры рабоч исям пользо ютерах мож ин перемеш Состоя Перем Локаль Локаль	него стола и ователей. кно создать даемый Изм 20.0 21.0 21.0 16.0	я информация Параметры ременные среды мена

# Копирование профиля "по умолчанию" на сервер

!!! В "Разрешить использование"

Копируем в папку с расширением .v6 (для Win10). Обязательно!

опирование профиля	× написать полн "Проверить им	ъзователя "Все" и мена"
Копировать профиль на	ок ("Everyone" в	англ.)
Обзор	Выбор: "Пользователь" или "Группа"	;
	Выберите тип объекта:	
Разрешить использование	"Пользователь" или "Встроенный субъект без	опасности" <u>Т</u> ипы объектов
	В с <u>л</u> едующем месте:	
	school.lan	<u>Р</u> азмещение
Изменить	Введите имена выбираемых объектов (примера	a):
Обязательный профиль	Bcel	Проверить имена
	Дополнительно	ОК Отмена

Только потом нажимаем "ОК" для копирования.

Можно скопировать профиль в папку на локальном диске, а потом перенести на сервер.

### Назначение профиля как перемещаемого

- 1. Назначаем в AD пользователю созданный ему перемещаемый профиль.
- 2. Даём полный доступ пользователю.
- 3. Заходим на клиенте, настраиваем профиль. (Русифицируем). Выходим.
- 4. На сервере переименовываем NTUSER.DAT в NTUSER.MAN.

Делаем всё как с обычным перемещаемым профилем, только теперь он еще и общий, соответственно, его можно назначать любому количеству пользователей.

Для внесения изменений рекомендую разрешить полный доступ к профилю на сервере только 1 пользователю ("дежурному"). Переименовывая МАN в DAT и входя под этим пользователем, можно вносить изменения в общий профиль - настраивать ярлыки, внешний вид, стартовую страницу и т.п.

По данной ссылке выложен файл unattend.xml и уже готовый профиль.

# Делегирование полномочий в домене Active Directory

К содержанию

### Предоставление прав



# Кому делегируем

Мастер делегирования упр	авления	×			
<u> A</u>	Мастер делегирования управ Этот мастер помогает предоставить управлен объектами службы каталогов. Можно предост пользователям право управлять пользователя группами, компьютерами, подразделениями и объектами службы каталогов. Для продолжения нажмите кнопку "Далее".	ления ние гавить ями, а другими			
		Мастер делег	ирования управления		×
177 S		Пользоват Выбери управле	е <b>ли или группы</b> ге пользователей или группы, к ние.	оторым вы хотите делегировать	B
		P. Konu			
		E tead	chers (SCHOOL\teachers)		
	< <u>Н</u> азад Далее>				
				Добавить Даалить	<u>,</u>
				< <u>Н</u> азад Далее> О	тмена

# Что делегируем

Мастер делегирования управления
<b>Делегируемые задачи</b> Можно выбрать обычные задачи или настроить особые.
<ul> <li>Делегировать следующие обычные задачи:</li> <li>Создание, удаление и управление учетными записями польз          <ul> <li>Создание, удаление и управление учетными записями польз</li> <li>Переустановить пароли пользователей и установить измене</li> <li>Чтение информации о всех пользователях</li> <li>Создание, удаление и управление группами</li> <li>Изменение членства в группах</li> <li>Управление ссылками на групповые политики</li> <li>Генерация RSoP (Планирование)</li> <li>Создать особую задачу для делегирования</li> </ul> </li> </ul>
< <u>Н</u> азад Далее> Отмена

# Просмотр делегированных прав. Включаем "дополнительные функции":



#### Просмотр делегированных прав.



### Просмотр делегированных прав.

.....

