ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ЧЕЛЯБИНСКИЙ МЕХАНИКО-ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

Рассмотрено и утверждено
на заседании ЦМК
Протокол
№ ___ от _____20___г.
_____/_____/

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНЫХ (ВНЕАУДИТОРНЫХ) ЗАНЯТИЙ В РАМКАХ ПОДГОТОВКИ К ПРОФЕССИОНАЛЬНЫМ КОНКУРСАМ С УЧЕТОМ РАЗДЕЛОВ РАБОЧЕЙ ПРОГРАММЫ

МДК 02.02 Организация администрирования компьютерных систем

для специальности
09.02.02 Компьютерные сети

Челябинск, 2018

Автор:

Черепанова Любовь Владимировна, преподаватель, эксперт WS и демонстрационного экзамена компетенции Сетевое и системное администрирование

ФИО, должность

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические рекомендации по выполнению самостоятельных (внеаудиторных) занятий по МДК02.02 «Организация администрирования компьютерных систем» направлены на оказание методической помощи студентам при выполнении практических заданий.

Выполнение практических заданий студентами влияет на формирование и развитие компетенций.

ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.

ПК 2.2. Администрировать сетевые ресурсы в информационных системах.

ПК 2.4. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

В результате изучения МДК обучающийся должен иметь практический опыт:

- настройки сервера и рабочих станций компьютерных систем для безопасной передачи информации;
- установки web-сервера, организации доступа к локальным и глобальным сетям, сопровождения и контроля использования почтового сервера, SQL-сервера;

В результате освоения дисциплины обучающийся должен уметь:

- администрировать локальные вычислительные сети;
- принимать меры по устранению возможных сбоев;
- устанавливать информационную систему, создавать и конфигурировать учетные записи отдельных пользователей и пользовательских групп, регистрировать подключение к домену, вести отчетную документацию;
- устанавливать и конфигурировать антивирусное программное обеспечение, программное обеспечение баз данных, программное обеспечение мониторинга;
- обеспечивать защиту при подключении к сети Интернет средствами операционной системы;

В результате освоения дисциплины обучающийся должен знать:

- основные направления администрирования компьютерных сетей;

- типы серверов, технологию "клиент-сервер", способы установки и управления сервером, утилиты, функции, удаленное управление сервером, технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в web;
- взаимодействие различных операционных систем;
- классификацию программного обеспечения сетевых технологий и область его применения;
- лицензирование программного обеспечения.

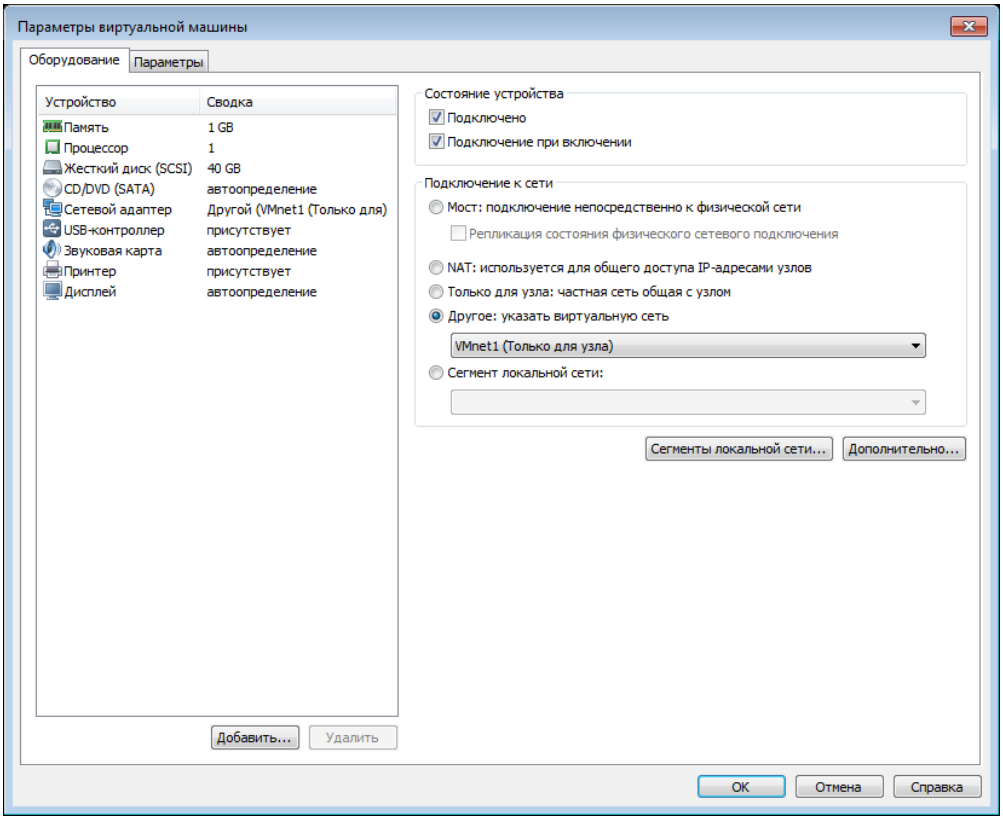
Выполнение комплексного задания предполагает выполнение практического задания в формате WSR по компетенции «Сетевое и системное администрирование», ч учетом типовых конкурсных заданий прошлых периодов подготовки.

Суть задания по компетенции «Сетевое и системное администрирование» состоит в настройке параметров серверной операционной системы MS Windows Server 2012 R2, отвечающих заданным требования.

Содержание

Базовая настройка сервера с GUI

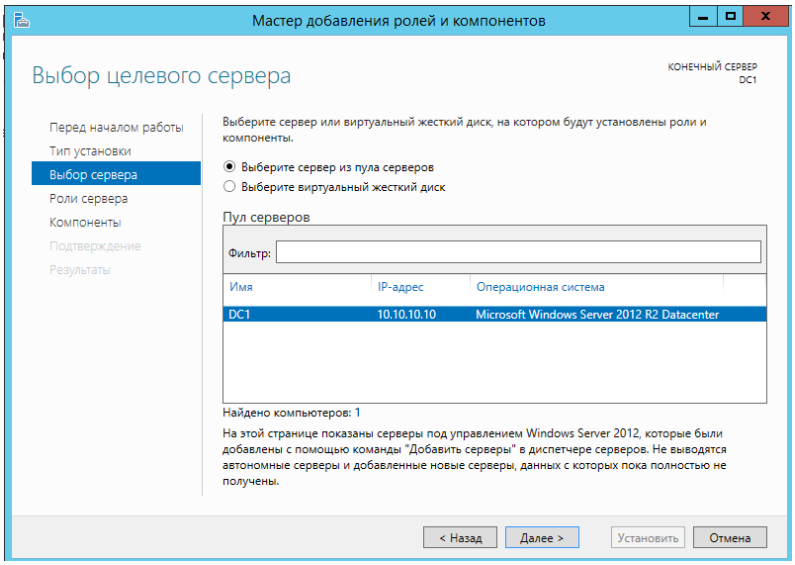
1. Базовая настройка (смена имени и IP-адреса -10.10.10.10, маска 255.255.255.0 и шлюза).
2. Зайдем в ***Панель управления → Учетные записи пользователей → Учетные записи пользователей → Управление другой учетной записью → Администратор (Administrator) → Создать пароль***.
3. Проверка и смена типа подключения (только узел).
   Виртуальная машина → Параметры виртуальной машины → Подключение к сети (***Только для узла***).



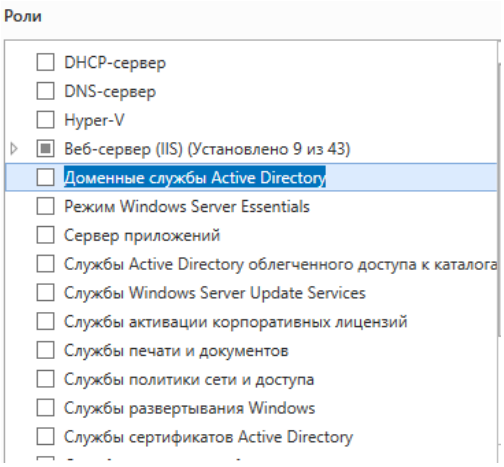
Создание домена - DC1

На сервере DC1 установите роль контроллера домена ural.prm.ru. В процессе установки так же установите роль DNS-сервера и настройте соответствующие зоны.

1. Установка роли AD:
   Диспетчер серверов → Панель мониторинга → Добавить роли и компонент → Тип установки (***установка ролей или компонентов***) → Выбор сервера



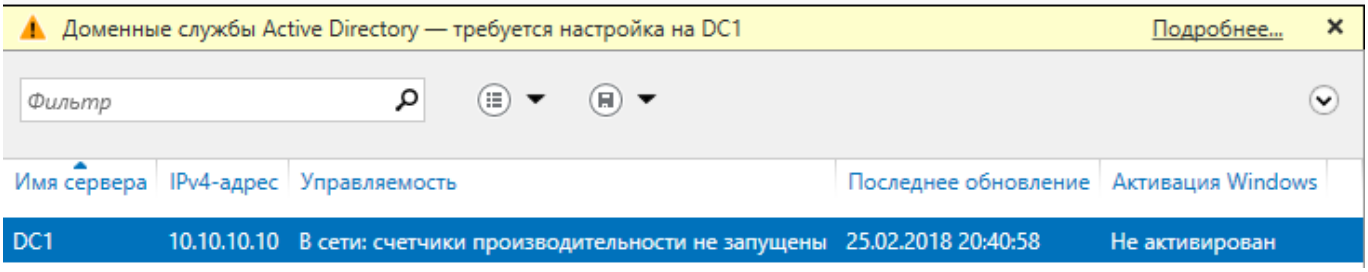
Выбираем роль – ***Доменная служба Active Directory (Active Directory Domain Services)*** и выбираем добавить компонент.



