

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Вятский государственный университет»
(ФГБОУ ВПО «ВятГУ»)
Факультет автоматики и вычислительной техники
Кафедра электронных вычислительных машин

УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ
Лабораторная работа №6 по дисциплине
«Сети ЭВМ и телекоммуникации»

Киров 2022

Цель работы: получить навыки по созданию и управлению учетными записями в домене Windows Server 2012.

Теоретические сведения:

Содержание учетной записи

Учётная запись - запись, содержащая сведения, которые пользователь сообщает о себе некоторой компьютерной системе. Как синонимы в обиходе могут использоваться учётка, аккаунт и эккаунт, от англ. Account — учётная запись, личный счёт.

Учётная запись, как правило, содержит сведения, необходимые для идентификации пользователя при подключении к системе, информацию для авторизации и учёта. Это имя пользователя (логин) и пароль. Пароль или его аналог, как правило, хранится в зашифрованном или хэшированном виде для обеспечения его безопасности.

Для аутентификации могут использоваться аппаратные средства (вырабатывающие одноразовые ключи, считывающие биометрические характеристики и т. п.), а также одноразовые пароли.

Учётная запись может содержать также дополнительные анкетные данные о пользователе - имя, фамилию, отчество, псевдоним, дату рождения, адрес email, домашний адрес, рабочий адрес, нетмейловый адрес, номер домашнего телефона, номер рабочего телефона, номер сотового телефона, адрес домашней страницы и/или блога в Паутине или интранете, о культурных предпочтениях и так далее. Учётная запись может также содержать одну или несколько фотографий пользователя.

Учётная запись пользователя также может учитывать различные статистические характеристики поведения пользователя в системе: давность последнего входа в систему, продолжительность последнего пребывания в системе, адрес использованного при подключении компьютера, интенсивность использования системы, суммарное и (или) удельное количество определённых операций, произведённых в системе, и так далее.

Ход работы:

Создание нового пользователя

Для создания доменной учетной записи в Windows Server 2012 необходимо выполнить следующую последовательность действий:

1. Открыть оснастку «Active Directory – пользователи и компьютеры» («Пуск» -> «Средства администрирования» -> «Пользователи и компьютеры Active Directory») (рисунок 1);

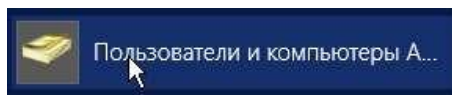


Рисунок 1 – Запуск оснастки «Active Directory – пользователи и компьютеры»

2. В дереве консоли щелкнуть правой кнопкой мыши папку, в которую нужно добавить учетную запись пользователя (например, в папку «Users» в домене); в появившемся контекстном меню выделить пункт «Создать» и щелкнуть «Пользователь» (рисунок 2);

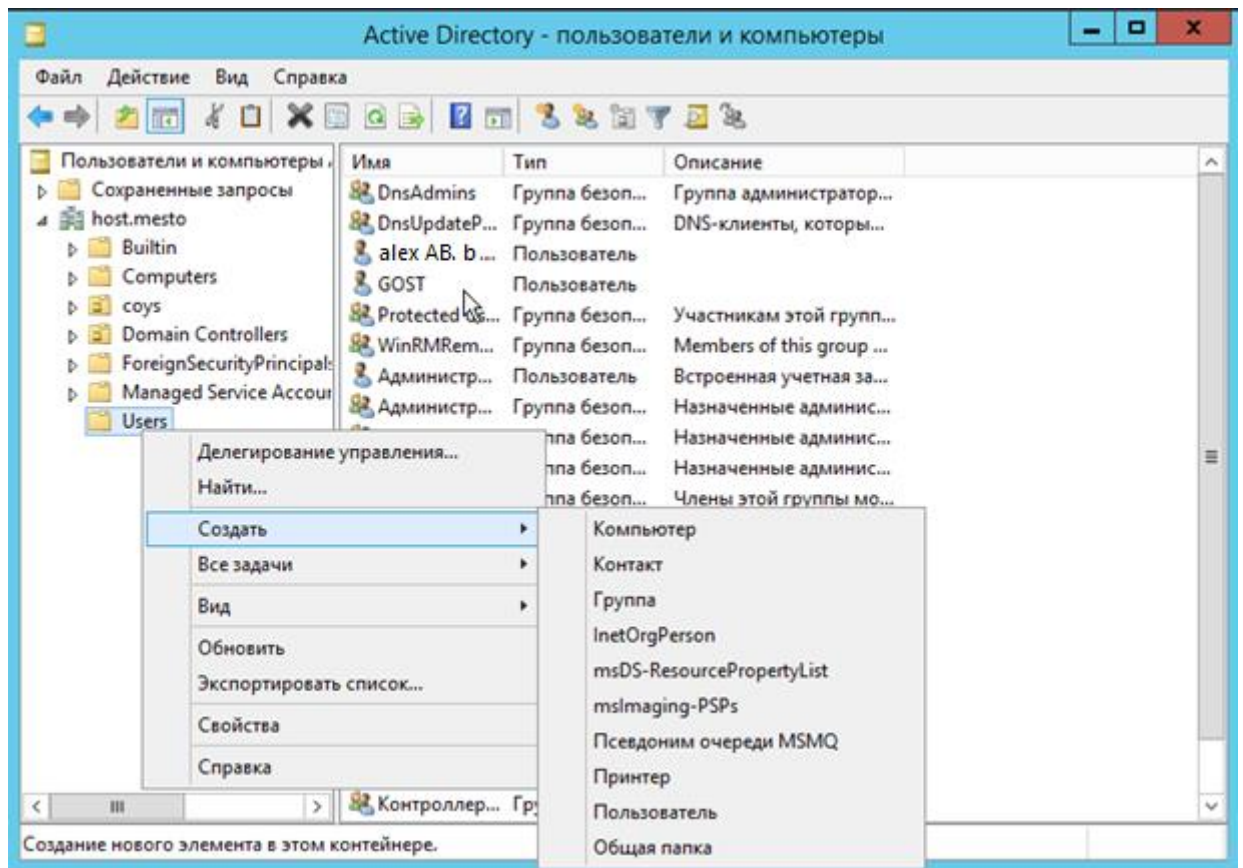


Рисунок 2 – Дерево консоли оснастки «Active Directory – пользователи и компьютеры»

3. В появившемся окне «Новый объект - пользователь» заполнить поля: в полях «Имя», «Инициалы», «Фамилия» ввести соответственно имя, инициалы и фамилию пользователя (при необходимости можно изменить поле «Полное имя», например, добавить инициалы или поменять имя и фамилию местами) (рисунок 3).

Новый объект - Пользователь

Создать в: host.mesto/Users

Имя: US1 Инициалы: US

Фамилия: US1

Полное имя: US1 US. US1

Имя входа пользователя: US @host.mesto

Имя входа пользователя (пред-Windows 2000): HOST0\ US

< Назад Далее > Отмена

Рисунок 2 – Окно «Новый объект - пользователь»

4. В полях «Пароль» и «Подтверждение» ввести пароль пользователя, а затем выбрать подходящие параметры пароля (рисунок 4). После этого нажать кнопку «Далее».

Новый объект - Пользователь

Создать в: host.mesto/Users

Пароль: [masked]

Подтверждение: [masked]

☐ Требовать смены пароля при следующем входе в систему

☐ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

< Назад Далее > Отмена

Рисунок 4 – Окно «Новый объект - пользователь»

5. В окне подтверждения создания нового пользователя нажать на кнопку «Готово» (рисунок 5).

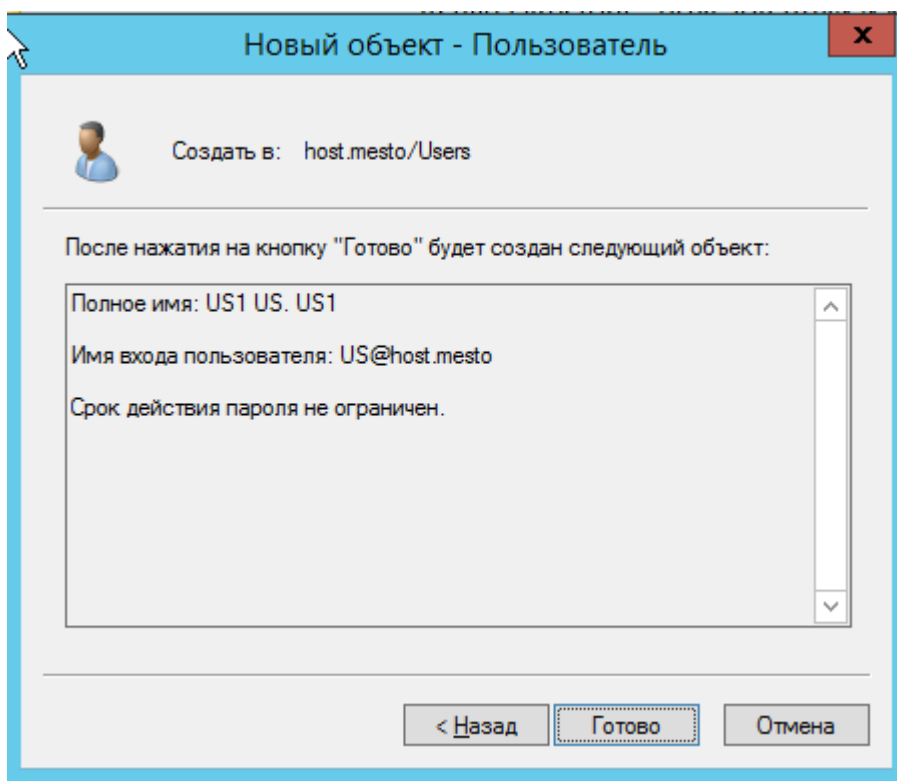


Рисунок 5 – Окно «Новый объект - пользователь»

После выполнения вышеприведенных действий в таблице объектов появится только что созданный пользователь (рисунок 6).

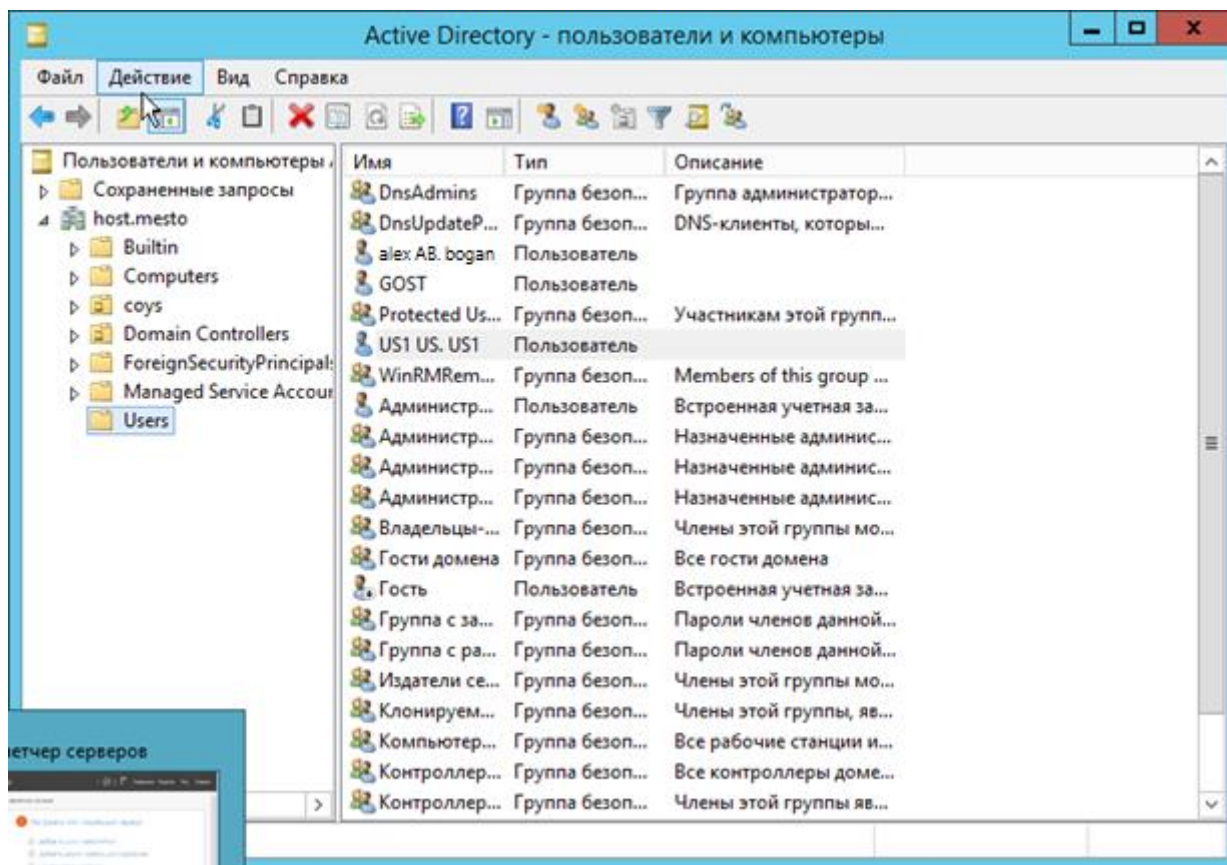


Рисунок 6 – Окно оснастки «Active Directory – пользователи и компьютеры»

Для выполнения процедуры добавления доменной учетной записи пользователя необходимо быть членом группы "Операторы учета", "Администраторы домена" или "Администраторы предприятия" в доменных службах Active Directory, либо получить соответствующие полномочия путем делегирования. По соображениям безопасности для выполнения этой процедуры рекомендуется использовать команду «Запуск от имени».

Новая учетная запись пользователя с таким же именем, как и у ранее удаленной учетной записи пользователя, не приобретает автоматически разрешения и членства ранее удаленной учетной записи, потому что идентификатор безопасности (SID) каждой учетной записи уникален. Если требуется воспроизвести удаленную учетную запись пользователя, необходимо вручную заново создать все разрешения и членства.

При создании учетной записи пользователя атрибут «Полное имя» создается в формате ИмяФамилия по умолчанию. Атрибут «Полное имя» также управляет форматом выводимого имени, которое отображается в глобальном списке адресов. Формат выводимого имени можно изменить с помощью средства "Редактирование ADSI". Если изменить формат выводимого имени, формат полного имени тоже изменится.