а́ства: STUDENTS		Для просы кнопку "И	мотра сведении об осо зменить".	оых разрешениях в	зыберите элемент (	разрешения и нажмит	e
Общие Управляется	a   0ć	<u>Э</u> лементы	і разрешений:				
Безопасность СОМ+	Групповая по	Тип	Имя	Разрешение	Унаследовано	Применять к	
руппы или пользователи:		Paspe Paspe	teachers (SCH00L\t teachers (SCH00L\t	Чтение и запи Сброс пароля	<не унаследов <не унаследов	Пользователь объ Пользователь объ	
SYSTEM		Paspe	SYSTEM	Полный доступ	<не унаследов	Только этот объект	
Eteachers (SCHOOL \teachers)		Paspe	Операторы учета (	Гюлный доступ Создание/уда	<не унаследов <не унаследов	Только этот объект	
	раторы)	Paspe	Операторы учета (	Создание/уда	<не унаследов	Только этот объект	
		Paspe Paspe	Операторы учета ( Операторы печати	Создание/уда	<не унаследов <не унаследов	Голько этот объект Только этот объект	
<b>▲</b>	Добавить	Добави Г Разрен дочерн	ить <u>И</u> зменить шить наследование раз ним объектам, добавля	<u>Удалит</u> зрешений от родит ия их к разрешения	ь ельского объекта н м, явно заданным	к этому объекту и его в этом окне.	
▲ Сазрешения для teachers	До <u>б</u> авить	До <u>б</u> аві Г Разреі дочерн	ить <u>И</u> зменить шить наследование ра: ним объектам, добавля	<u>У</u> далит зрешений от родит ія их к разрешения	ь ельского объекта н м, явно заданным	< этому объекту и его в этом окне.	
Азрешения для teachers Полный доступ	До <u>б</u> авить	До <u>б</u> ави Г Разрек дочерн	ить <u>И</u> зменить шить наследование раз ним объектам, добавля	<u>Удалит</u> зрешений от родит я их к разрешения	ь ельского объекта н ім, явно заданным	к этому объекту и его в этом окне.	
Азрешения для teachers           Полный доступ           Чтение	До <u>б</u> авить	Добави Г Разрен дочерн Чтобы зам	ить <u>И</u> зменить шить наследование раз им объектам, добавля менить все элементы р «нопкч "По чмолчанию"	<u>Удалит</u> зрешений от родит ия их к разрешения разрешений значен	ь ельского объекта к м, явно заданным чиями по умолчанию	к этому объекту и его в этом окне. о, По умолуа	эн
<ul> <li>Зазрешения для teachers</li> <li>Полный доступ</li> <li>Чтение</li> <li>Запись</li> </ul>	До <u>б</u> авить	До <u>б</u> аві дочерн Чтобы зан нажмите н Подробне	ить <u>И</u> зменить шить наследование раз им объектам, добавля менить все элементы р кнопку "По умолчанию е об <u>чправлении достчи</u>	<u>У</u> далит зрешений от родит ия их к разрешения азрешений значен  <u>том</u> .	ь ельского объекта н м, явно заданным ниями по умолчанию	к этому объекту и его в этом окне. <sup>0,</sup> По умолуа	эни
<ul> <li>Сазрешения для teachers</li> <li>Полный доступ</li> <li>Чтение</li> <li>Запись</li> <li>Создание всех дочерних объектов</li> </ul>	До <u>б</u> авить	Добави дочерн Чтобы зам нажмите н Подробнее	ить <u>И</u> зменить шить наследование раз им объектам, добавля менить все элементы р кнопку "По умолчанию" е об <u>чправлении достчи</u>	<u>У</u> далит зрешений от родит ия их к разрешения оазрешений значен 	ь ельского объекта к м, явно заданным чиями по умолчанию	к этому объекту и его в этом окне. о. По умолуа	9146
<ul> <li>Сазрешения для teachers</li> <li>Полный доступ</li> <li>Чтение</li> <li>Запись</li> <li>Создание всех дочерних объектов</li> <li>Удаление всех дочерних объектов</li> <li>Генерация RSoP (Планирование)</li> </ul>	До <u>б</u> авить	До <u>б</u> аві дочерн Чтобы зан нажмите н Подробнея	ить <u>И</u> зменить шить наследование раз им объектам, добавля менить все элементы р кнопку "По умолчанию е об <u>чправлении достчи</u>	<u>У</u> далит зрешений от родит ия их к разрешения разрешений значен 	ь ельского объекта н м, явно заданным ниями по умолчанию ОК	к этому объекту и его в этом окне. о. По умолуа Отмена При	1) 2) 1)