Выбор компонентов оставляем по умолчанию и нажимаем ***Далее*** и подтверждаем установку.

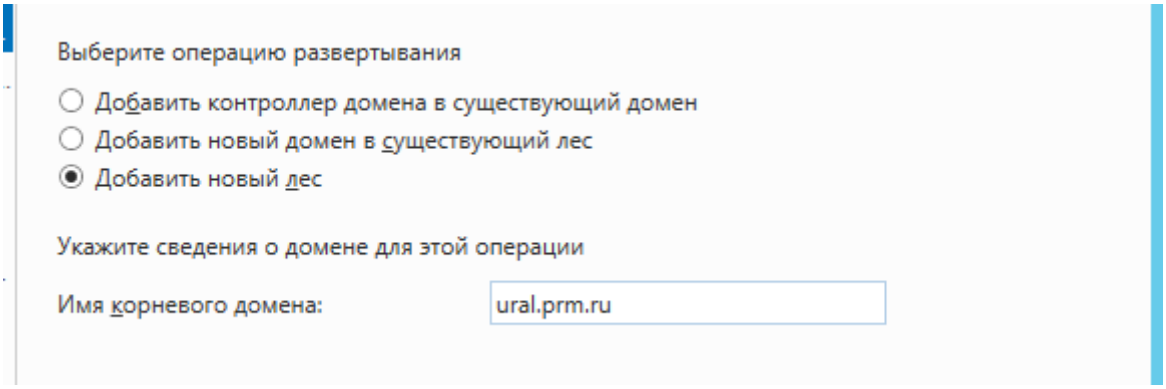
Пока служба AD можно осуществить базовую настройку остальных серверов.

4. **Базовая настройка. Сервер RRAS1.**
   - На Сервере добавим еще одну сетевую карту для этого зайдем в ***Виртуальную машину*** → ***Параметры виртуальной машины*** и нажмем на кнопку ***Добавить,*** выбираем ***сетевой адаптер*** и Подключение к сети (***Только для узла***).
   - Смена имени и IP-адреса – 10.10.10.1, маска 255.255.255.0 для первого интерфейса и для второго интерфейса IP-адреса – 20.17.255.1, маска 255.255.255.248 (т.к. маска 29 – 11111111.11111111.11111111.11111000) и шлюз.
5. ***Настройка AD***. Для этого в диспетчере серверов выберете AD DS, нажмем на ссылку ***Подробнее***.

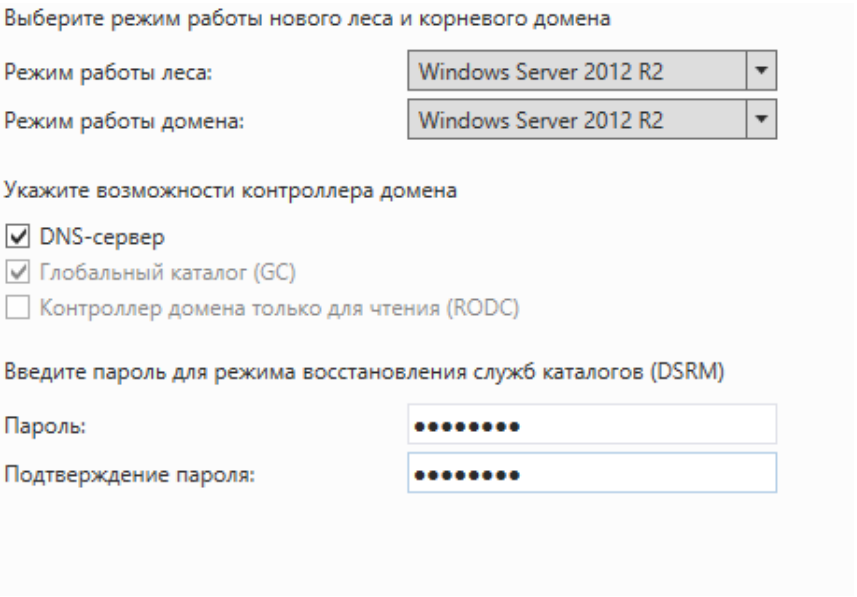


Далее выбираем ***Повысить роль этого сервера до уровня контролера домена***.

6. В конфигурации развертывания выбираем – ***Добавить новый лес*** (***Add a new forest***) и введите имя корневого домена – ***ural.prm.ru***.

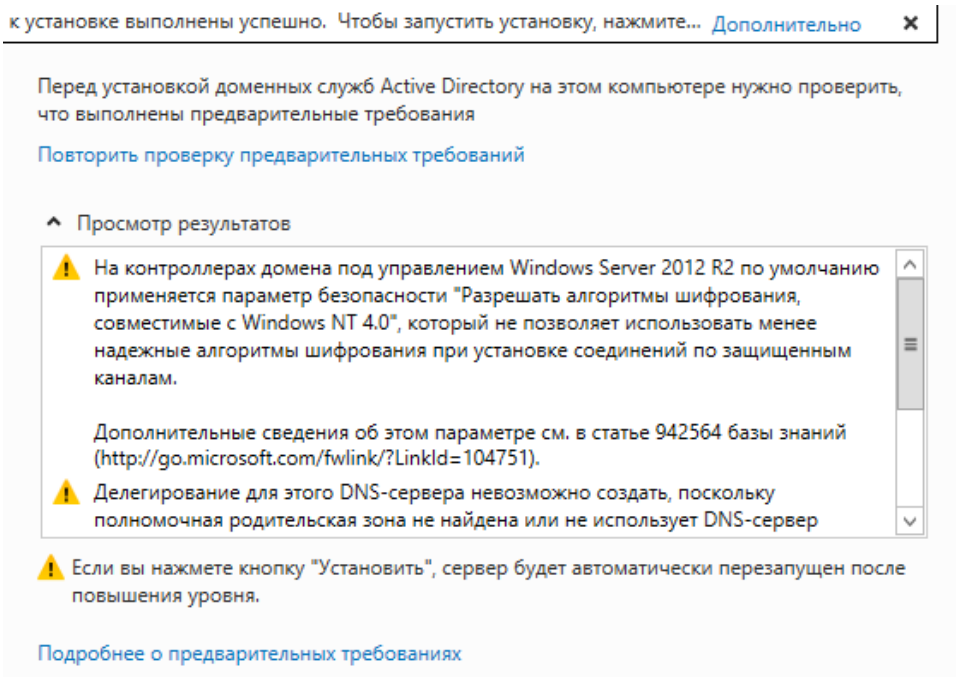


7. Введите пароль на восстановление и подтвердите установку службы DNS.

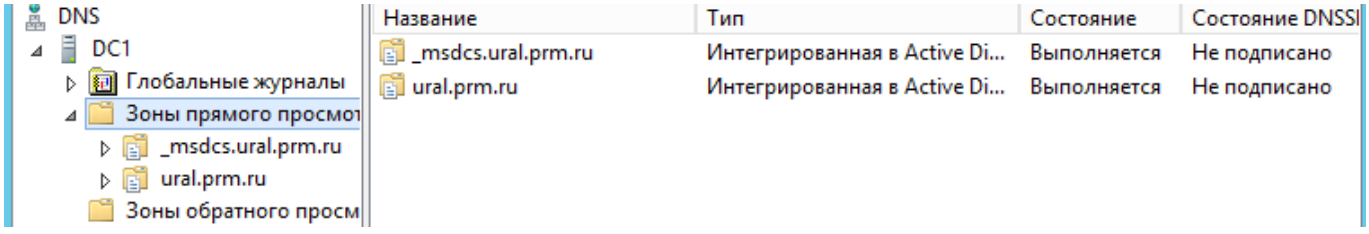


Затем нажмите 2 раза ***Далее***.