Открыть «Модуль Active Directory для Windows PowerShell» можно через «Диспетчер серверов» (рисунок 7).

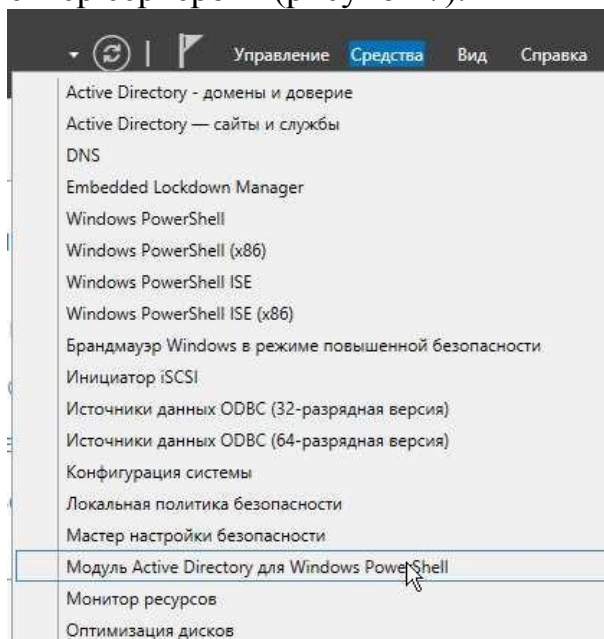


Рисунок 7 – Запуск модуля Active Directory для Windows PowerShell через «Диспетчер серверов»

Создание учетной записи пользователя с помощью командной строки

Для создания учетной записи пользователя с помощью командной строки необходимо выполнить следующую последовательность действий:

1. Открыть командную строку
2. Ввести команду, представленную на рисунке 8, и нажать клавишу ВВОД.

Для просмотра полного синтаксиса данной команды, а также сведений о вводе в командную строку информации учетной записи пользователя необходимо ввести команд `dsadd user /?`, а затем нажать клавишу ВВОД.

Для выполнения процедуры добавления учетной записи пользователя с помощью командной строки необходимо быть членом группы "Операторы учета", "Администраторы домена" или "Администраторы предприятия" в доменных службах Active Directory, либо получить соответствующие полномочия путем делегирования. По соображениям безопасности для выполнения этой процедуры рекомендуется использовать команду «Запуск от имени».

Новая учетная запись пользователя с таким же именем, как и у ранее удаленной учетной записи пользователя, не приобретает автоматически разрешения и членства ранее удаленной учетной записи, потому что идентификатор безопасности (SID) каждой учетной записи уникален. Если требуется воспроизвести удаленную учетную запись

пользователя, необходимо вручную заново создать все разрешения и членства.

Результат выполнения команды представлен на рисунке 9.

<pre>dsadd user <UserDN> [-samid <SAMName>] -pwd {<Password> *}</pre>	
Параметр	Описание
<UserDN>	Задаёт различающееся имя добавляемого объекта пользователя.
-samid	Устанавливает значение <SAMName>.
<SAMName>	Задаёт имя диспетчера учетных записей безопасности (SAM) как уникальное имя учетной записи SAM для данного пользователя (например, Linda). Если имя SAM не указано, «dsadd» попытается создать имя учетной записи SAM, используя до 20 первых символов обычного имени (CN) UserDN.
-pwd	Устанавливает значение пароля.
<Password>	Задаёт пароль для использования в учетной записи пользователя. Если для этого параметра установлено значение *, выводится запрос на ввод пароля.

Рисунок 8 – Команда создания учетной записи пользователя и ее описание

```
C:\Users\Администратор>dsadd user "CN=UserCMD, CN=Users, DC=datainfo, DC=datainfo" -pwd *
Ввод пароля пользователя:
Подтверждение пароля:
```

Рисунок 9 – Результат выполнения команды создания учетной записи пользователя в командной строке

Создание перемещаемых профилей

При первом создании перемещаемых профилей необходимо выполнить все действия, описанные ниже (создание группы безопасности, общей папки, GPO для перемещаемых профилей пользователей, настройка перемещаемых профилей в учетных записях пользователей и на компьютерах, включение GPO перемещаемых профилей пользователей).

Создание группы безопасности перемещаемых профилей пользователей

Первым шагом при создании перемещаемых профилей пользователей является создание их группы безопасности. Для этого необходимо выполнить следующую последовательность действий:

1. Открыть диспетчер серверов («Пуск» → «Диспетчер серверов»)
2. В меню «Средства» выбрать «Центр администрирования Active Directory» (рисунок 10);

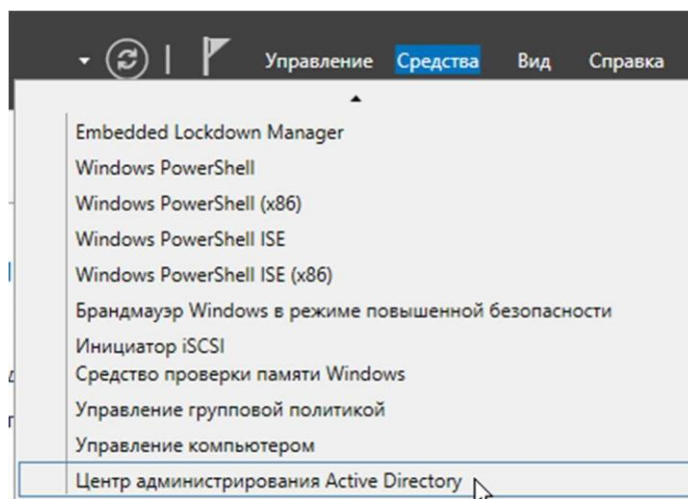


Рисунок 10 – Запуск средства «Центр администрирования Active Directory» через «Диспетчер серверов»

3. В открывшемся окне «Центр администрирования Active Directory» щелкнуть правой кнопкой мыши по необходимому домену или подразделению, нажать «Создать» и выбрать «Группа» (рисунок 11);

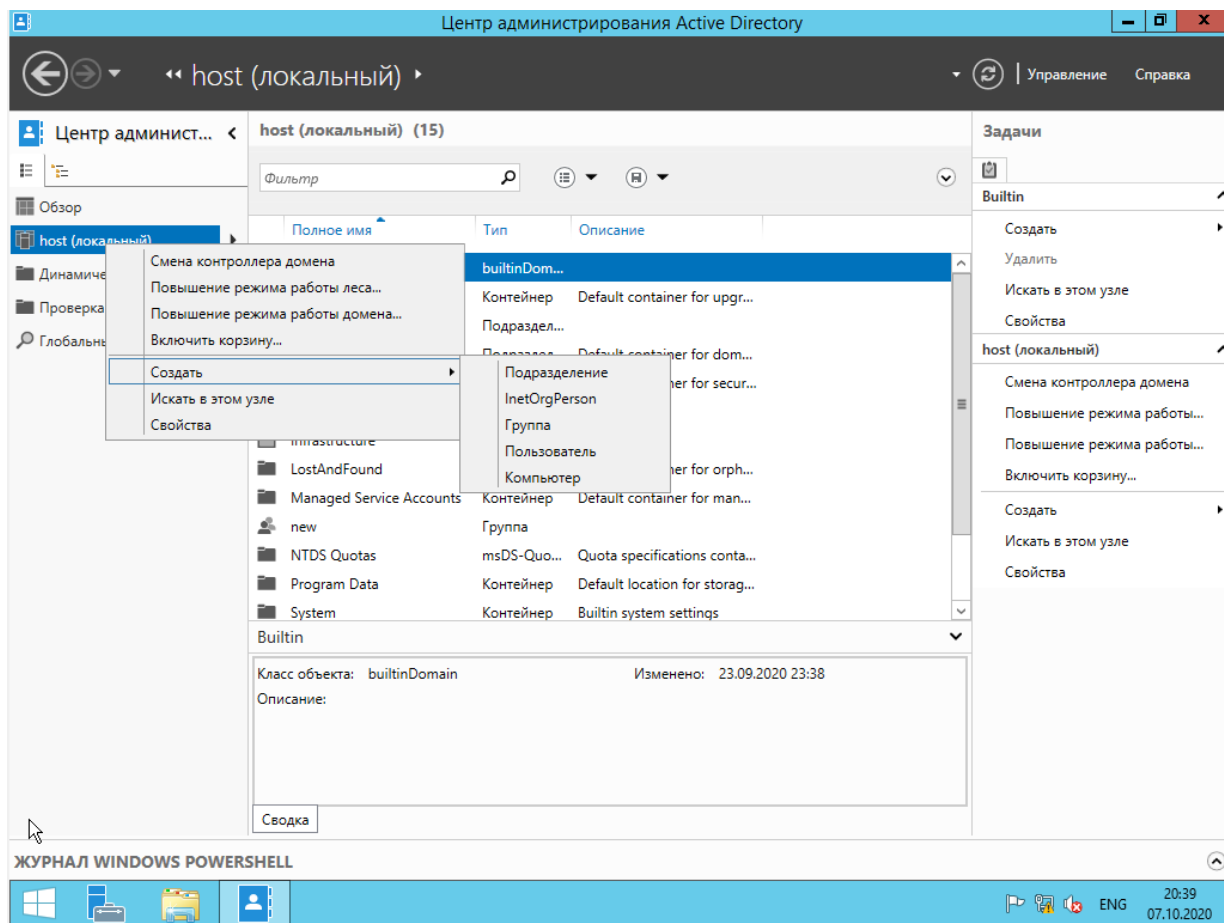


Рисунок 11 – Открытие окна создания группы для выбранного домена

4. В окне создания группы в разделе «Группа» необходимо ввести в поле «Имя группы» имя группы безопасности (например, «Пользователи перемещаемых профилей и компьютеры») и в разделах «Тип группы» и «Область группы» выбрать соответственно «Безопасность» и «Глобальная» (рисунок 12);

Создать Группа: Пользователи перемещаю... ЗАДАЧИ РАЗДЕЛЫ

Группа

Управляется

Членство

Члены группы

Параметры паролей

Группа

Имя группы: *

Имя группы (... *

Эл. почта:

Создать в: DC=host,DC=mesto

Изменить...

Тип группы: ☒ Безопасность ☐ Распространение

Область группы: ☐ Локальная в домен ☒ Глобальная ☐ Универсальная

☐ Защита от случайного удаления

Описание:

Заметки:

Управляется

Управляется:

☐ Менеджер может изменять членов груп...

Телефоны:

Основной:

Мобильный:

Факс:

Комната:

Адрес:

Город: Область, к...: Почтовый...:

Страна или регион:

Член групп

Дополнительные св...

ОК Отмена

Рисунок 12 – Создание группы безопасности

5. В разделе «Члены группы» нажать кнопку «Добавить»;
6. Если требуется включить в группу безопасности учетные записи компьютеров, то необходимо щелкнуть «Типы объектов», установить флажок рядом с пунктом «Компьютеры», после чего нажать «ОК» (рисунок 13).

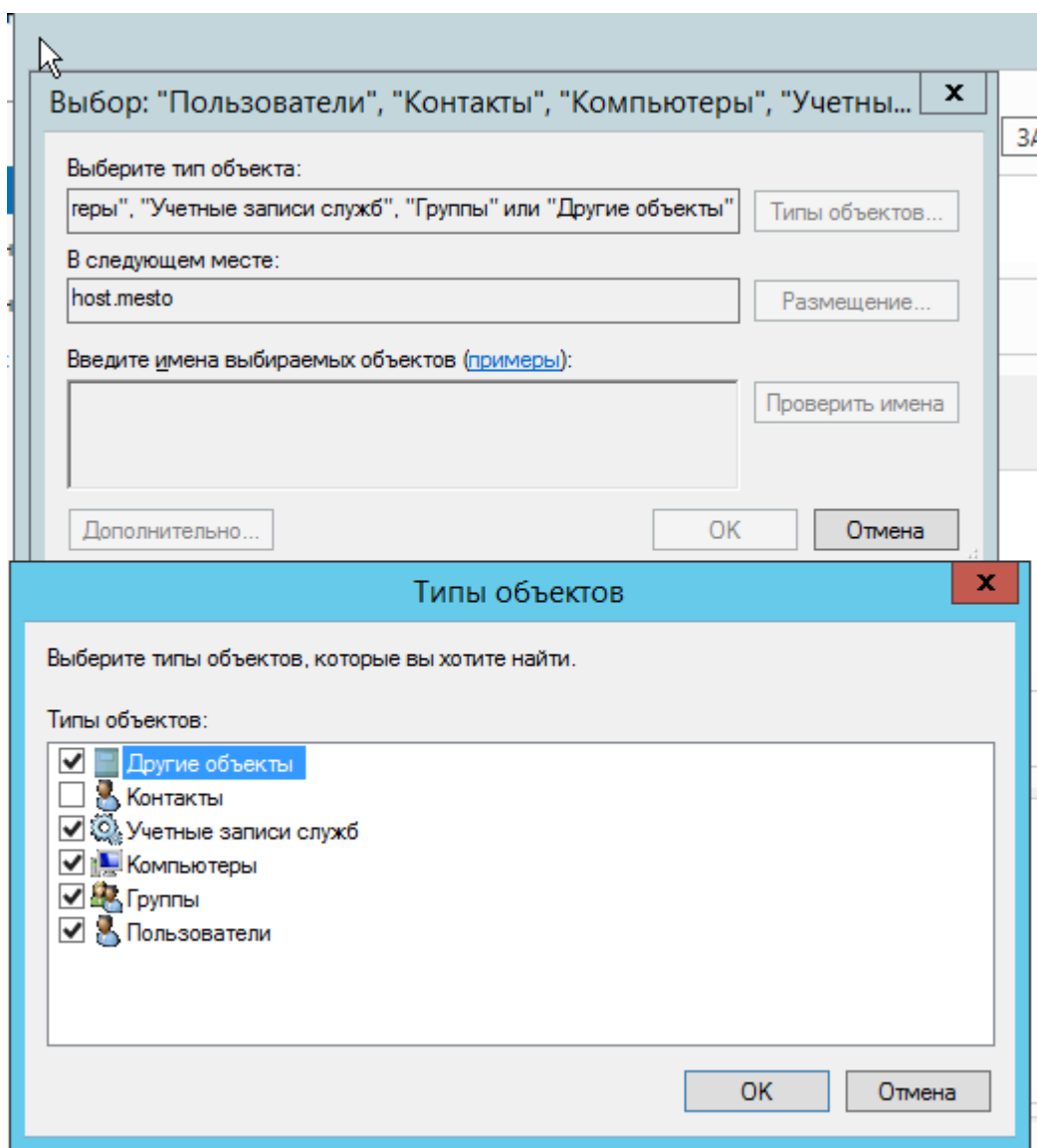


Рисунок 13 – Создание группы безопасности

7. Далее необходимо указать имена пользователей, групп и/или компьютеров, для которых требуется выполнить развертывание перемещаемых профилей пользователей. Для этого необходимо нажать на кнопку «Дополнительно», в окне выбора нажать «Поиск», выбрать нужный элемент из списка и кликнуть «ОК» 2 раза (рисунок 14);