TORENLIA REPORTALI GORARDOCTU REG STUDENT

21 1

# Файловый сервер

К содержанию

### Сетевой каталог

При создании сетевых каталогов можно руководствоваться следующим:

- Права безопасности устанавливаются для каталога и на SMB (протокол сетевого доступа-сетевая файловая система) и на NTFS (дисковая файловая система), но NTFS позволяет изменять права для подкаталогов. Поэтому для SMB делаем полный доступ всем, а ограничения - на уровне NTFS.
- 2. Имя каталога SMB может отличаться от NTFS, добавление символа \$ к имени SMB сделает каталог скрытым (для Windows-машин).
- 3. На NTFS-уровне не забываем следить за наследованием прав безопасности оставляйте только нужные.
- 4. Пользователям "СИСТЕМА" и "Администраторы" всегда делайте полный доступ.
- 5. Сетевые каталоги создавайте на отдельном диске или разделе.

## Создание общего каталога

Сделать каталог, доступный учителям на запись, ученикам только для чтения.

- 1. Создать каталог СОММОN в C:\SRV.
- 2. Создать в AD группы безопасности "teachers" и "students"
- 3. Настроить сетевую (SMB) доступность
- 4. Настроить NTFS-безопасность

Итоговые права безопасности должны выглядеть следующим образом (но сначала отключить наследование):

#### Элементы разрешений:

Гип	Субъект	Доступ	Унаследовано от	Применяется к
азр	students (SCHOOL\students)	Чтение и выполнение	Нет	Для этой папки, ее подпапок
Разр	teachers (SCHOOL\teachers)	Полный доступ	Нет	Для этой папки, ее подпапок
Разр	СИСТЕМА	Полный доступ	Нет	Для этой папки, ее подпапок
Разр	Администраторы (SCHOOL\	Полный доступ	Нет	Для этой папки, ее подпапок
	ип азр азр азр азр	ип Субъект aзp students (SCHOOL\students) aзp teachers (SCHOOL\teachers) aзp СИСТЕМА aзp Администраторы (SCHOOL\	ип Субъект Доступ aзр students (SCHOOL\students) Чтение и выполнение aзр teachers (SCHOOL\teachers) Полный доступ aзр СИСТЕМА Полный доступ азр Администраторы (SCHOOL\ Полный доступ	ип Субъект Доступ Унаследовано от aзр students (SCHOOL\students) Чтение и выполнение Нет aзр teachers (SCHOOL\teachers) Полный доступ Нет aзр СИСТЕМА Полный доступ Нет азр Администраторы (SCHOOL\ Полный доступ Нет

# Уровень SMB

Локальный диск (C:) > SRV	∨ ⊘ Пои	ск: SRV	
Имя	Дата изменения	Тип	Разме
COMMON	27.05.2020 10:37	Папка с фай	лами
Свойства: COMMON	×	Папка с фай Папка с фай	лами
Предыдущие версии	Настройка		Вазрешения аля группы "СОММОМ"
Общие Доступ Общий доступ к сетевым файлам и СОММОN	Расширенная настройка	общего доступа и к этой папке	Разрешения для общего ресурса Группы или пользователи:
Нет общего доступа Сетевой путь: Нет общего доступа Общий доступ	Параметры Имя общего ресурса: СОММОN Добавить Удалит	b	See See
Расширенная настройка общего до Предоставляет пользовательские общие папки и задает другие допол общего доступа.	Ограничить число одн пользователей до: Примечание:	новременных	Добавить Удалить Разрешения для группы "Все" Разрешить Запретить
Расширенная настройка	Разрешения Кэш	ирование	Полный доступ Изменение Чтение И Изменение И И И И И И И И И И И И И И И И И И И
	OK	Отмена	
Закрыть	Отмена Применить		ОК Отмена Примен