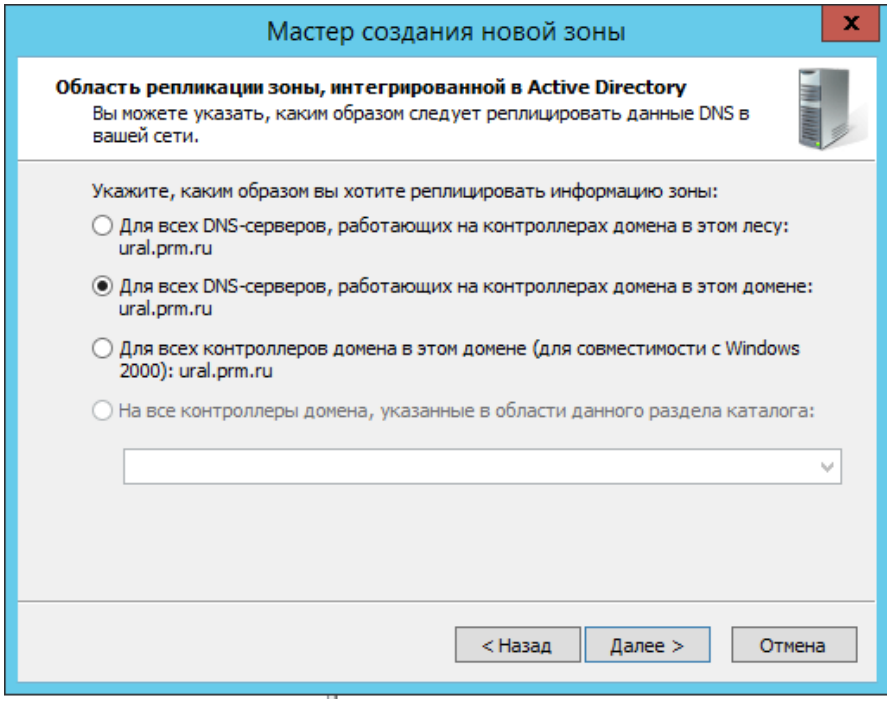
8. Подтвердите имя NetBIOS, а затем пути хранения файлов баз данных.
9. Посмотрите проверку предварительных требований, если забыли установить пароль на Администратора, требуется его установить и в данном окне повторить проверку предварительных требований и нажать ***Установить***



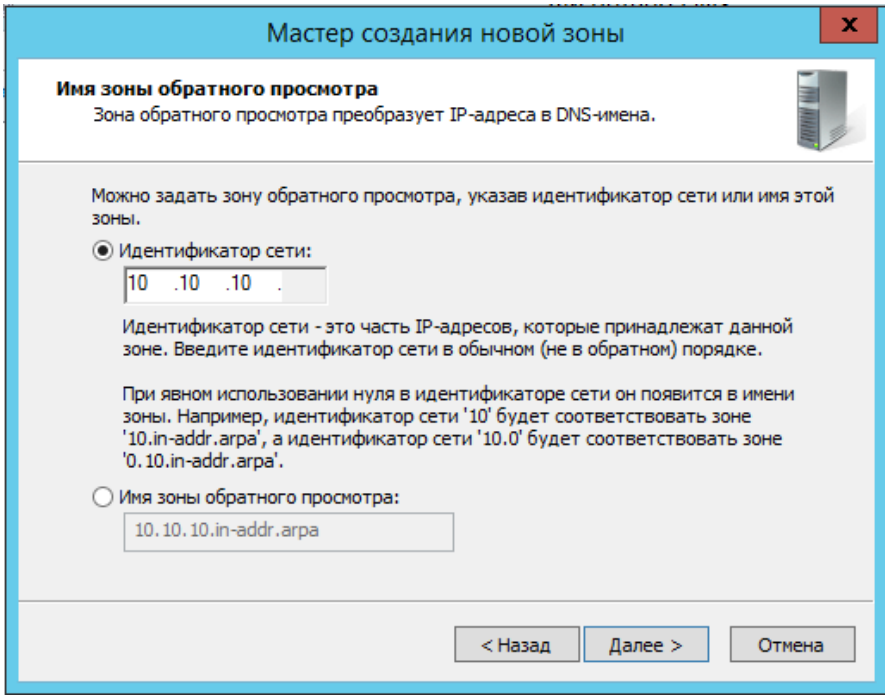
10. ***Настройка DNS***. В диспетчере серверов выбираем ***Средства → DNS***. Открываем сервер, проверяем наличие зоны прямого просмотра и создаем зону обратно просмотра.



11. Выбираем зону обратного просмотра, щелкаем по ней правой кнопкой мыши и выбираем ***Создать***.
12. Выбираем тип зоны – ***Основная зона*** и выбираем область репликации.



13. Выбираем тип Ip-адресов v4.
14. Выбор имени зоны обратного просмотра, нажимаем 2 раза ***Далее*** и подтверждаем создание зоны.



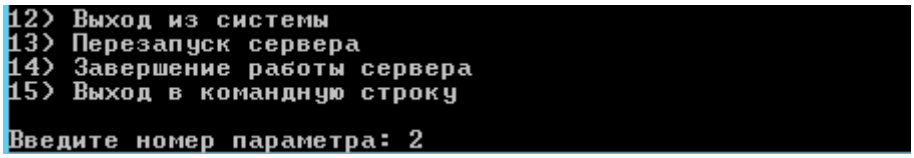
Создание второго домена DC2

1. Базовая настройка (смена имени, IP-адреса и пароля).
2. На сервере DC2 установите роль контроллера домена chel.prm.ru. В процессе установки так же установите роль DNS-сервера и настройте соответствующие зоны.
   Аналогично установите и настройте службы AD и DNS сервера DC2.

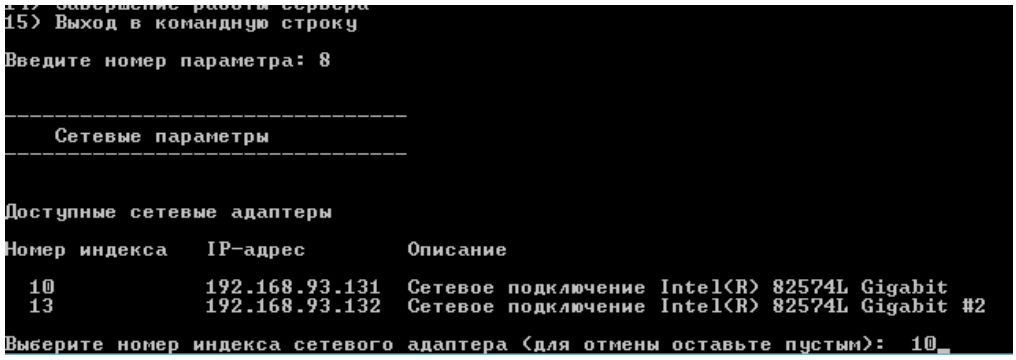
Базовая настройка RRAS3 (без графики)

1. На Сервере добавим еще одну сетевую карту для этого зайдем в ***Виртуальную машину*** → ***Параметры виртуальной машины*** и нажмем на кнопку ***Добавить,*** выбираем ***сетевой адаптер*** и Подключение к сети (***Только для узла***).
2. ***Базовая настройка***. При отсутствии графики для смены параметров в командной строке набрать

3. В начале строки появится PS, которое обозначает, что вы находитесь в PowerShell. В строке забить команду – Sconfig.
4. Введите номер параметра – 2



5. И введите новое имя компьютера – RRAS3.
6. Для смены ip-адреса – 8

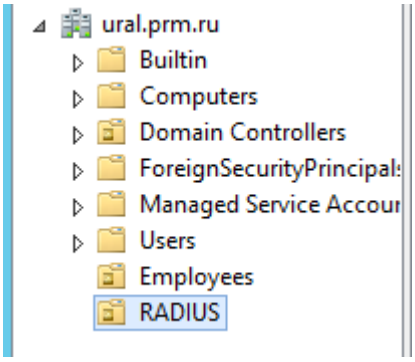


7. Выберете номер первого сетевого адаптера, выберете номер 1 для смены ip-адреса, а затем S для задания статического адреса и установите ip-адрес – 10.20.20.1, маску – 255.255.255.0. Затем выберете номер 2 для установления адреса DNS – 10.20.20.10. Затем нажмите 4 для возвращения в меню.
8. Аналогично поменяйте адрес второго сетевого адаптера (ip-адрес, маску, шлюз и адрес DNS).
9. Добавление в домен. Настройка конфигураций – Sconfig, номер 1, завет вводится домена.

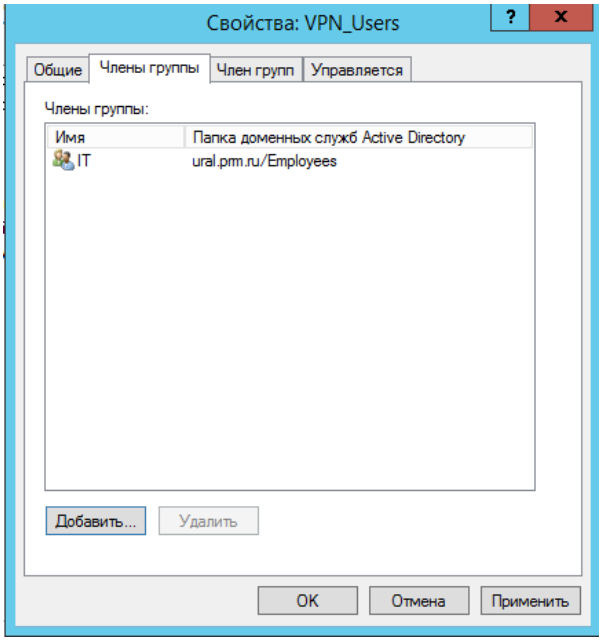
Создание иерархии AD контролеров DC1 и DC2

Создайте пользователей, группы и организационные подразделения в доменах согласно таблице 3. Учтите, что создавать каждого пользователя вручную накладно, используйте соответствующий скрипт. Все созданные учетные записи пользователей должны быть включены и иметь пароль P@ssw0rd1.