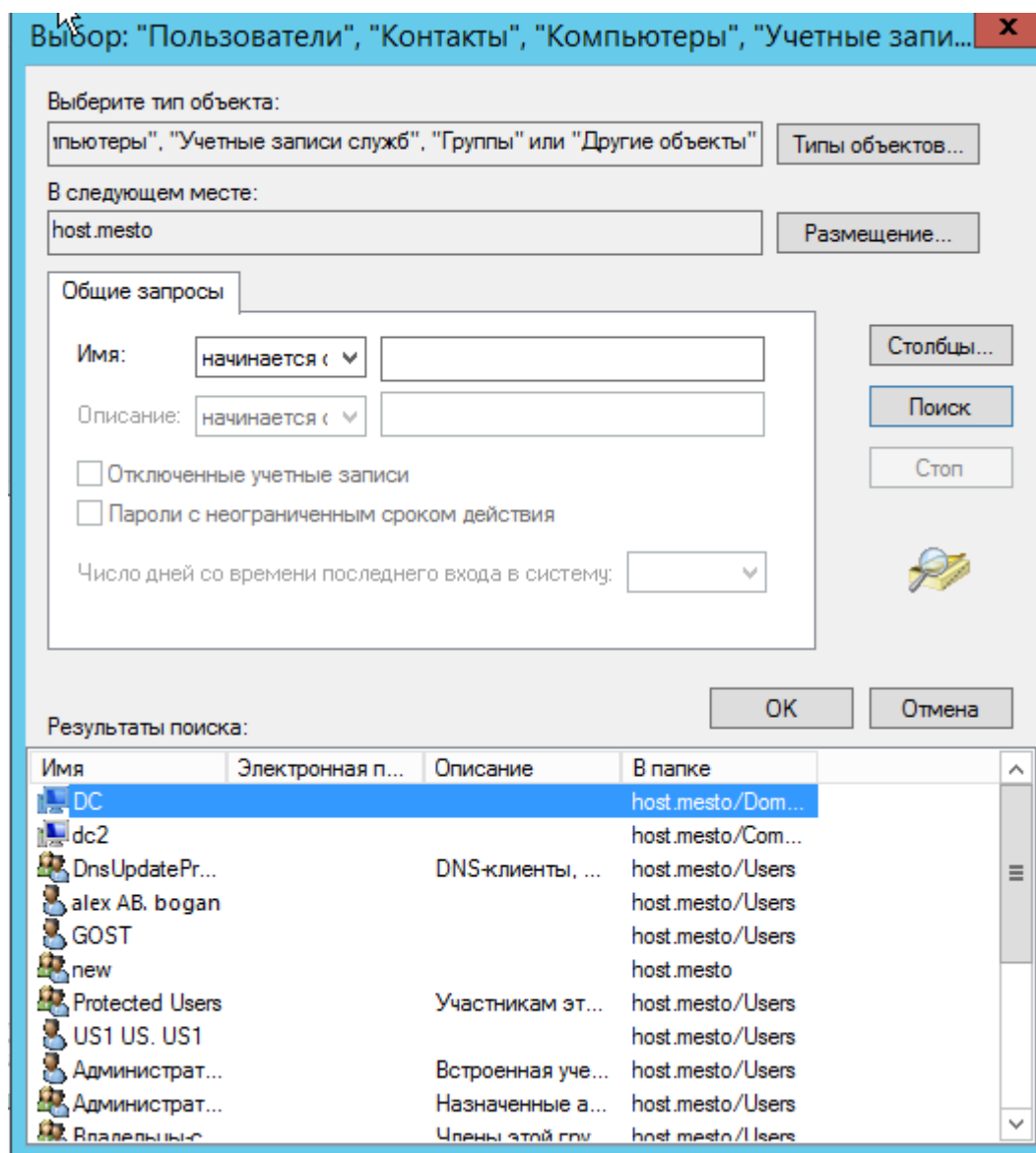


Рисунок 13 – Создание группы безопасности

8. После этого в окне создания группы необходимо нажать на «ОК» (рисунок 15).

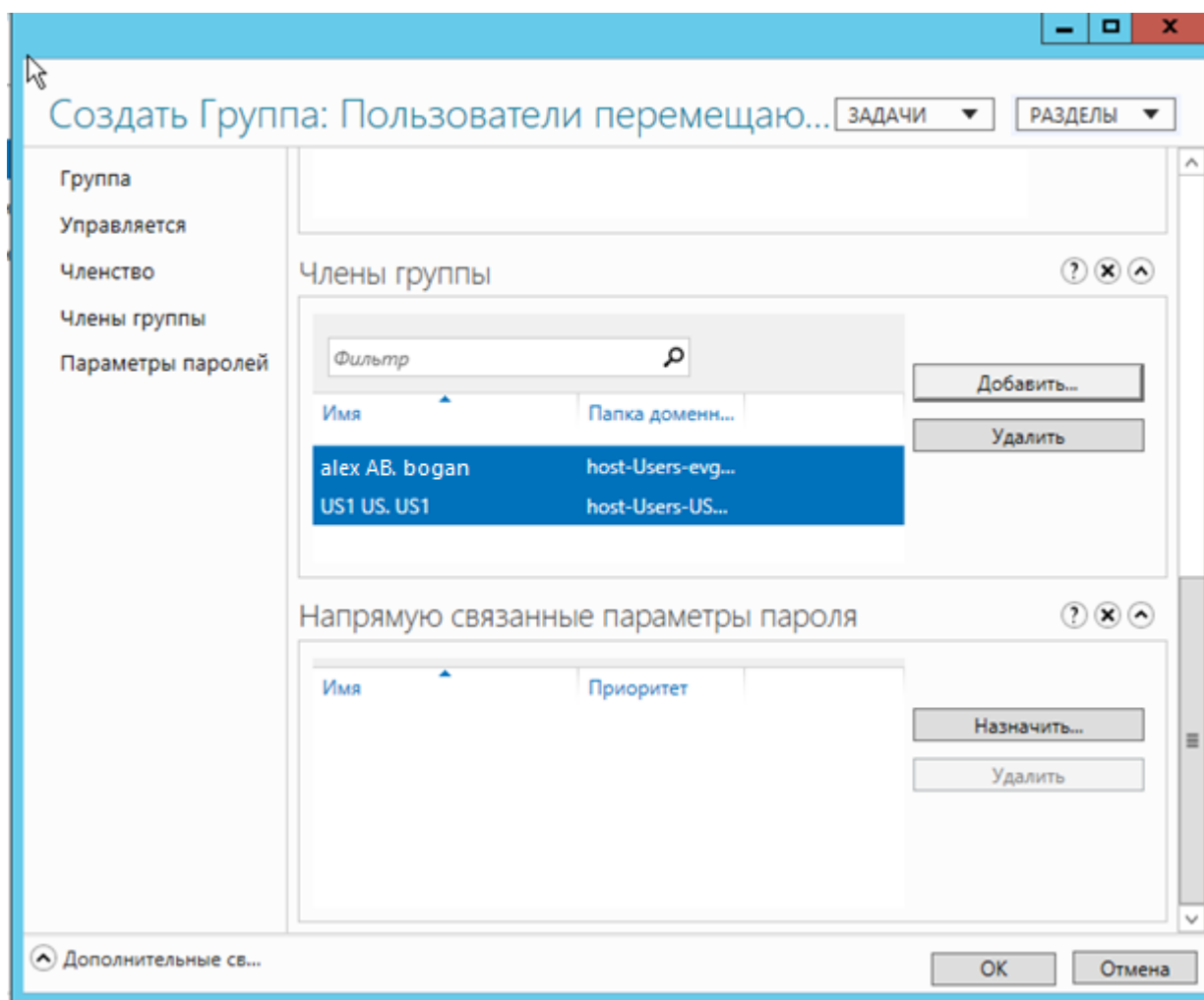


Рисунок 15 – Создание группы безопасности

Создание общей папки для перемещаемых профилей пользователей

Вторым шагом при создании перемещаемых профилей пользователей является создание для них общей папки. Для этого необходимо выполнить следующую последовательность действий:

1. В области навигации диспетчера сервера выбрать элемент «Файловые службы и службы хранилища», после чего нажать кнопку «Общие ресурсы», чтобы перейти на страницу общих ресурсов (рисунок 16);

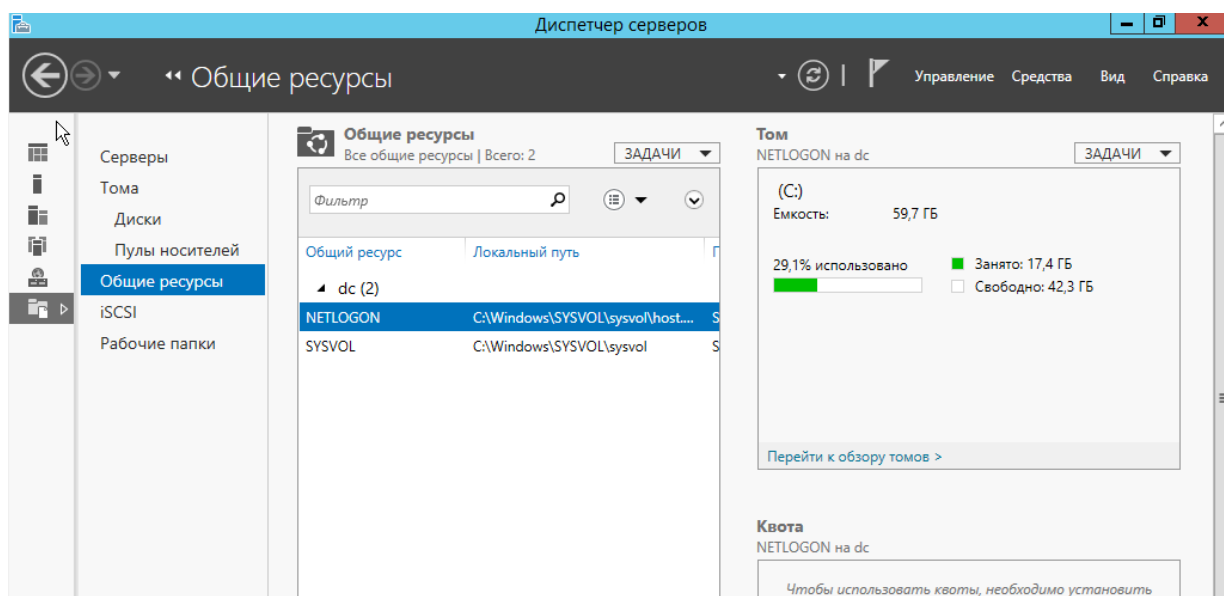


Рисунок 16 – «Общие ресурсы»

2. На странице общих ресурсов выбрать «Задачи», а затем нажать на «Новый общий ресурс», после чего откроется мастер создания общих ресурсов (рисунок 17);

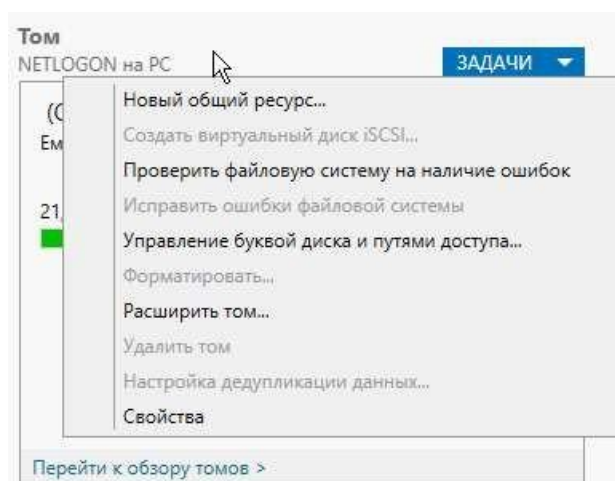


Рисунок 17 – Создание общей папки

3. На странице «Выбор профиля для общего ресурса» щелкнуть «Общий ресурс SMB — быстрый профиль». Если у вас установлен диспетчер ресурсов файлового сервера и вы используете свойства управления папками, вместо этого выберите пункт «Общий ресурс SMB — дополнительные» (рисунок 18);