# Уровень NTFS. Отключение наследования

Предыдущие версии Наст Общие Доступ Безог	ройка асность	Имя:	C:\SRV\COMMON
Имя объекта: C:\SRV\COMMON		Владелец:	Администраторы (SCHOOL\Администраторы) 🛭 🌍 Изменить
руппы или пользователи:		Разрешения	Блокировать наследование
🕵 СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ			
СИСТЕМА Администраторы (SCHOOL\Администраторы Пользователи (SCHOOL\Пользователи)		Для получения дополнител ее и нажмите кнопку "Изме Элементы разрешений:	ыных с нить" Что вы хотите сделать с текущими унаследованными разрешениями?
тобы изменить разрешения, ажмите кнопку "Изменить". изрешения для группы СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ" Разрешить	иненить Запретить	Тип Субъект В Разр СИСТЕМА В Разр Администрато	Наследование для данного объекта будет заблокировано. В результате разрешения, унаследованные от родительского объекта, больше не будут применимы к данном объекту. оры (Sf
Полный доступ Изменение	^	<ul> <li>Разр Пользователи</li> <li>Разр Пользователи</li> <li>Разр СОЗДАТЕЛЬ.</li> </ul>	(SCH) Преобразовать унаследованные разрешения в явные разрешения этого объекта.
Список содержимого папки Чтение			→ Удалить все унаследованные разрешения из этого объекта.
Запись тобы задать особые разрешения или араметры, нажмите кнопку Дополнительно".	олнительно	Добавить У Отключение наследован	Отмена
Закрыть Отмена	Применит	🛛 Заменить все записи раз	рециений дочернего объекта наследуемыми от этого объекта

### Подключение общего каталога пользователям

Подключить общий каталог можно

- **1. К букве диска**. (Настроить шаблонный профиль, или в групповых политиках, или скриптом\командой при старте (net use z: \\wserver\common) в настройках пользователя, или в автозагрузке).
- 2. Ярлыком на рабочем столе (можно через общий профиль).

Из опыта, с точки зрения безопасности, ярлык намного предпочтительней, т.к. к буквам диска часто пытаются прицепиться вирусы с файлом "autorun", который стартует при двойном клике именно на букве диска, один неаккуратный пользователь заразит всю сеть. С ярлыками таких проблем нет...





## Домашние персональные каталоги через AD

**Персональные каталоги** - способ хранения данных пользователя в сетевой папке, доступной только этому пользователю (иногда группе). Способ очень важен при использовании общих профилей, там все данные в профиле удаляются.

Создание ресурса для хранения персональных каталогов учителей (C:\SRV\THOMES, отключаем наследование, права как на рисунке):

Имя:	C:\SRV\THO	MES				
Владелец:	Администра	торы (SCHOOL\Адми	інистраторы) 🏼 🌍 Из	зменить		
Разр	ешения	Аудит Де	📕 Свойства: THOMES	Расширенная настр	Разрешения для группы "Т	HOMES"
Для получе ее и нажми Элементы р	ния дополнительных сведений те кнопку "Изменить" (если он разрешений:	вных сведений дважды щелкните з енить" (если она доступна).		<ul> <li>Открыть общий</li> <li>Параметры</li> <li>Имя общего ресу</li> <li>THOMES</li> </ul>	Разрешения для общего ресурса Группы или пользователи:	1
Тип 🞎 Разр 🎎 Разр	Субъект СИСТЕМА Администраторы (SCHOOL\	Доступ Полный доступ Полный доступ	Сетевой путь: Нет общего доступа Общий доступ	Добавить Уд Ограничить чис пользователей д Примечание:		Добавить
			Расширенная настрой Предоставляет польз общие папки и задает общего доступа.	Разрешения	Разрешения для группы "Все" Полный доступ Изменение Чтение	Разрешит

### Домашние персональные каталоги через AD

Назначаем путь к домашнему каталогу в AD.

!!! Каталог в NTFS создастся автоматически!!!.

📔 Active Directory - пользователи и ком	ипьютеры	Свойства:	teache	r				?
Файл Действие Вид Справка		Член груг	n Bxo	дящие звонки	Сред	а Сеан	сы Удале	нное управл
		Общие	Адрес	Учетная заг	ись П	рофиль	Телефоны	ы Организ
<ul> <li>Сохраненные запросы</li> <li>School.lan</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal:</li> <li>Managed Service Accour</li> <li>STUDENTS</li> <li>TEACHERS</li> <li>Users</li> </ul>	a eacher eachers	Профи Путь к Сцена Домац () Лок	иль поль с профил рий вхол шняя паг кальный дключит	азователя пю: \\wse да: пка й путь: ть:S:	rver\prof	iles\teach	ner r\thomes\tea	acher

(C:) > SRV > THOMES > Имя Права доступа только для teacher (+наследованные). При следующем входе к букве S: подключится каталог.