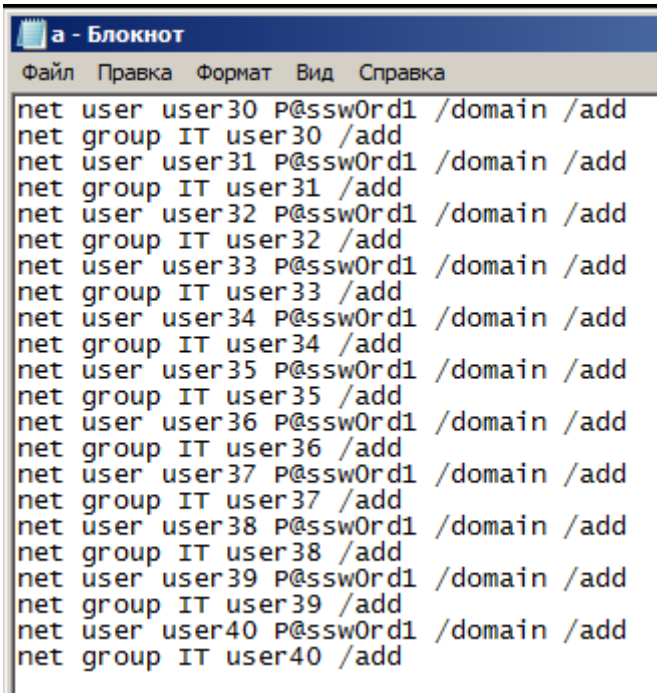
1. На сервере DC1 в ***Диспетчере серверов → Средства → Пользователь и компьютеры AD*** выберете ***ural.prm.ru*** и щелкните правой кнопкой мыши → ***Создать → Подразделение***. В соответствие с таблицей 3 создайте подразделения.



2. Щелкнете правой кнопкой по подразделению ***Employees → Создать → Группа*** и создайте 2 группы (Employees и IT). В подразделении RADIUS создайте группу RadiusAdmins, а в Users создайте группу VPN_Users.
3. Выбираем группу VPN_Users → Свойства → Члены группы → Добавить → IT.



4. Выбираем группу RadiusAdmins → Свойства → Члены группы → Добавить → Администраторы домена.
5. Создайте пользователей, используя информацию в таблицу 3.

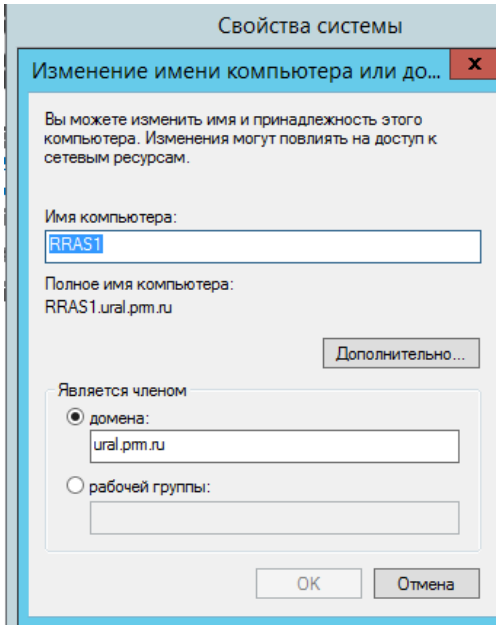


Сохраните файл с расширением bat и запустите его.

6. Перенесите созданных пользователей из подразделения Users в Employees.
7. На сервере DC2 в Диспетчере серверов → Средства → Пользователь и компьютеры AD выберете chel.prm.ru и щелкните правой кнопкой мыши → Создать → Подразделение. В соответствие с таблицей 3 создайте подразделения, группы и пользователей.

Введение компьютеров в домен

1. *Введите компьютер RRAS1 в домен ural.prm.ru.*
   Диспетчер серверов → Локальный сервер → Рабочая группа (для этого у вас должен быть включены оба компьютера контролер домена и клиент).



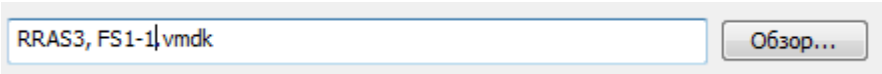
2. *Введите компьютеры FS2, CLI2 и RRAS3 в домен chel.prm.ru.*
   Аналогично введите компьютеры в домен

Создание RAID

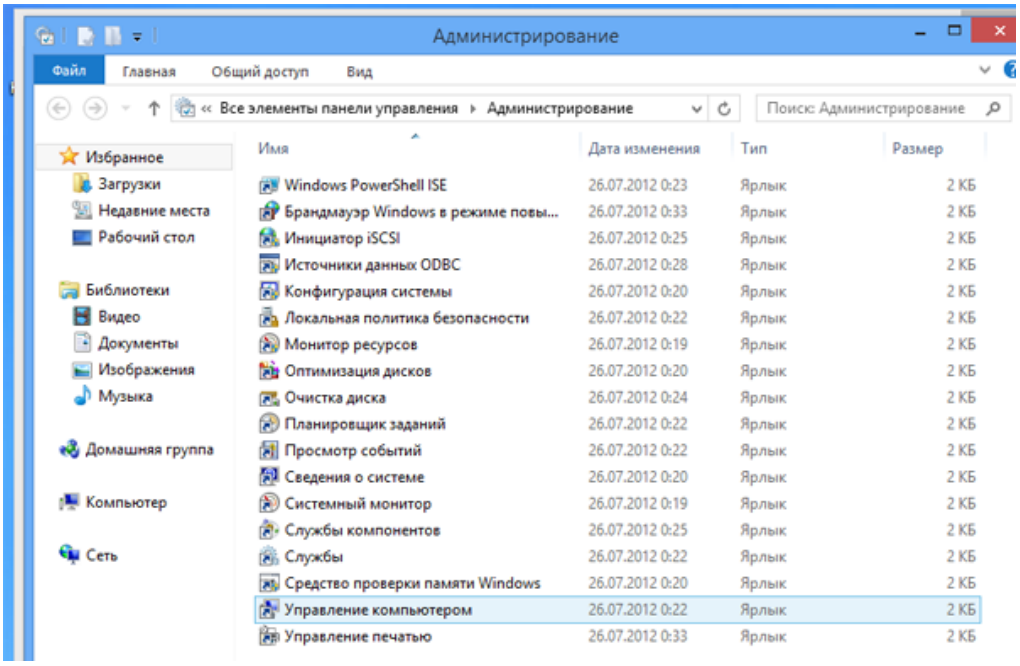
Настройте отказоустойчивость дисковой подсистемы

– *В домене chel.prm.ru на сервере RRAS3 настройте программное зеркалирование системного диска. Используйте для этого один из имеющихся в составе сервера дополнительных дисков! Будьте внимательны, переразметить системный раздел после зеркалирования не удастся, поэтому можете использовать второй из имеющихся дополнительных на сервере дисков для создания резервных копий.*

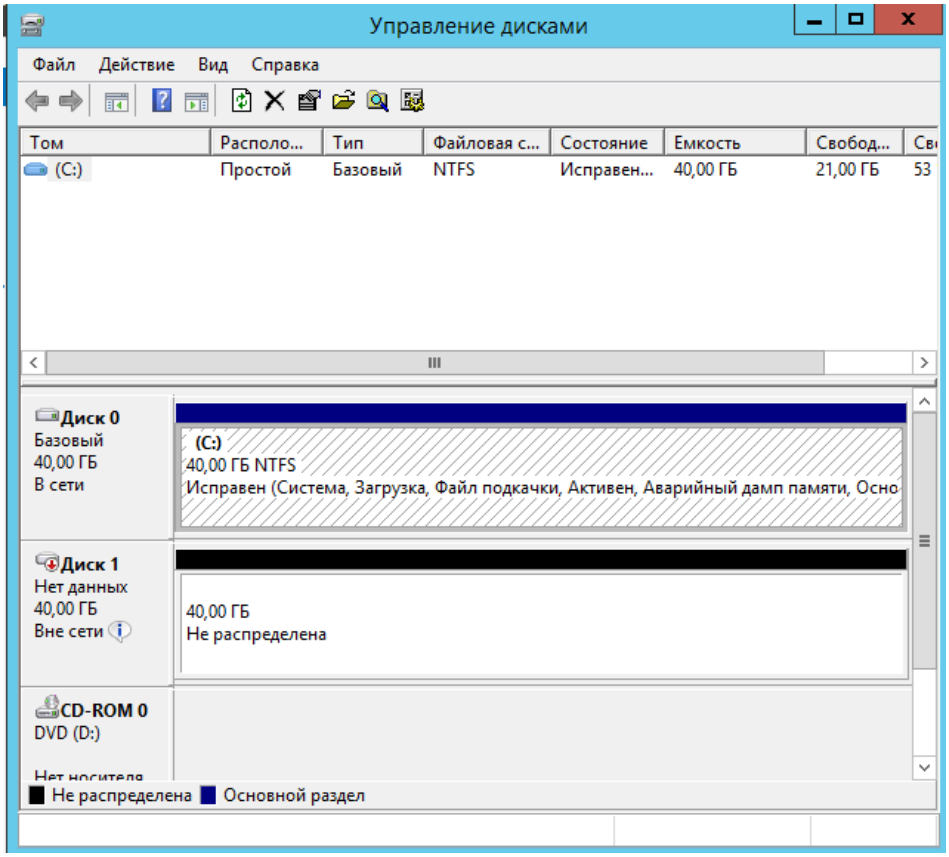
1. На Сервере добавим еще один диск чуть большего объема, что и основной для этого зайдем в ***Виртуальную машину*** → ***Параметры виртуальной машины*** и нажмем на кнопку ***Добавить***, выбираем ***жесткий диск*** → тип диска (по рекомендации) → Создать новый виртуальный диск → Выставляем объем диска → и меняем цифру на 1



2. Для создания зеркала необходимо войти в управление дисками. Для этого заходим в ***Панель управления*** и выбираем "***Администрирование***".
3. В Администрировании находим "Управление компьютером".