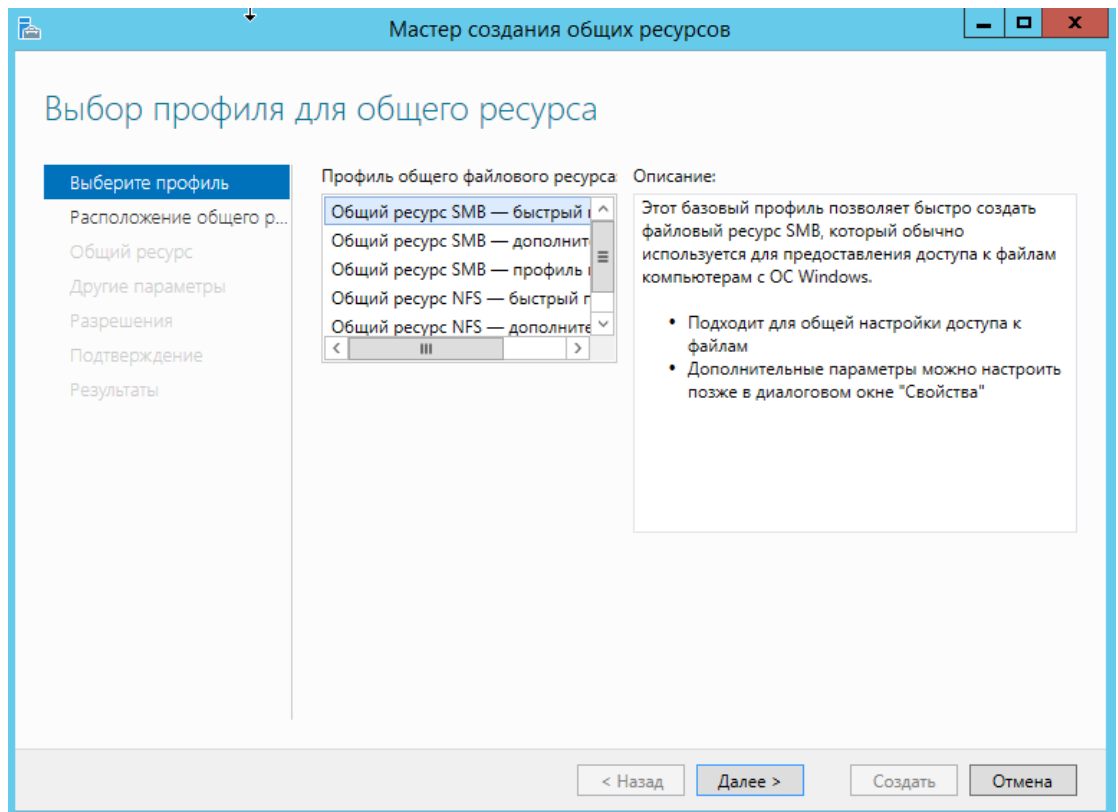


Рисунок 18 – Выбор профиля для общего ресурса

4. На странице «Расположение общего ресурса» выберите сервер и том, в котором хотите создать общий ресурс (рисунок 19);

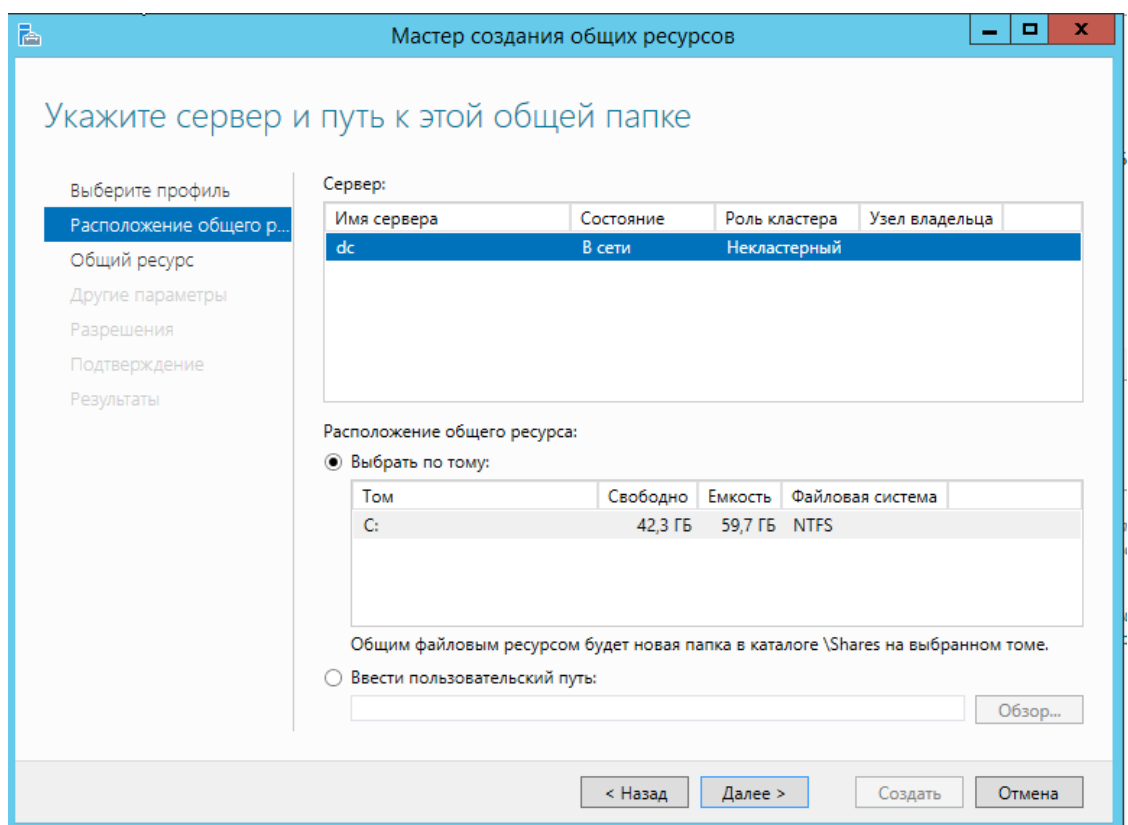


Рисунок 19 – Выбор сервера и задание пути к общей папке

5. На странице «Общий ресурс» необходимо указать имя (например, «User Profiles\$») в поле «Общий ресурс» (при создании общего ресурса необходимо скрыть его, добавив после имени символ \$ – это предотвратит доступ к нему случайных веб-обозревателей) (рисунок 20);

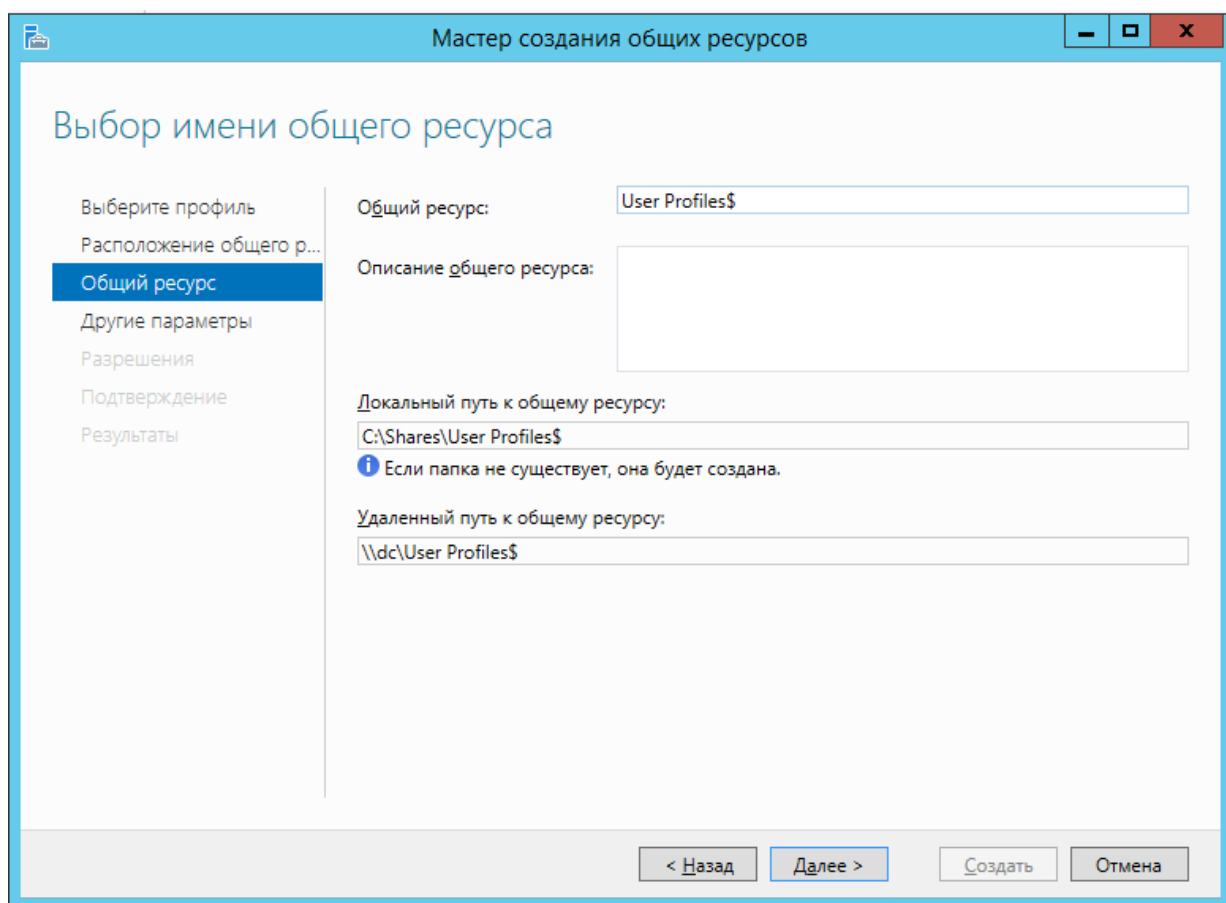


Рисунок 20 – Выбор имени общего ресурса

6. На странице «Другие параметры» снять флажок «Разрешить кэширование общего ресурса», если он показан, и при необходимости установить флажки «Включить перечисление на основе доступа» и «Зашифровать доступ к данным» (рисунок 21);

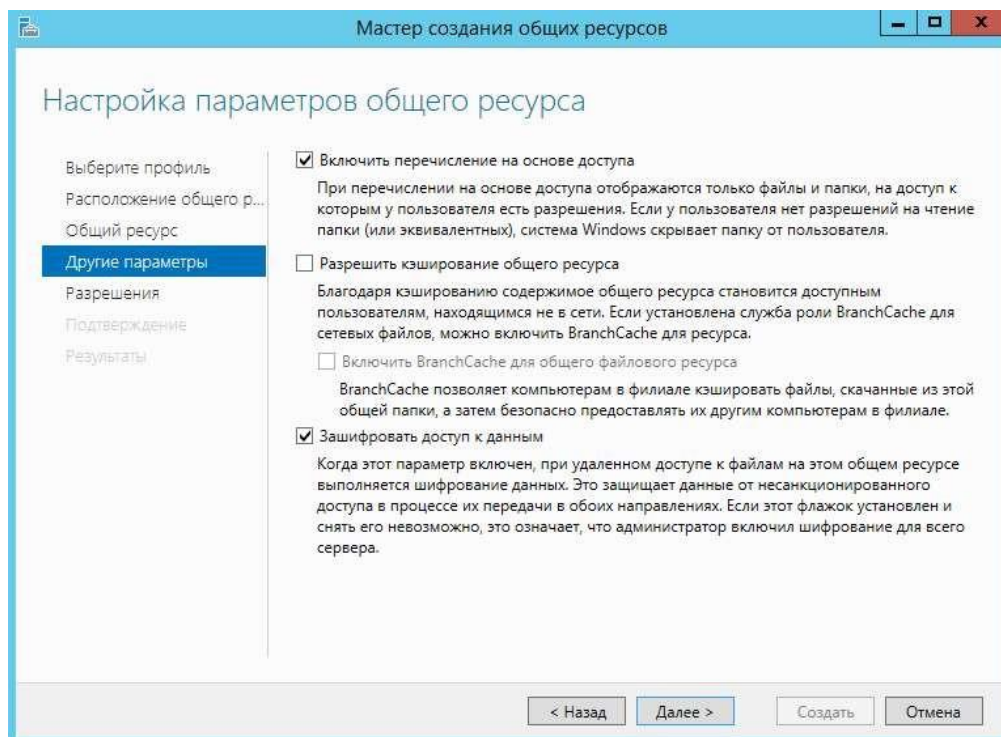


Рисунок 21 – Настройка параметров общего ресурса

7. На странице «Разрешения» щелкнуть «Настройка разрешений...», после чего отобразится диалоговое окно с расширенными параметрами безопасности (рисунок 22);

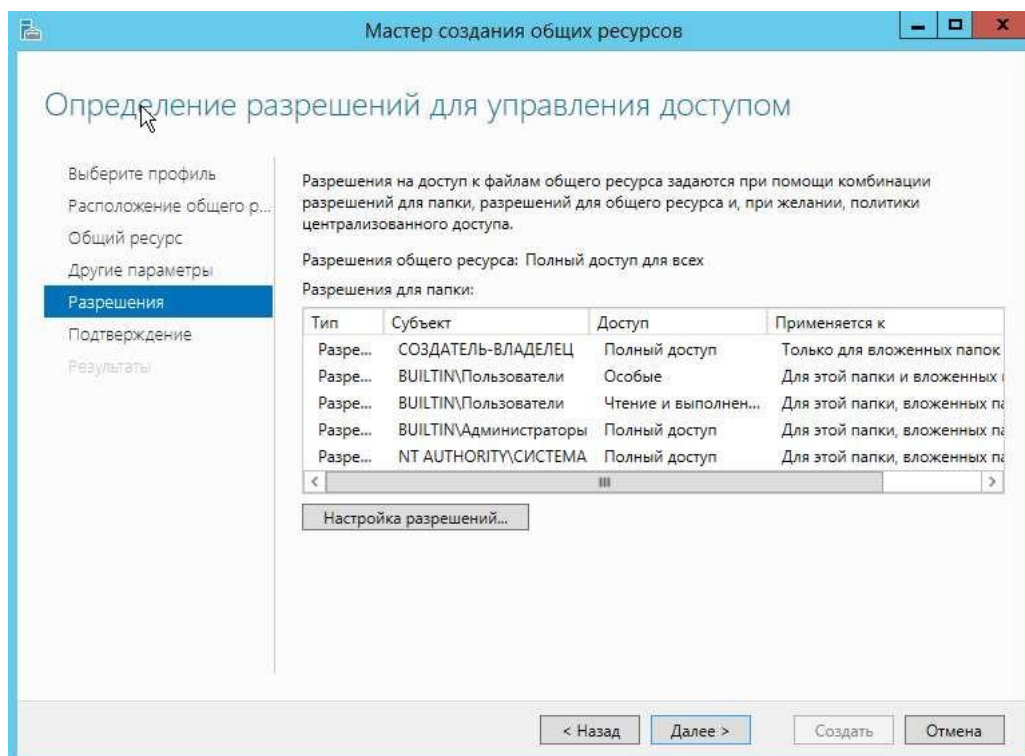


Рисунок 22 – Определение разрешений для управления доступом

8. Щелкнуть «Отключение наследования», после чего нажать на «Преобразовать унаследованные разрешения в явные разрешения этого объекта» (рисунок 23);