#### Перенаправление каталогов профиля

> 📓 TEACHERS	
🗸 📑 Объекты	Создать объект групповой политики
Новый объект группо	овой политики Х
Имя:	
redirect	
Исходный объект груп	повой политики:
(нет)	×
	ОК Отмена



Лучше не трогать доменную политику, которая действует на всех, а создать отдельный объект GPO для OU, которая будет действовать на всех пользователей, размещенных в данном подразелении.

# Перенаправление каталогов профиля

		Свойства: Документы	? ×			
Редактор управления групповыми пол	итиками	Конечная папка Параметры				
Файл Действие Вид Справка			оложение папки "Покументы"			
🔶 🧼 🞽 📰 🖼 🗟 🖬		Политика:	иложение папки документы .			
<ul> <li>Политика redirect [WSERVER.S(</li> <li>Имя</li> <li>Конфигурация компьютер</li> <li>Политики</li> <li>Настройка</li> <li>Конфигурация пользовате</li> <li>Политики</li> <li>Конфигурация пользовате</li> <li>Изоб</li> </ul>	Data(перемещаемая) эчий стол ное меню <mark>/менты</mark> бражен Свойства	Перенаправлять папки всех поль Эта папка будет перенаправлена в Расположение целевой папки — Создать папку для каждого пол	зователей в одно расположение в указанное расположение. пьзователя на корневом пути 💌			
<ul> <li>Конфигурация прог</li> <li>Конфигурация Winc</li> <li>Конфигурация Winc</li> <li>Виде</li> </ul>	ыка Справка	Корневой путь:				
<ul> <li>Сценорин (скод)</li> <li>Параметры безс</li> <li>Перенаправлени</li> <li>Конт</li> <li>ОСУ на основе п</li> <li>Загр</li> <li>Развернутые при</li> <li>Ссы.</li> <li>Административные</li> </ul>	оанное Сво такты узка Ко лки ски	ойства: Документы нечная папка Параметры Задайте условия перенаправления для	? Х			
> 🗎 Настройка 🛛 🖺 Сохр После входа пользователя	аненные игры а проверяйте	<ul> <li>Предоставить права монопольно</li> <li>Перенести содержимое "Докуме</li> <li>Применить политику перенаправа операционным системам Window Server, Windows XP и Windows Server</li> </ul>	e teacher (\\wserver\thomes) (S teacher Эдокументы			
редирект на каталогах пол	ьзователя!		<ul> <li>Видео</li> <li>Изображения</li> <li>Музыка</li> </ul>			

### Копирование пользователей

Если создавать нового пользователе в оснастке AD в режиме копирования, то перенесутся не только параметры принадлежности к группам, но и ссылка на профиль и домашний каталог.

Причем, если домашний каталог у шаблонного пользователя совпадал с его именем, то для нового сгенерируется каталог с его созданным именем!!!

📃 Active Directory - пользователи	и компьютеры			Копировать объек	т - Пользовател	пь	×
Файл Действие Вид Справка	] 🕢 📑 🔽	II 8 🐮 🖬	y 🖸 🍇	🧏 Созда	ть в: school.lar	n/TEACHERS	
Пользователи и компьютеры	Имя	Тип	Описание	Имя:	tumanov	Инициа	алы:
<ul> <li>✓ jiii school.lan</li> </ul>	teacher	Копировать		Фамилия:			
> 🧾 Builtin	agreachers	Добавить в гру	/nny	Полное имя:	tumanov		
				Имя входа польз	ователя:		
Локальный лиск (С	·) > SRV > T	HOMES >		tumanov		@school.lan	~
Nokononi Anci (		^		Имя входа польз	ователя (пред-W	/indows 2000):	
* ^	Имя	10000		SCHOOL		tumanov	
*	teacher						
*	tumanov					< Назад Дал	ее > Отмена