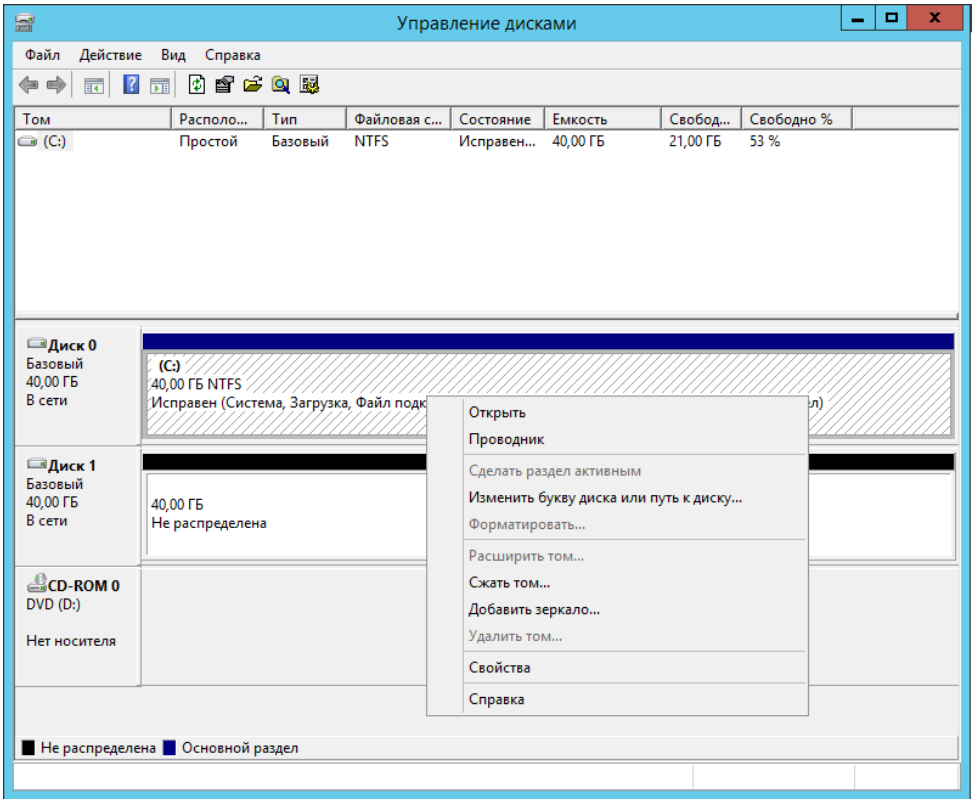


4. В окне Управления компьютером слева выбираем "Управление дисками".

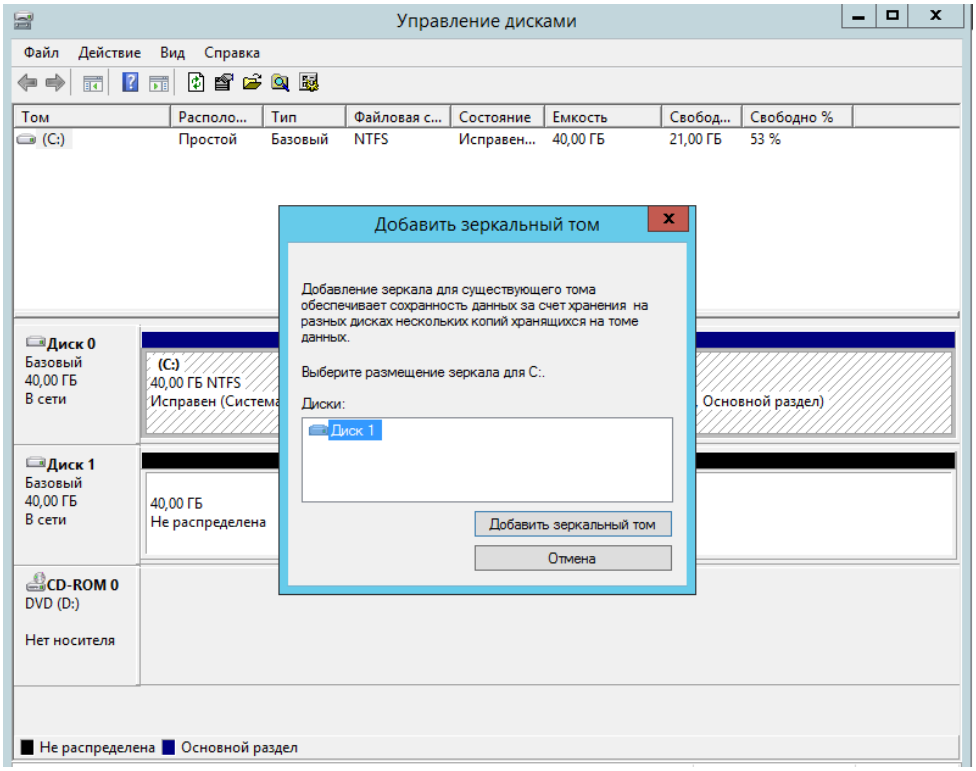


5. Щелкнем по диску 1 правой кнопкой мыши и выберем «В сети» → ПКМ Инициализировать диск →Подтверждаем инициализацию.

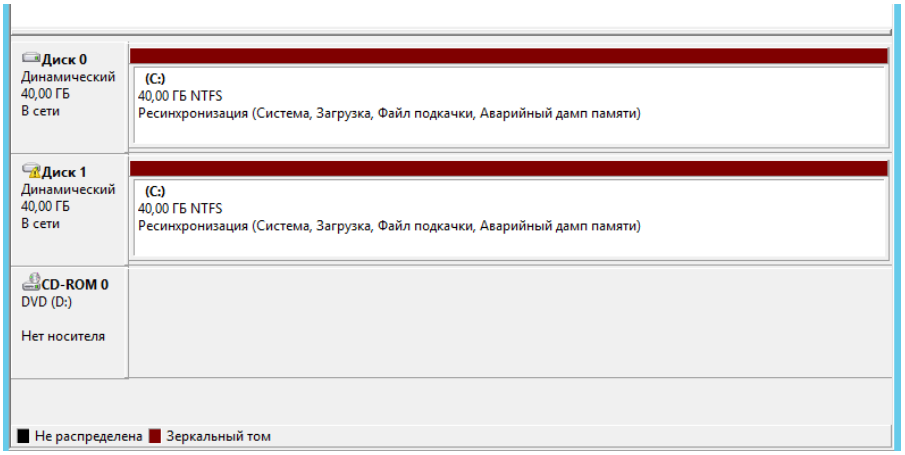
   Из рисунка видно, что на компьютере есть 2 физических диска - "Диск 0" и "Диск 1". Будем создавать зеркало для логического диска С. Объем этого раздела 40Гб. На втором диске должно быть нераспределенное свободное место, объем которого не меньше объема зеркалируемого диска.
6. Щелкаем правой кнопкой мыши на нужном разделе и в контекстном меню выбираем "Добавить зеркало".



7. Система предложит выбрать диск, который будет использоваться в качестве зеркала.

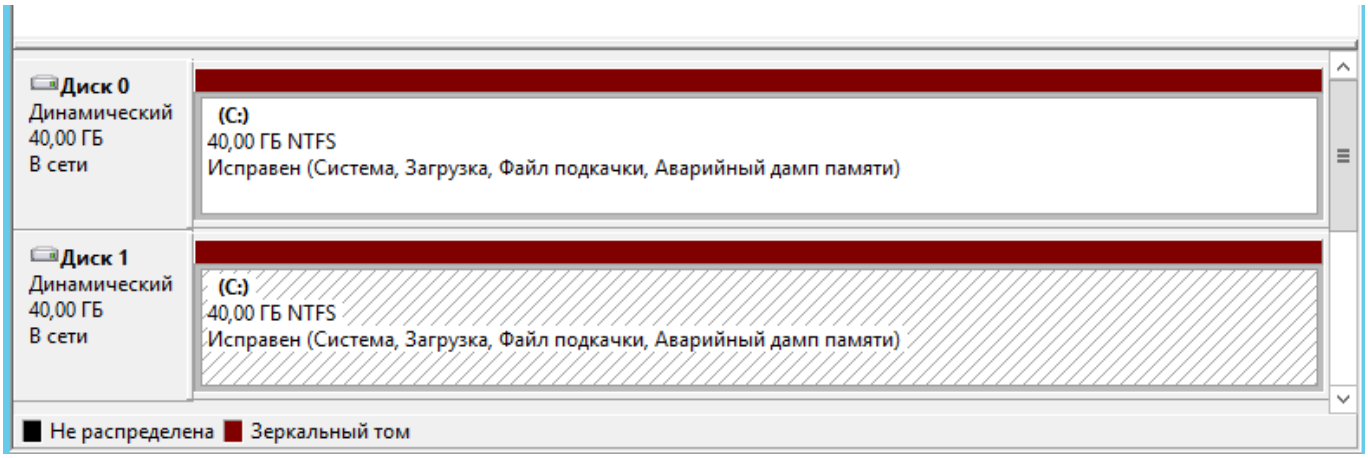


8. Выбираем нужный диск из списка и нажимаем "Добавить зеркальный том". Начнется процесс создания зеркала - если на диске C есть какие-то данные, они будут скопированы на зеркальный диск.