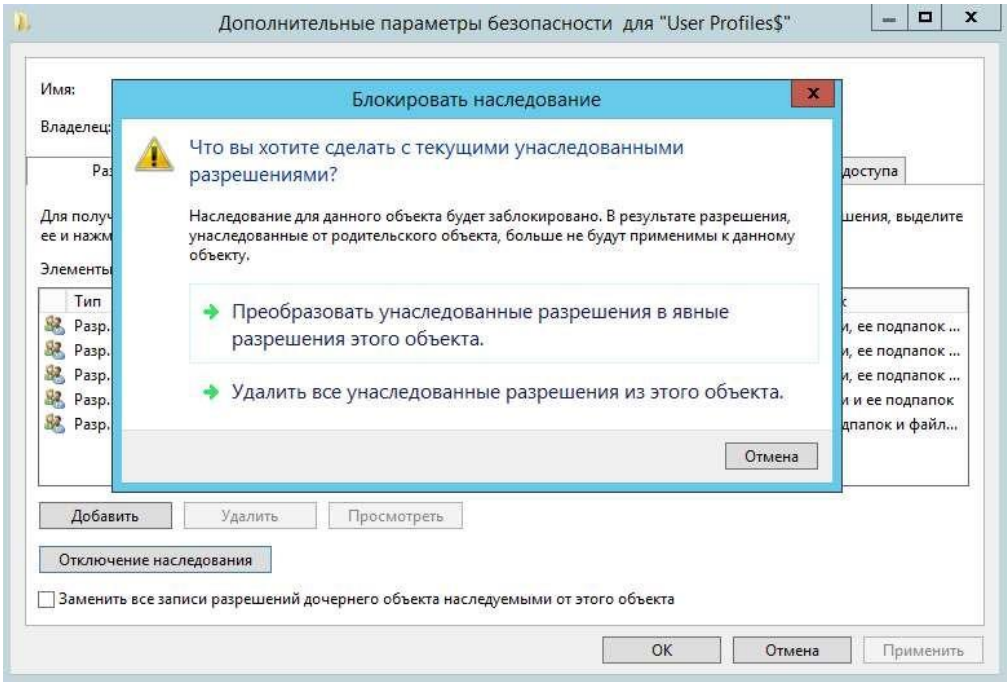


Рисунок 23 – Настройка наследования

9. Установить разрешения, как описано в таблице 1. Результат представлен на рисунке 24.

Таблица 1 – Описание разрешений для установки

Учетная запись пользователя	Доступ	Область применения
Система	Полный доступ	Данная папка, вложенные папки и файлы
Администраторы	Полный доступ	Только эта папка
Создатель/владелец	Полный доступ	Только вложенные папки и файлы
Группа безопасности пользователей, которым требуется обеспечить общий доступ к данным (пользователи перемещаемых профилей и компьютеры)	Содержание папки/чтение данных (дополнительные разрешения) Создание папок/дозапись данных дополнительные разрешения)	Только эта папка
Прочие группы и учетные записи	Нет (удаление)	Только эта папка

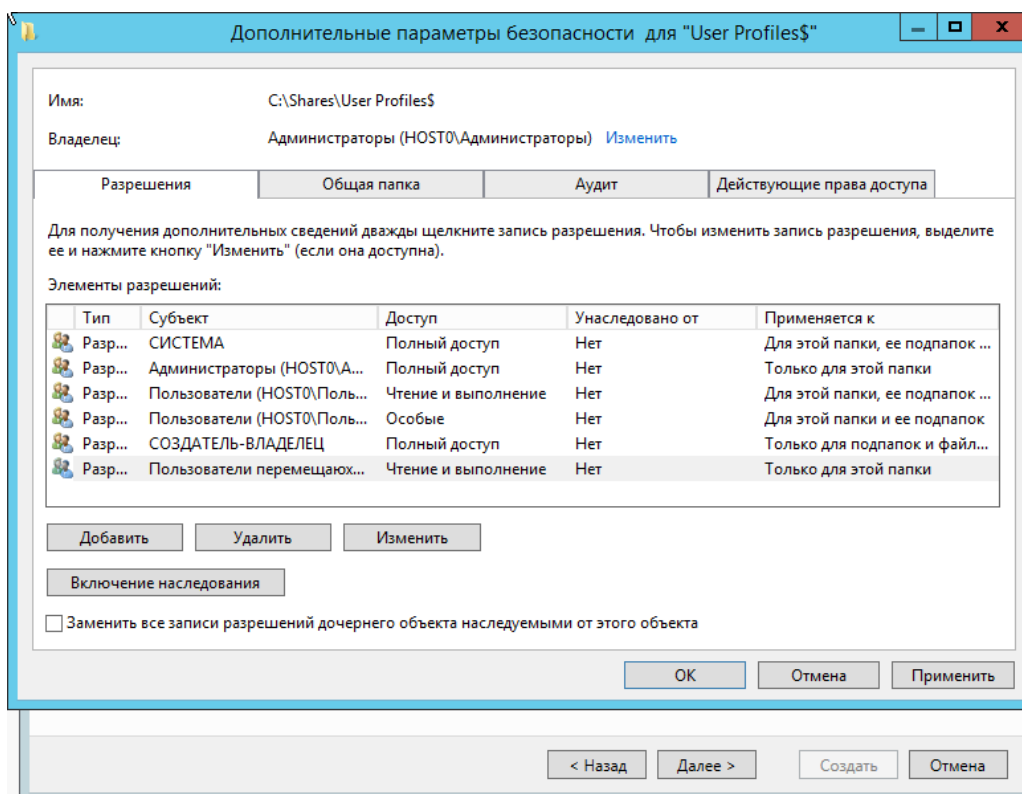


Рисунок 24 – Установка разрешений

10. На странице «Подтверждение» нажать кнопку «Создать» (рисунок 25).

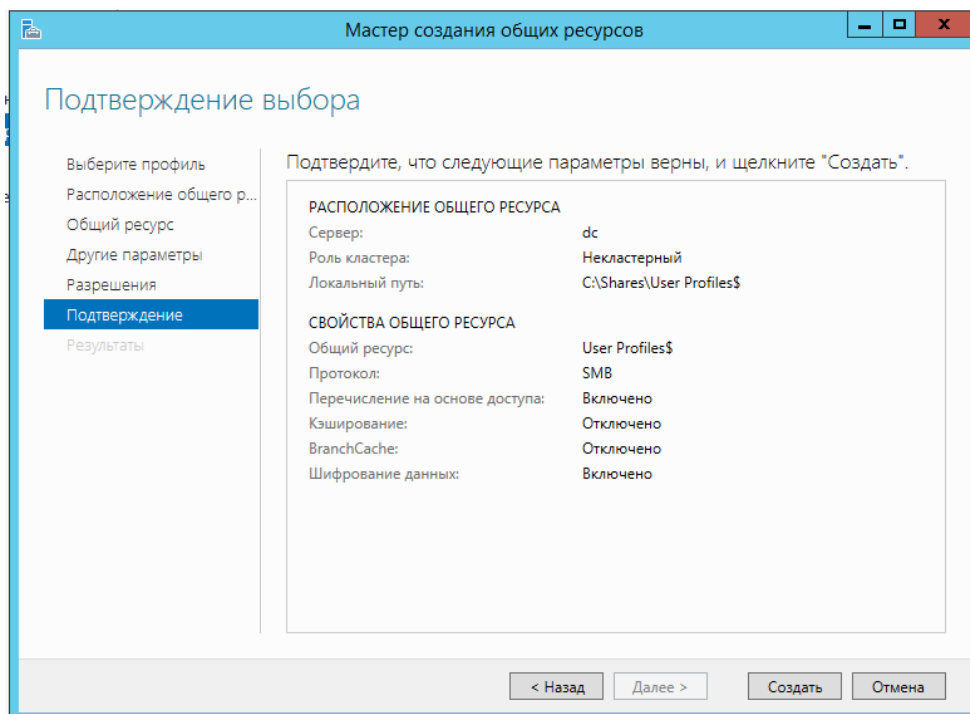


Рисунок 25 – Подтверждение выбора

11. На странице «Результаты» нажать кнопку «Заккрыть» (рисунок 26).

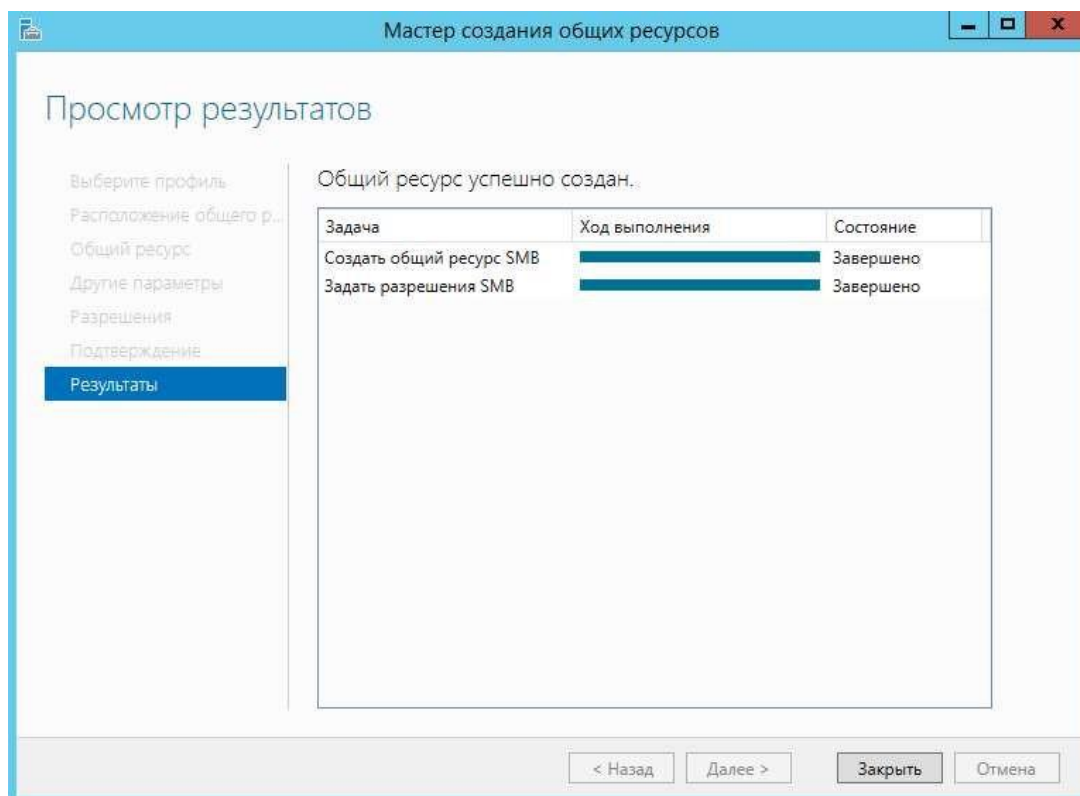


Рисунок 26 – Просмотр результатов

Создание GPO для перемещаемых профилей пользователей

Третьим шагом при создании перемещаемых профилей пользователей является создание для них GPO (объекта групповой политики). Для этого необходимо выполнить следующую последовательность действий:

1. Открыть диспетчер серверов («Пуск» → «Диспетчер серверов»);
2. В меню «Средства» выбрать «Управление групповой политикой», после чего появится окно управления групповыми политиками (рисунок 27);

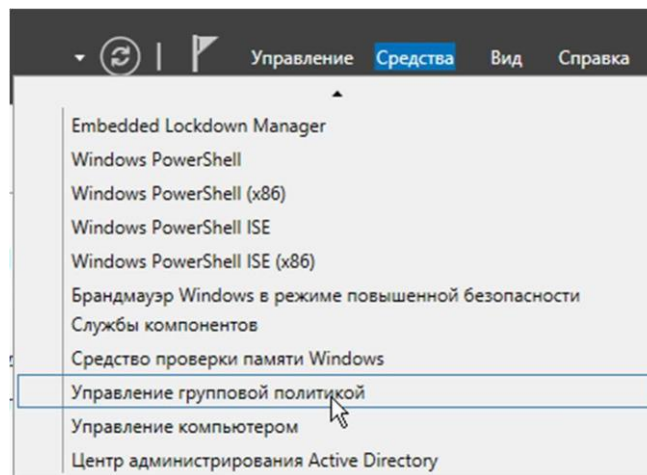


Рисунок 27 – Создание GPO

3. Правой кнопкой мыши щелкнуть по домену или организационному подразделению, в котором требуется настроить перемещаемые профили пользователей, после чего нажать «Создать объект групповой политики в этом домене и связать его» (рисунок 28);

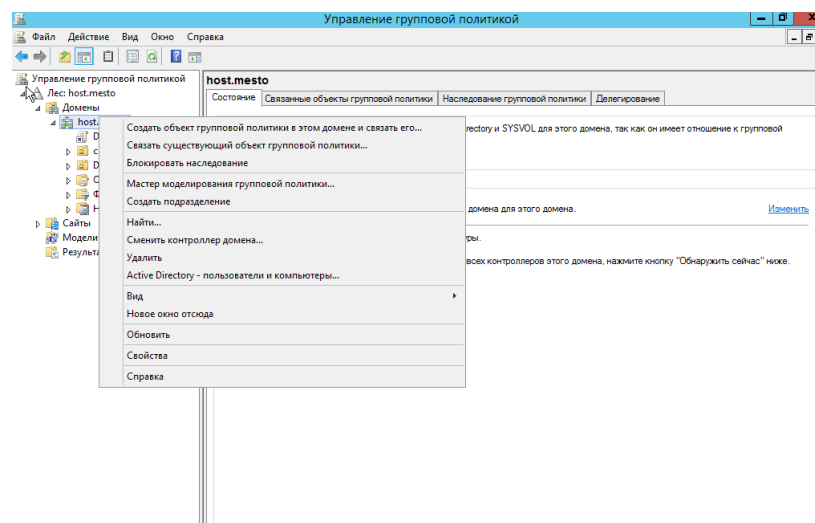


Рисунок 28 – Создание объекта групповой политики

4. В диалоговом окне «Новый объект групповой политики» указать имя GPO (например, «Настройки перемещаемого профиля пользователя») и щелкнуть «ОК» (рисунок 29);

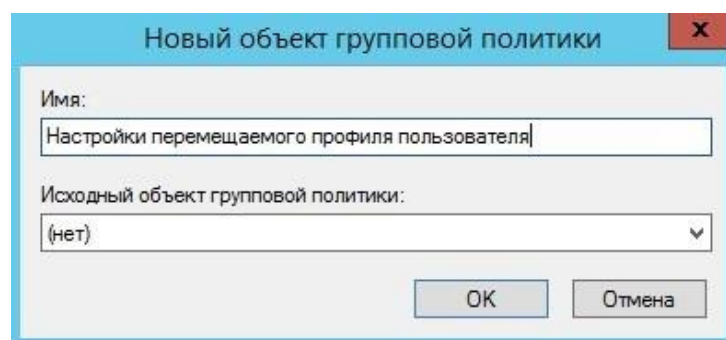


Рисунок 29 – Задание имени нового объекта групповой политики

5. Щелкнуть правой кнопкой мыши по новому объекту групповой политики и снять флажок «Связь включена» – это исключит применение GPO до завершения его настройки (рисунок 30);

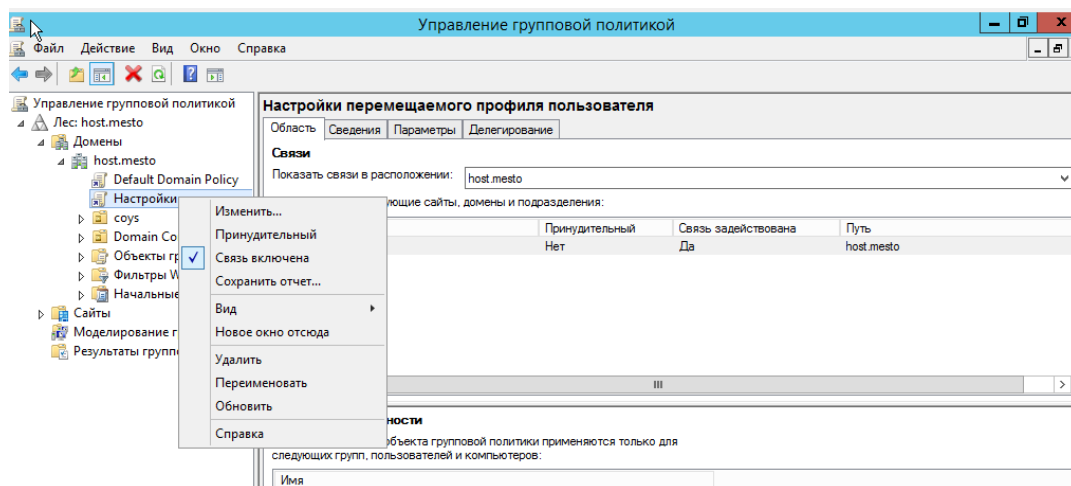


Рисунок 30 – Отключение связи

6. Выбрать GPO, на вкладке «Область» в разделе «Фильтры безопасности» выбрать пункт «Прошедшие проверку» и щелкнуть «Удалить» (рисунок 31);

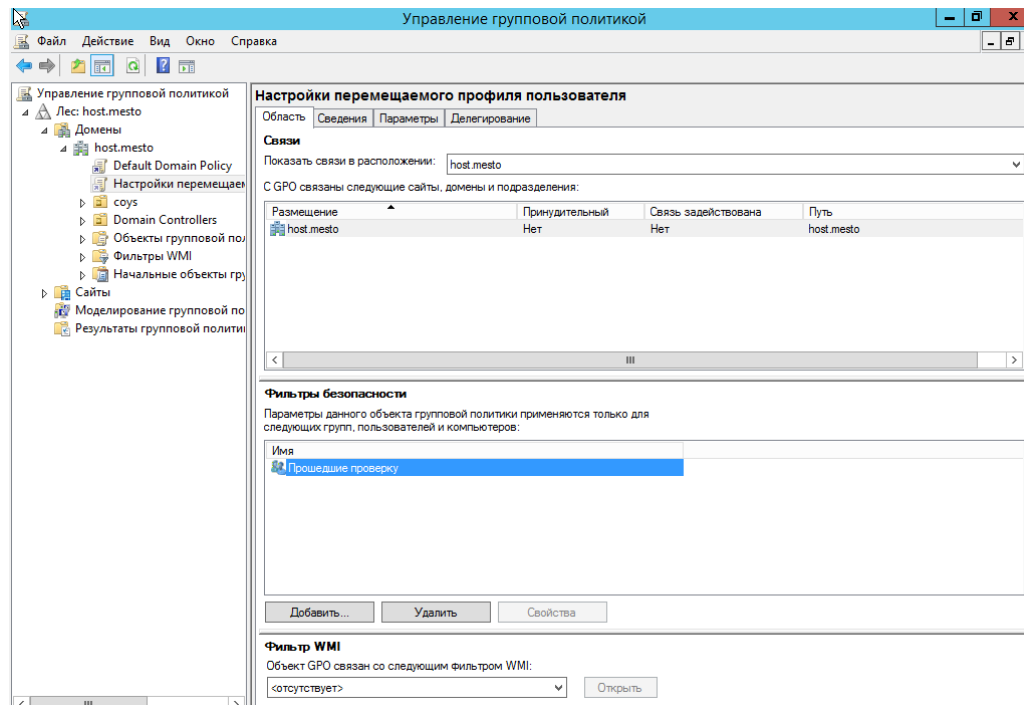


Рисунок 31 – Удаление GPO

7. В разделе «Фильтры безопасности» щелкнуть кнопку «Добавить» (рисунок 32);

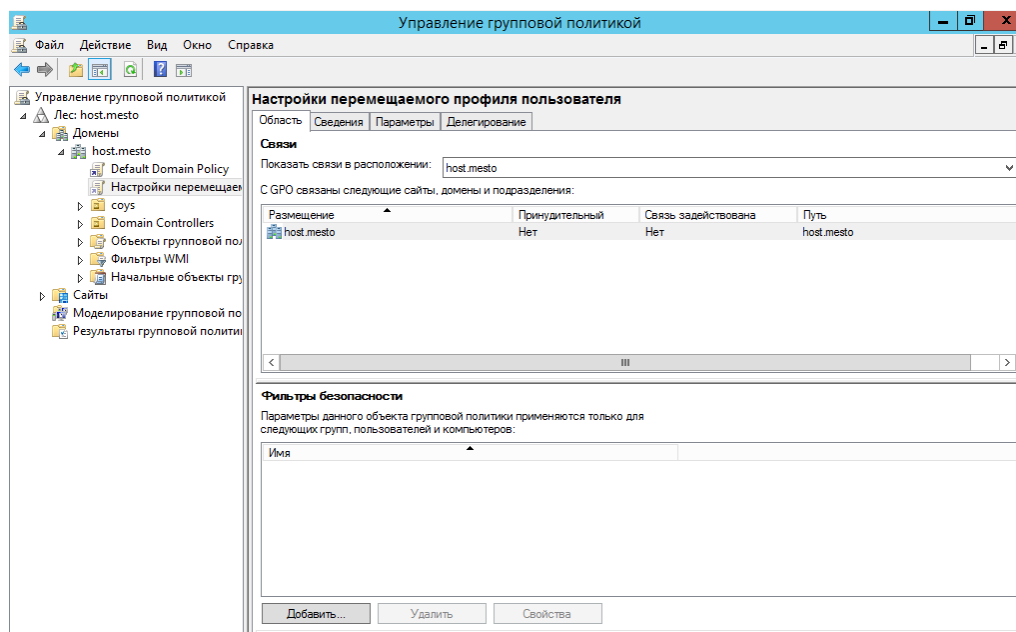


Рисунок 32 – Создание GPO

8. В появившемся диалоговом окне указать имя группы безопасности, которая была создана при создании группы безопасности (например, «Пользователи перемещаемых профилей и компьютеры»). Для этого необходимо нажать на кнопку «Дополнительно», в окне выбора нажать «Поиск», выбрать нужный элемент из списка и кликнуть «ОК» 2 раза (рисунок 33);

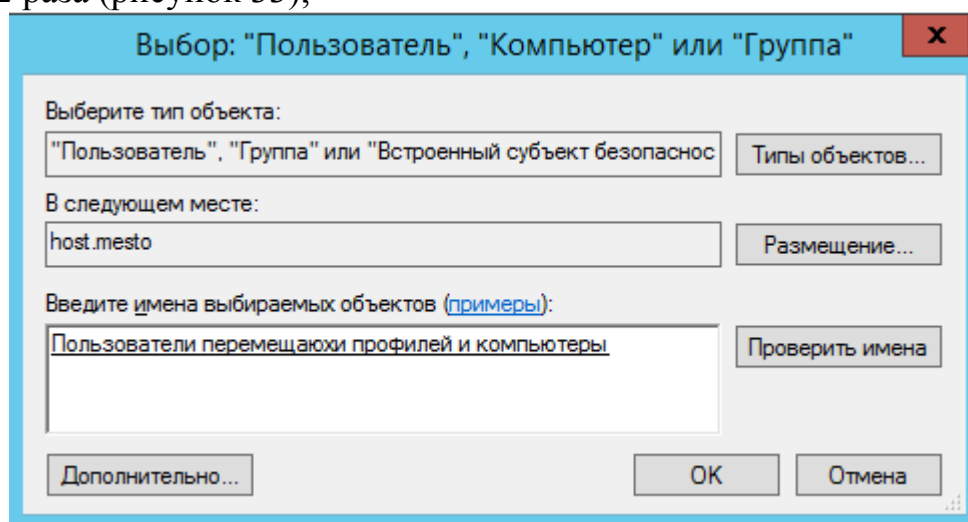


Рисунок 33 – Указание имени группы безопасности

Настройка перемещаемых профилей в учетных записях пользователей

Четвертым шагом при создании перемещаемых профилей пользователей является их настройка в учетных записях пользователей. Для этого необходимо выполнить следующую последовательность действий:

1. Открыть диспетчер серверов («Пуск» → «Диспетчер серверов»);
2. В меню «Средства» выбрать «Центр администрирования Active Directory» (рисунок 34);

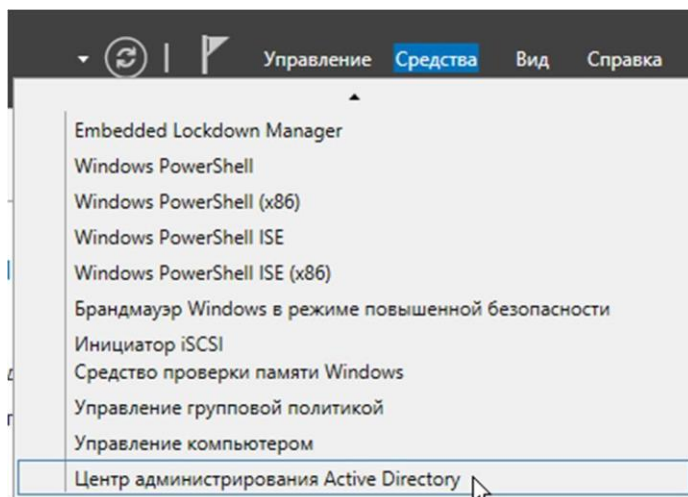


Рисунок 34 – Запуск средства «Центр администрирования Active Directory» через «Диспетчер серверов»

3. В открывшемся окне «Центр администрирования Active Directory» перейти в контейнер «Пользователи» (или в контейнер подразделений) в соответствующем домене (рисунки 35 и 36);