Синхронизация дисков при создании зеркала

9. После завершения всех процессов получаем вот такую картину.



Результат создания зеркала диска

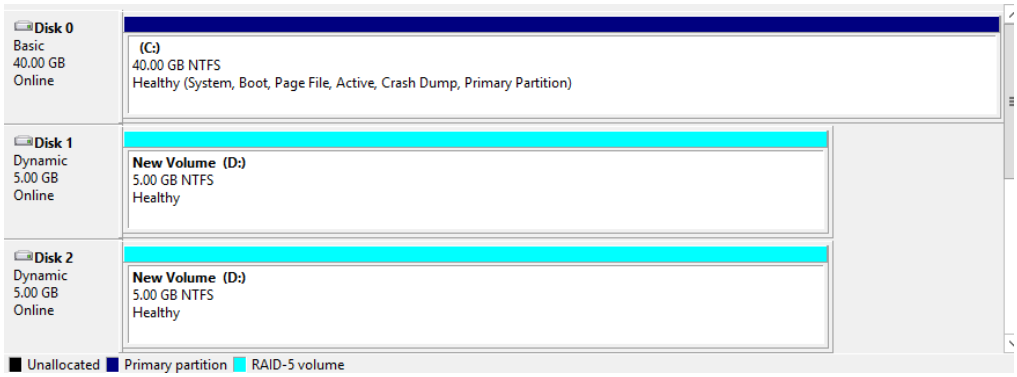
Система забирает со второго диска пространство, объем которого равный объему зеркалируемого диска.

– *В домене chel.prm.ru на сервере FS2 настройте RAID5-массив с участием диска D:\ и дополнительно имеющихся на сервере дисков. Помните, что на сервере должна функционировать система DFS, которая после настройки RAID должна сохранить работоспособность и функциональность.*

RAID-5 - Чередование дисков с записью четности. ***Три или более тома***. Например, в вашей системе 4 жестких диска, и эти жесткие диски пронумерованы как 0, 1, 2 и 3. Также будем считать, что диск 0 – это наш системный диск, а диски 1, 2 и 3 пустые жесткие диски, которые мы хотим превратить в том RAID 5.

Прежде чем мы сможем создать том RAID 5, мы должны убедиться, что каждый из дисков подключен как динамический диск.

1. Зайти в ***Управление дисками***.
2. Включить диски в сеть.
3. Сделать их динамическими
4. Выбрать диск 1 нажать на правую кнопку мышь и выбрать ***Создать том RAID5***.
5. Выбрать диски.
6. Выбрать букву диска D (при необходимости сменить у привода букву).

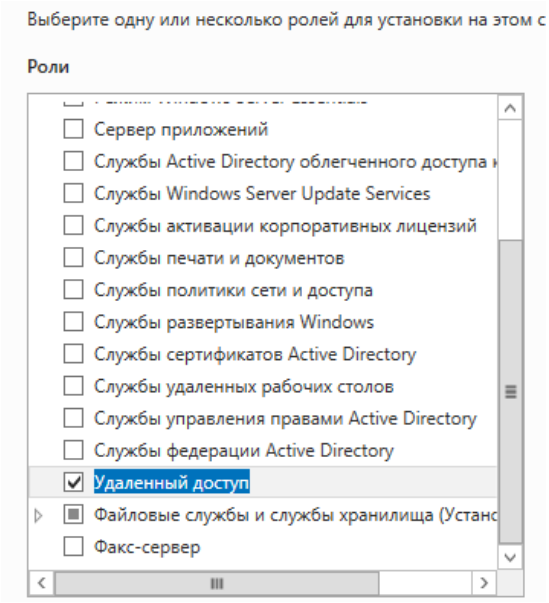


Настройка маршрутизации

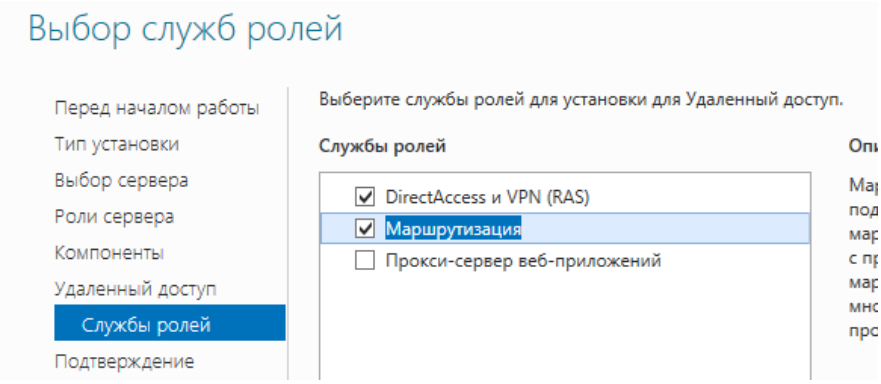
На серверах RRAS1(он же RDS), RRAS3 (он же FS1) разверните соответствующие роли для обеспечения возможностей маршрутизации и удаленного доступа.

Настройте протокол динамической маршрутизации RIP между офисами chel.prm.ru и ural.prm.ru.

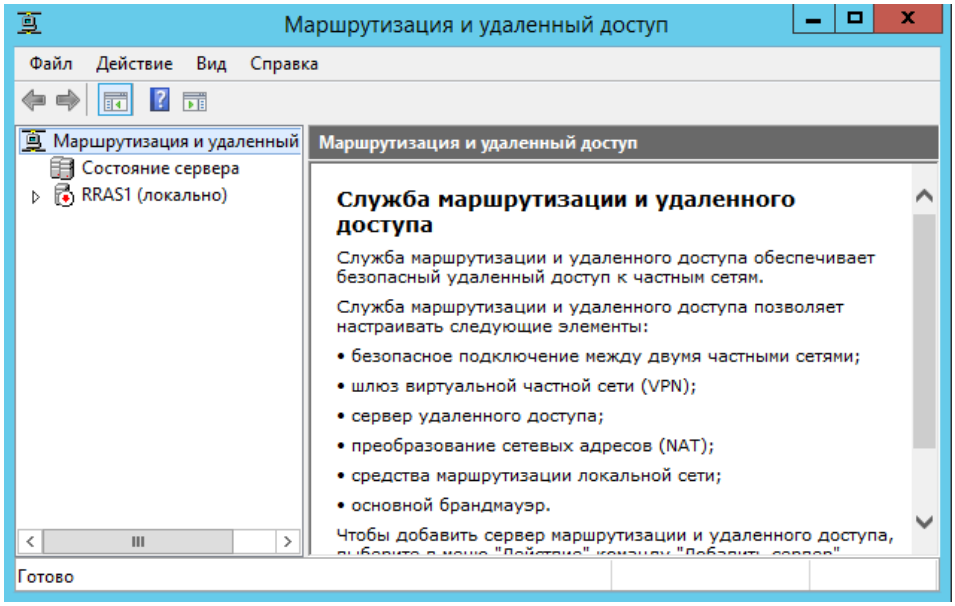
1. Запускаем RRAS1, открываем ***Диспетчер серверов → Панель мониторинга → Добавить роли и компонент*** Тип установки (***установка ролей или компонентов***) → Выбор сервера → Выбираем роль «***Удаленный доступ***».



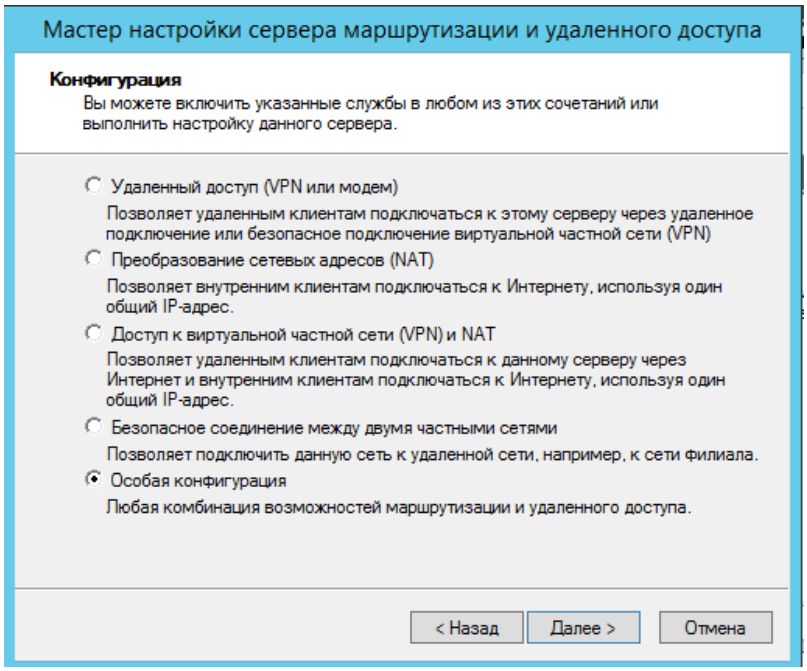
2. Нажимаем 2 раза ***Далее***, затем выбираем службы ролей «***DirectAccess***» и «***Маршрутизация***».