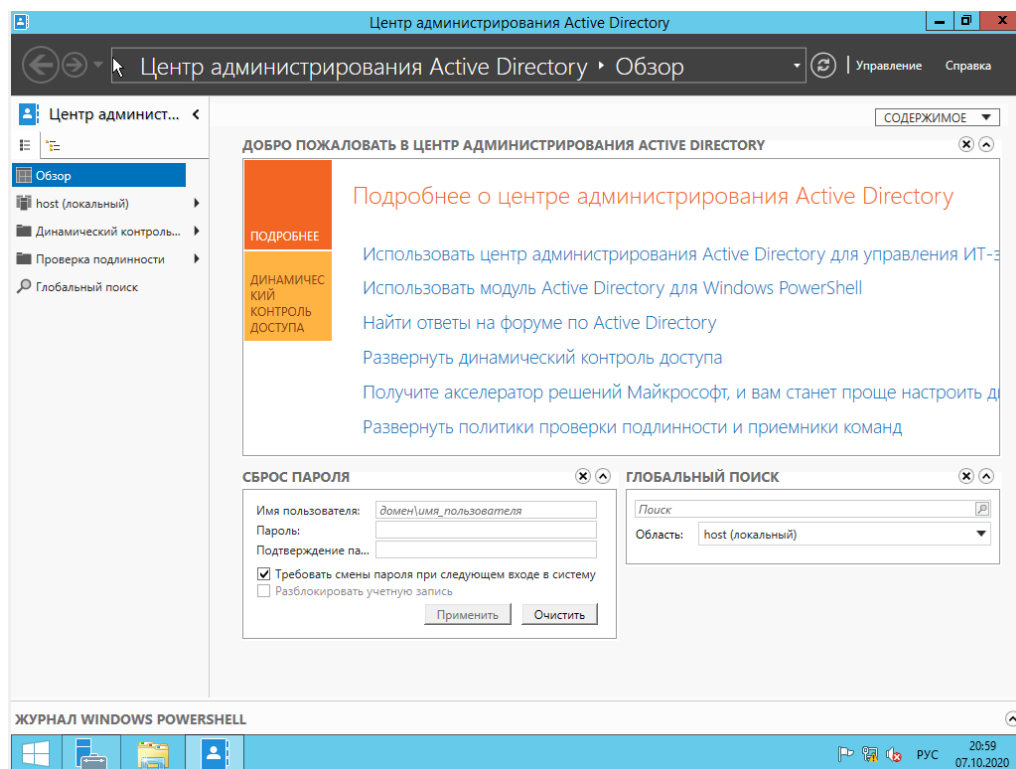
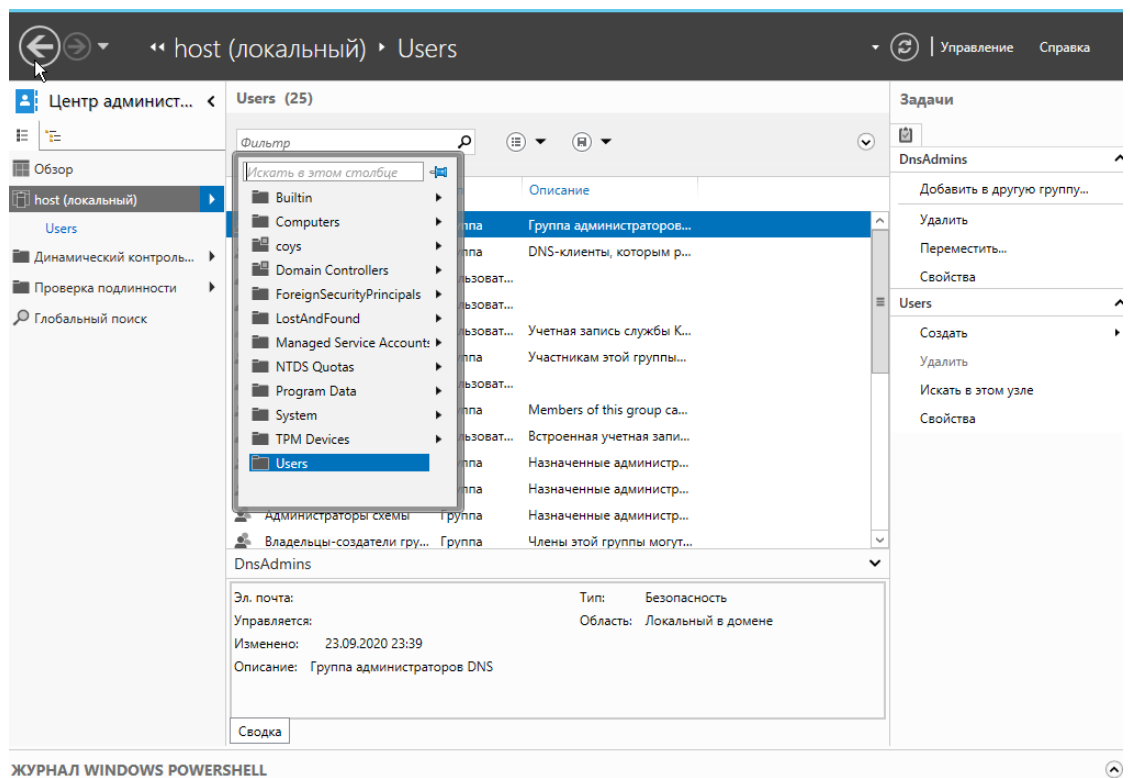


Рисунок 35 – Настройка перемещаемых профилей в учетных записях

пользователей



ЖУРНАЛ WINDOWS POWERSHELL

Рисунок 36 – Настройка перемещаемых профилей в учетных записях пользователей

4. Выбрать всех пользователей, для которых требуется использовать перемещаемые профили, щелкнуть по ним правой кнопкой мыши и выбрать пункт «Свойства» (рисунок 37);

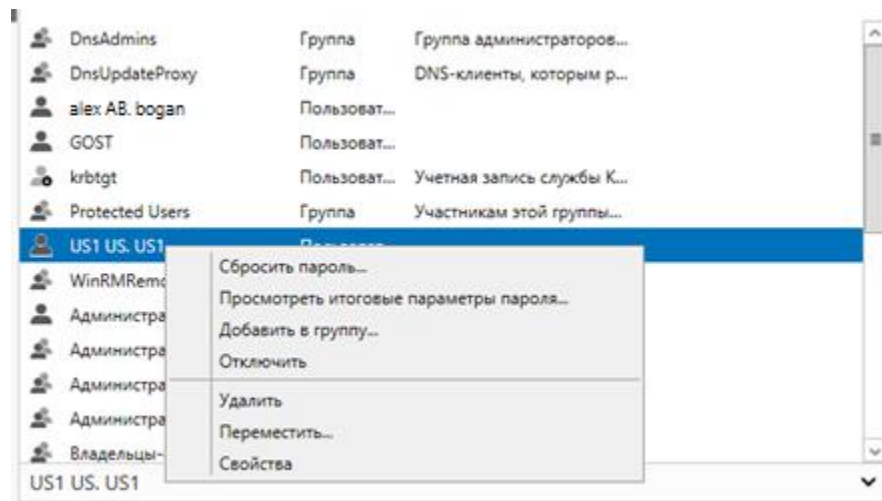


Рисунок 37 – Настройка перемещаемых профилей в учетных записях пользователей

5. В разделе «Профиль» в поле «Путь к профилю» указать путь к общей папке, в которой планируется хранить перемещаемый профиль

пользователя (в конце пути следует добавить «%username%» - автоматически заменится на имя пользователя при первом входе) (рисунок 38). После этого нажать на «ОК» (рисунок 39).

\\datainfo\User Profiles\$\%username%

Рисунок 38 – Пример пути к общей папке

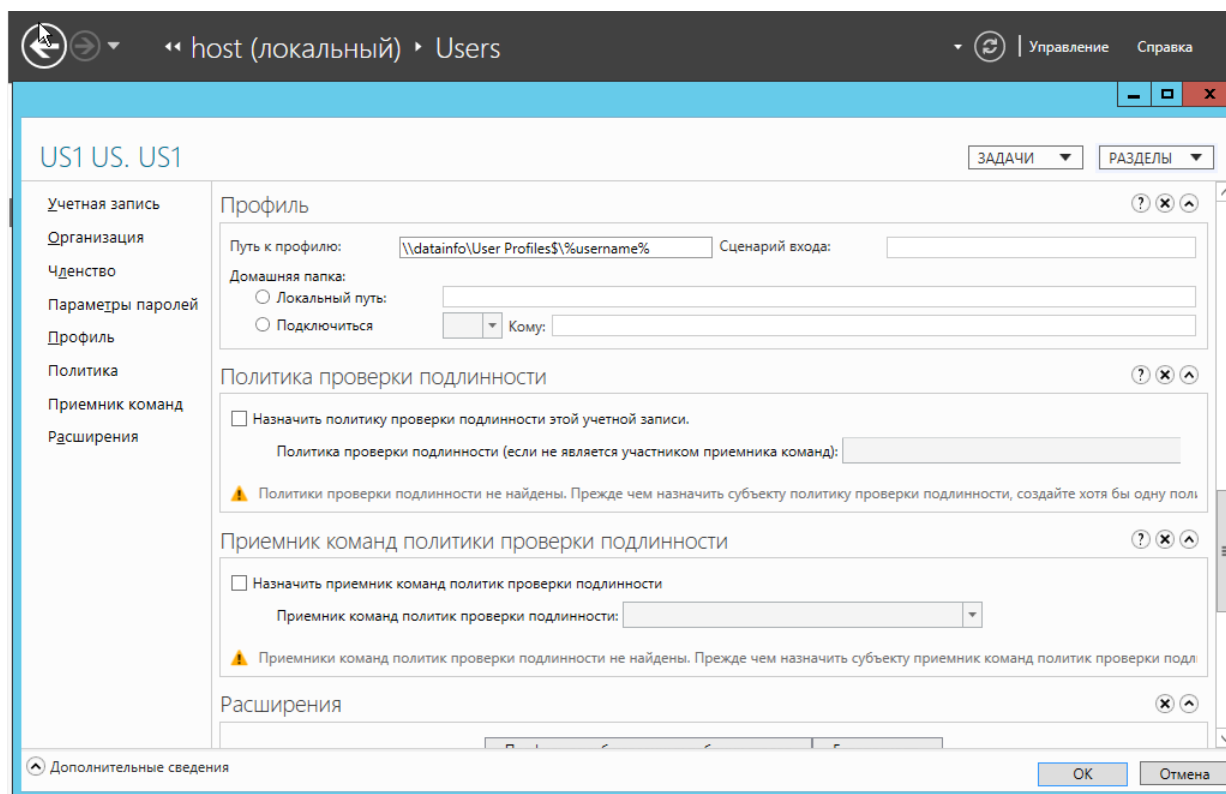


Рисунок 39 – Настройка перемещаемых профилей в учетных записях пользователей

Настройка перемещаемых профилей пользователей на компьютерах

Пятым шагом при создании перемещаемых профилей пользователей является их настройка на компьютерах. Для этого необходимо выполнить следующую последовательность действий:

1. Открыть диспетчер серверов («Пуск» → «Диспетчер серверов»);
2. В меню «Средства» выбрать «Управление групповой политикой», после чего появится окно управления групповыми политиками (рисунок 40);

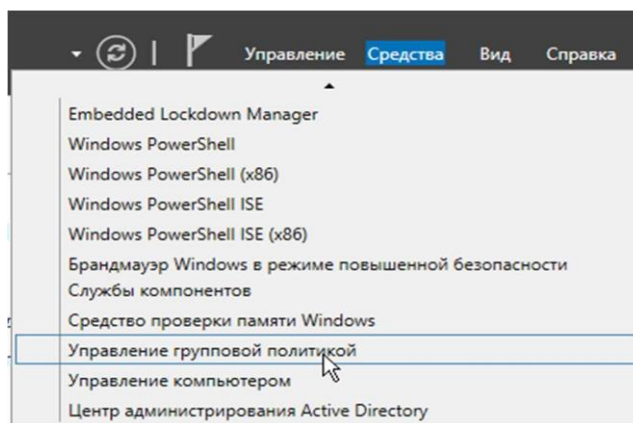


Рисунок 40 – Управление групповой политикой

3. В компоненте управления групповыми политиками щелкнуть правой кнопкой мыши по GPO, который был создан ранее (например, «Настройки перемещаемого профиля пользователя»), после чего выбрать пункт «Изменить» (рисунок 41);

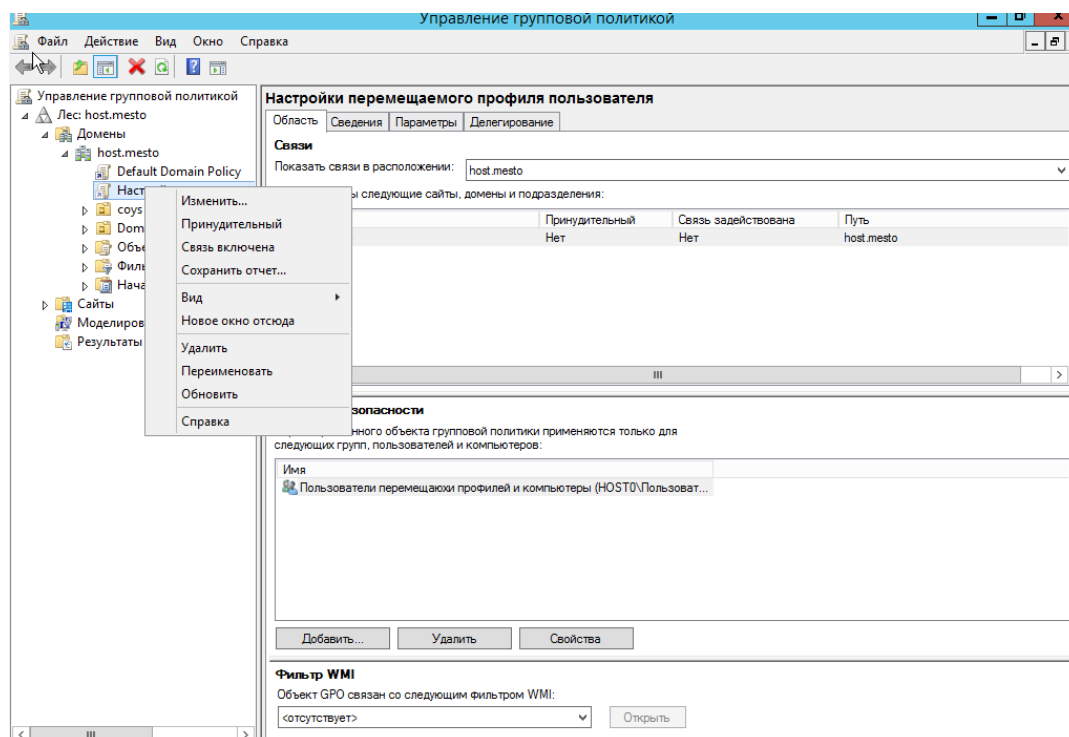


Рисунок 41 – Настройка перемещаемых профилей

4. В окне редактора управления групповыми политиками перейти к разделу «Профили пользователей» («Конфигурация компьютера» > «Политики» -> «Административные шаблоны» -> «Система» -> «Профили пользователей») (рисунок 42);