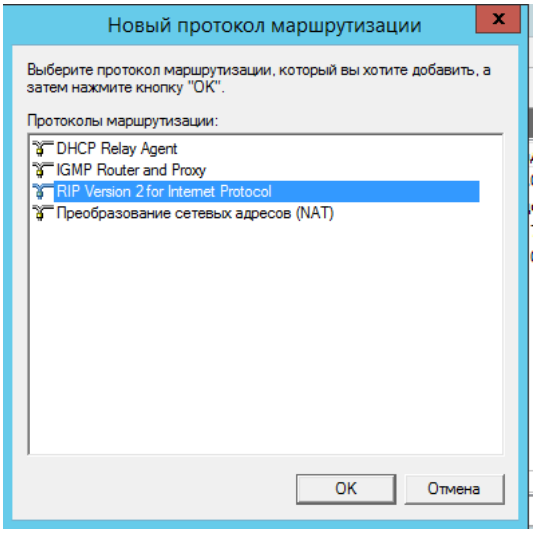
3. После установки закрываем «***Мастер добавления ролей и компонентов***».
4. Открываем «***Панель управления***» → «***Администрирование***» → консоль «***Маршрутизация и удаленный доступ***».



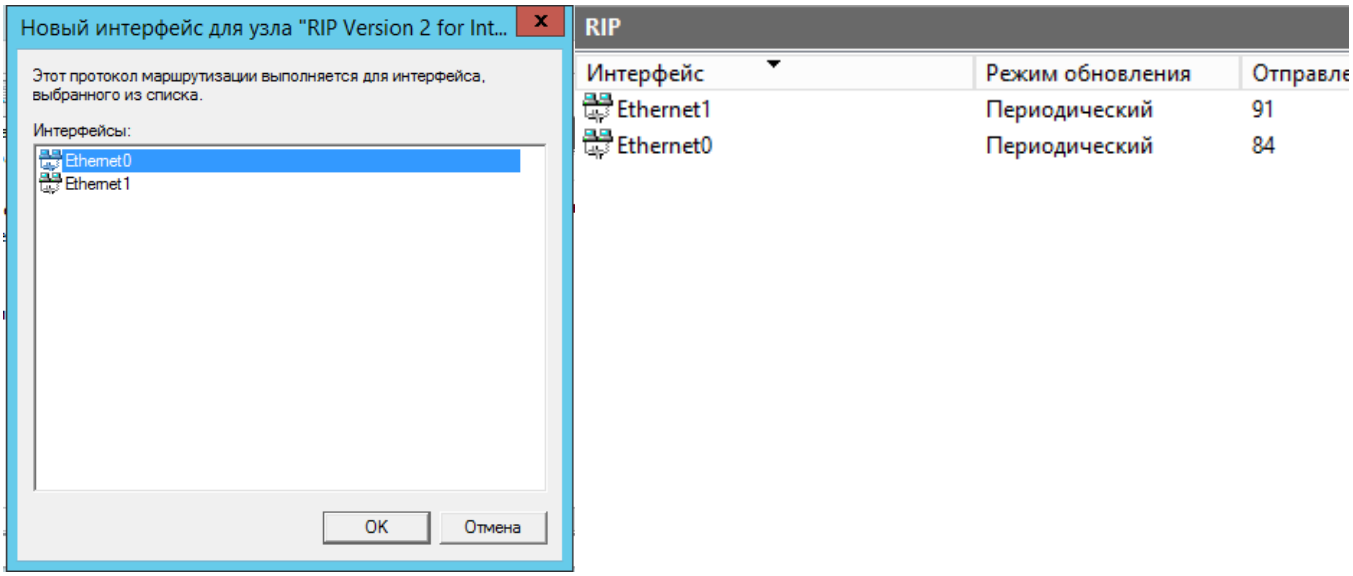
5. Щелкаем правой кнопкой мыши и в контекстном меню выбираем «***Настроить и включить маршрутизацию и удаленный доступ***». Выбираем «***Преобразование сетевых адресов (NAT)***».



6. Отмечаем «Преобразование сетевых адресов» и «Маршрутизация локальной сети».
7. Завершаем работу мастера. Запускаем службу. На данном этапе настройка маршрутизации закончена.
8. Открываем RRAS IPv4 на ссылке ***Общие*** щелкаем правой кнопкой и выбираем ***Новый протокол маршрутизации*** → Выбираем RIP и нажимаем на подтверждение.



9. Настройка заключается в добавление интерфейсов, которые вы захотите использовать для обмена маршрутами RIP. Для этого перейдите в секцию RIP, щелкните правой кнопкой, щелкните на New Interface, выберите интерфейс, который собираетесь добавить под RIP.

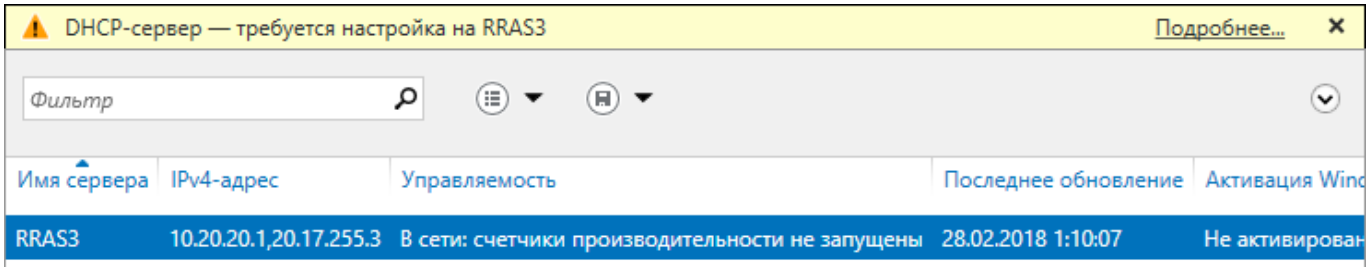


10. Аналогично настройте сервер RRAS3.

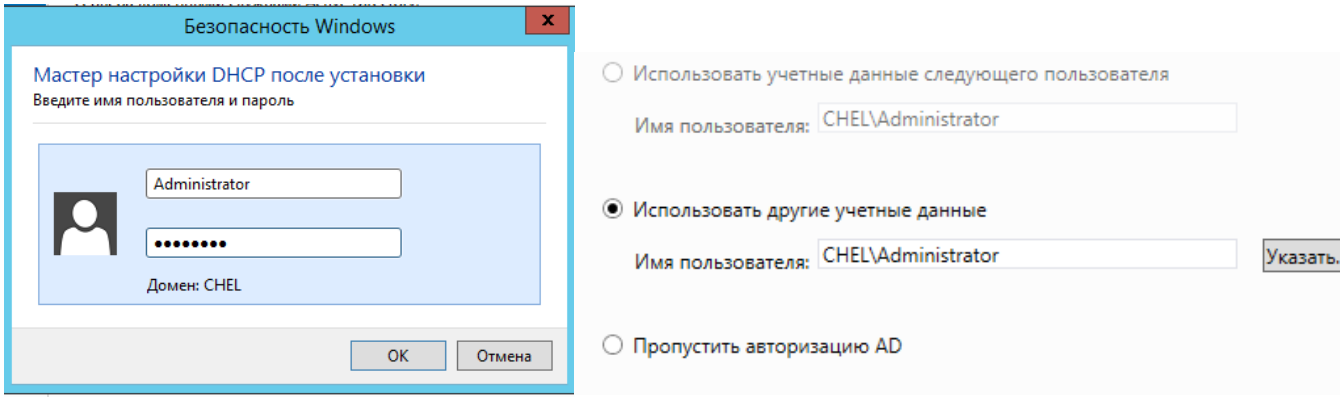
Служба DHCP. RRAS1, RRAS3

На серверах RRAS1, RRAS3 разверните роль для динамической выдачи IP-адресов и других сетевых настроек клиентам соответствующих сетей, и настройте пулы адресов в соответствии с таблицей 2. Учтите, что при получении IP-адреса компьютеры должны автоматически регистрироваться в базе DNS соответствующего домена.