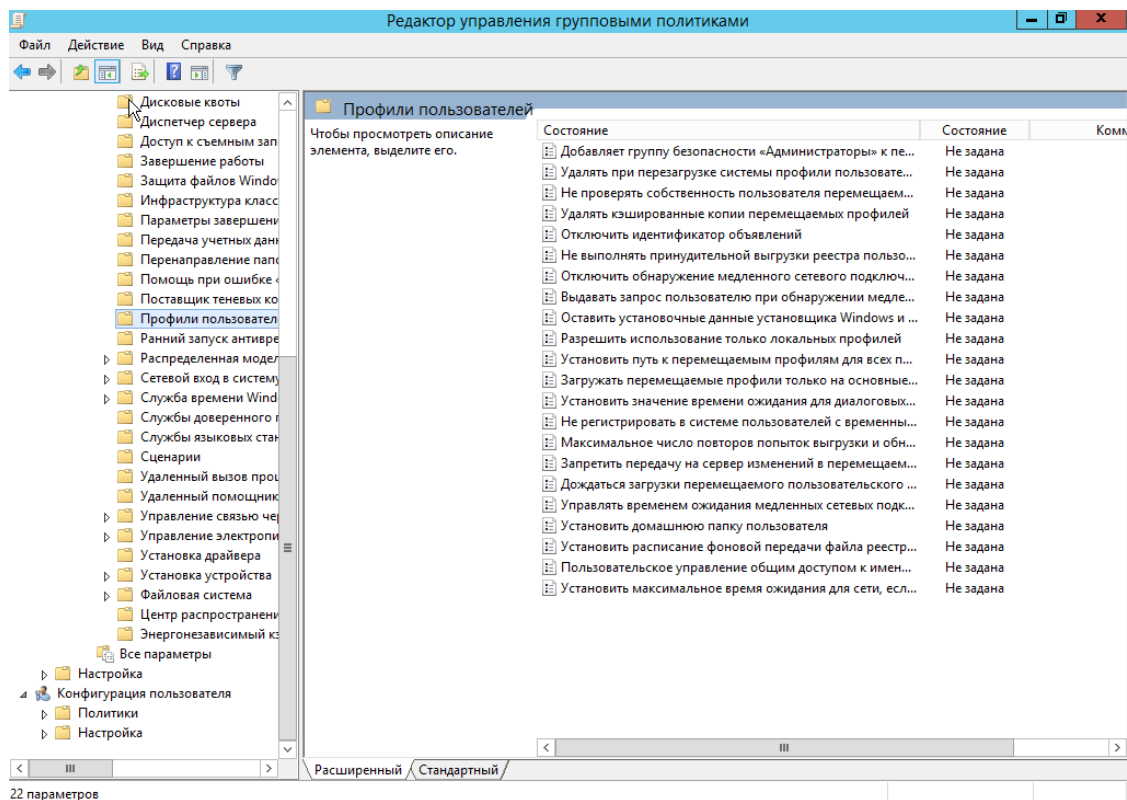


Рисунок 42 – Настройка перемещаемых профилей

5. Щелкнуть правой кнопкой мыши «Установить путь к перемещаемым профилям для всех пользователей, входящих в систему на данном компьютере» и нажать «Изменить» (рисунок 43);

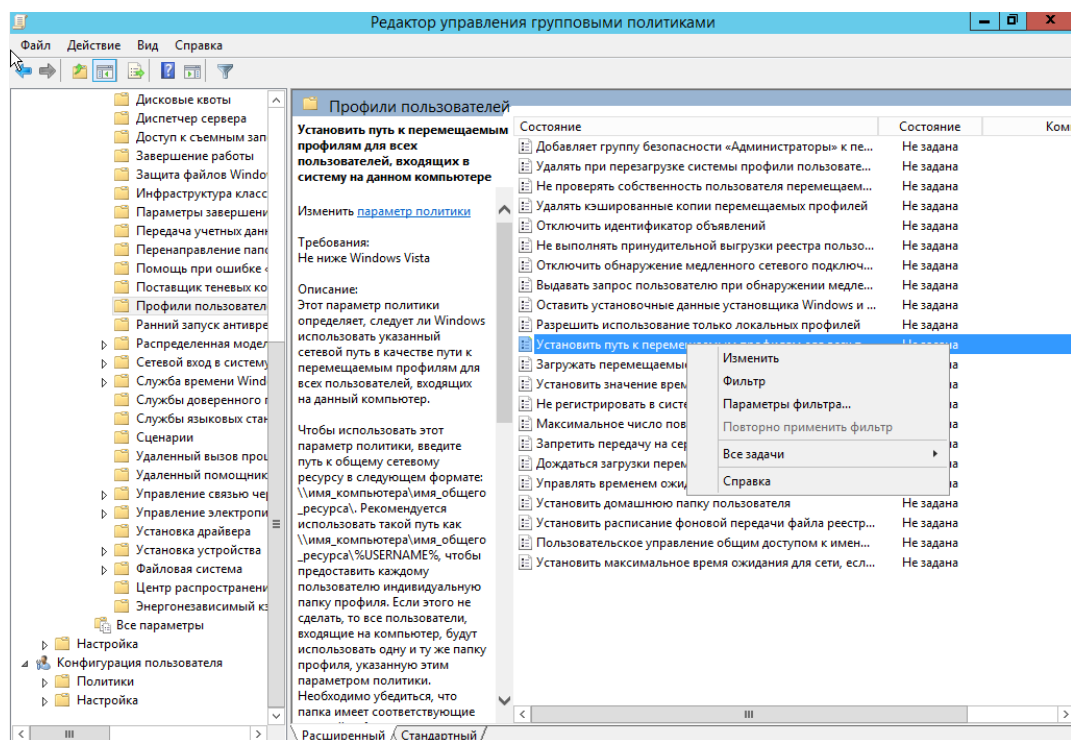


Рисунок 43 – Настройка перемещаемых профилей

6. В появившемся диалоговом окне щелкнуть «Включено» (рисунок 44);

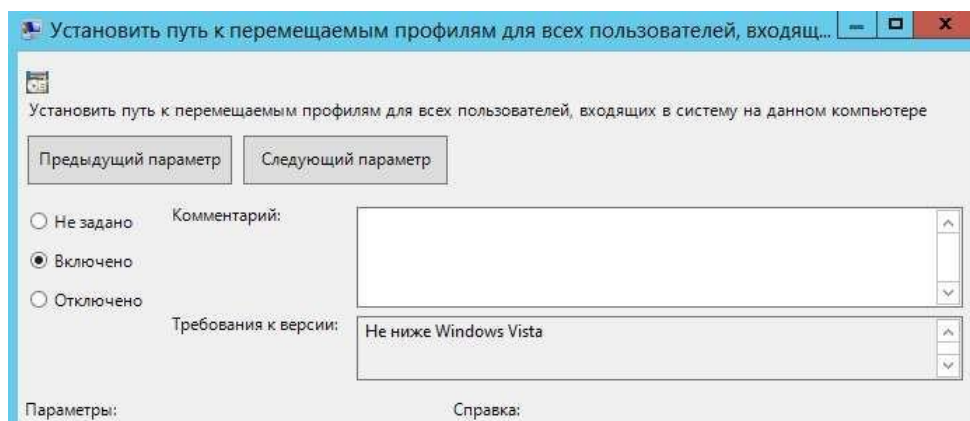


Рисунок 44 – Настройка перемещаемых профилей

7. В поле «Пользователи, входящие на данный компьютер, должны использовать следующий путь для перемещаемых профилей» указать путь к общей папке, в которой планируется хранить перемещаемый профиль пользователя (в конце пути следует добавить «%username%» - автоматически заменится на имя пользователя при первом входе). После этого нажать на «ОК» (рисунок 45).

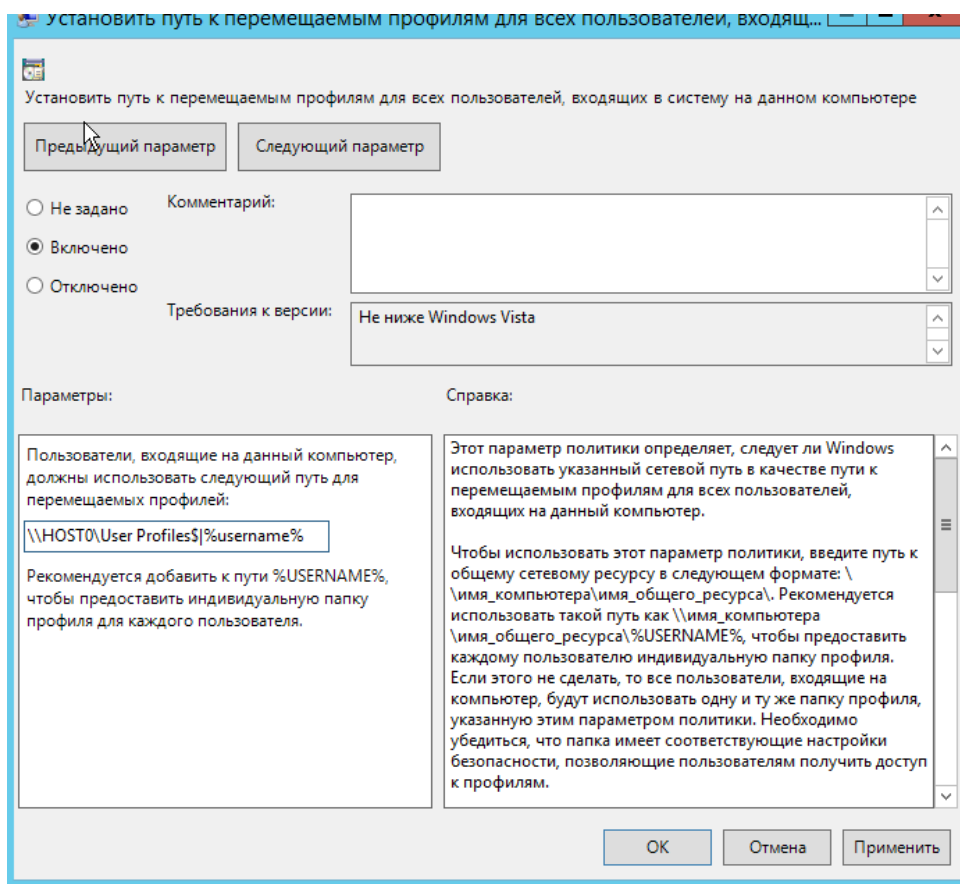


Рисунок 45 – Настройка перемещаемых профилей

Включение GPO перемещаемых профилей пользователей

Для включения GPO перемещаемых профилей пользователей необходимо выполнить следующую последовательность действий:

1. Открыть диспетчер серверов («Пуск» → «Диспетчер серверов»);
2. В меню «Средства» выбрать «Управление групповой политикой», после чего появится окно управления групповыми политиками (рисунок 46);

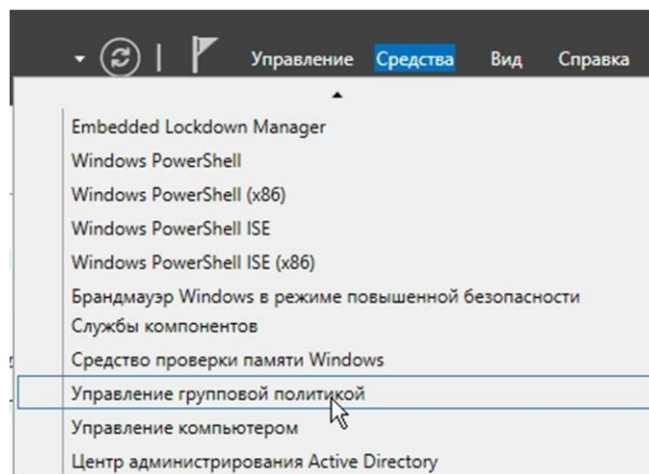


Рисунок 46 – Управление групповой политикой

3. Щелкнуть правой кнопкой мыши по созданному GPO и нажать «Связь включена» (рядом с соответствующим пунктом меню появится флажок) (рисунок 47).

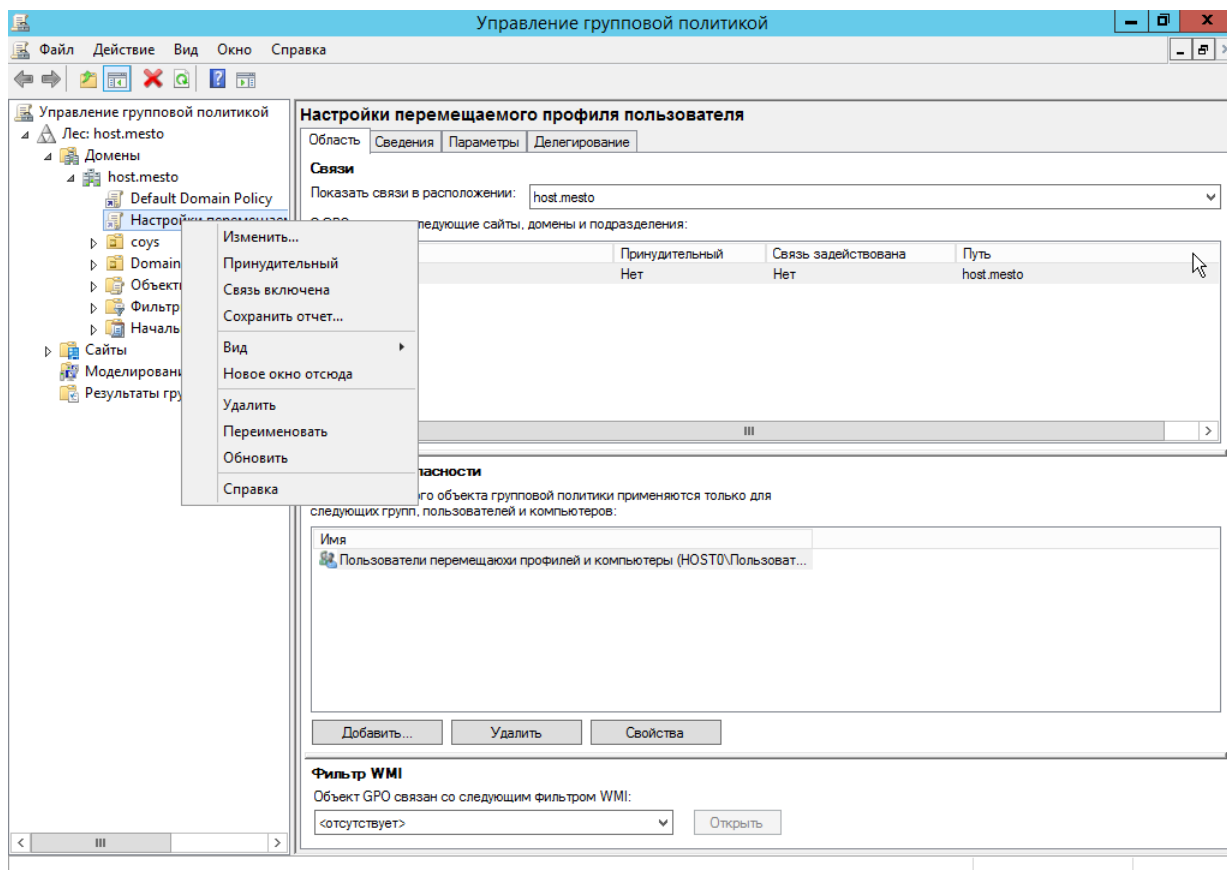


Рисунок 47 – Включение GPO перемещаемых профилей пользователей

Вывод: в ходе выполнения данной лабораторной работы были получены навыки по созданию и управлению учетными записями в домене Windows Server 2012.