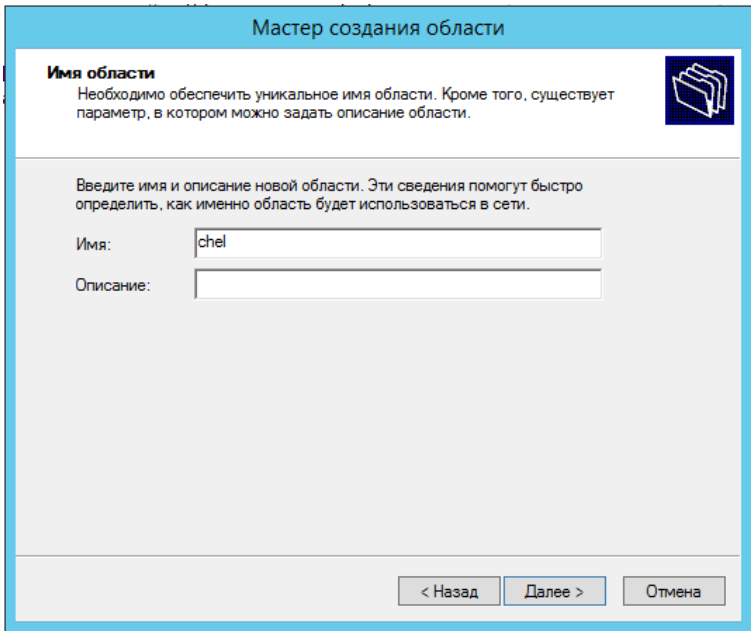
1. Открываем сервер RRAS3. ***Диспетчер серверов → Панель мониторинга → Добавить роли и компонент*** → Тип установки (***установка ролей или компонентов***) → Выбор сервера.
2. Выбираем роль – ***DHCP***.
3. Выбираем установить роль.
4. ***Настройка DHCP***. Для этого в диспетчере серверов выберете DHCP, нажмем на ссылку ***Подробнее***.



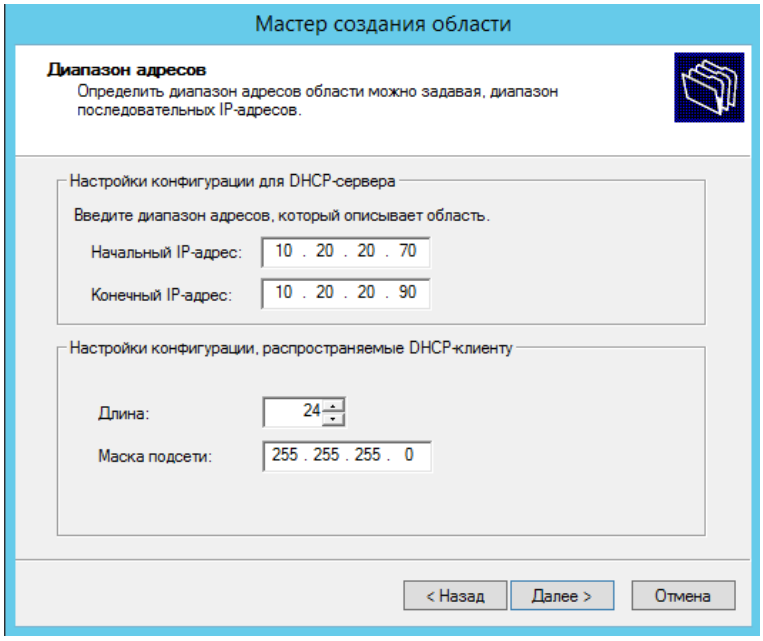
5. Выберете учетные данные



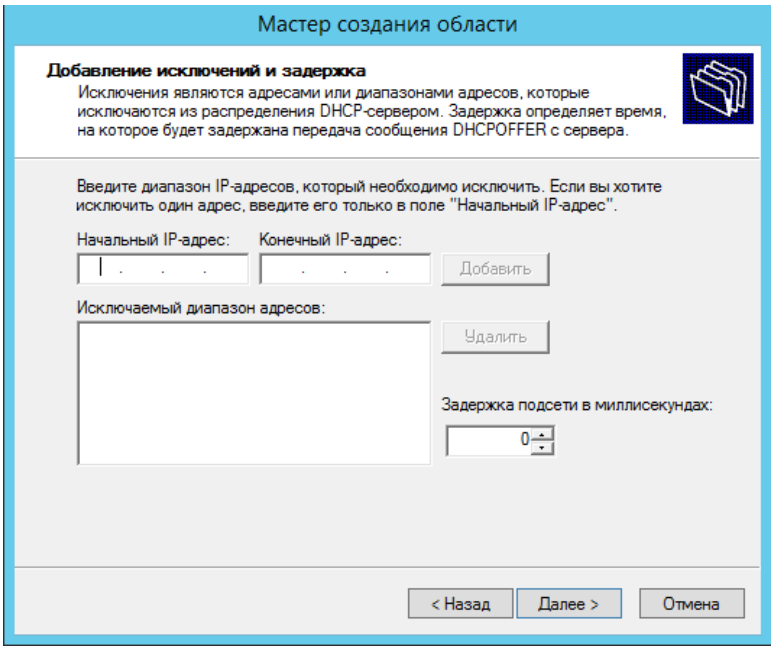
6. Нажать на IPv4 правой кнопкой и выбрать Создать область.
7. Введите имя области.



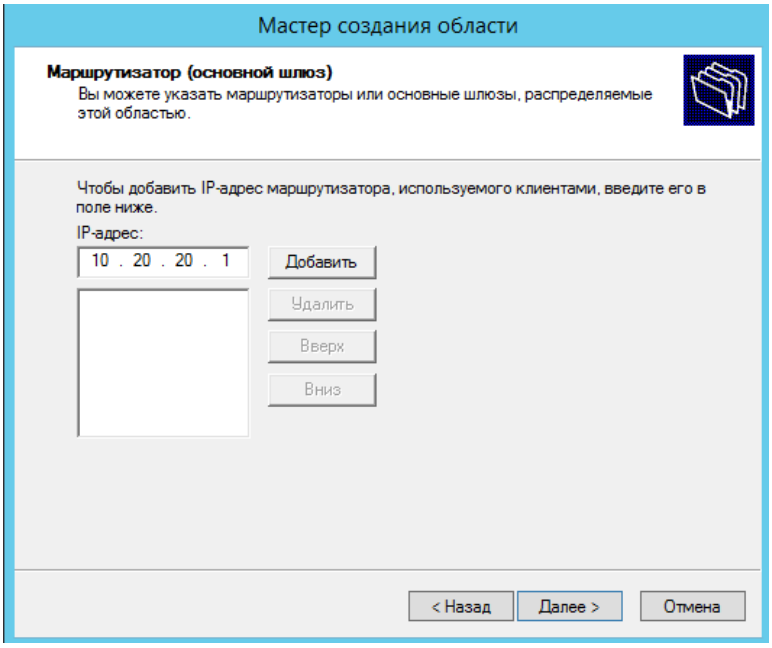
8. Введите диапазон адресов – 10.20.20.70-10.20.20.90.



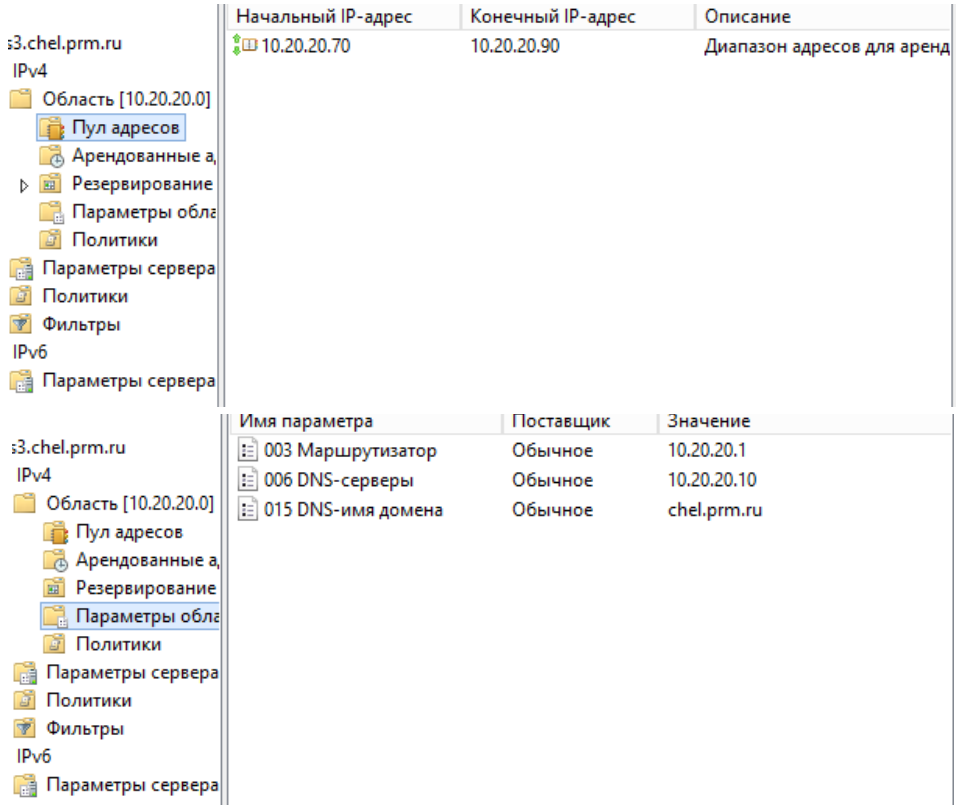
9. Введите адреса исключения, те которые раздавать нельзя, в домене chel их нет, в домене ural – 10.10.10.150. Затем нажимаем ***Добавить.***



10. При необходимости введите срок аренды, если данный параметр не указан, оставьте параметр по умолчанию. Добавьте адрес шлюза.



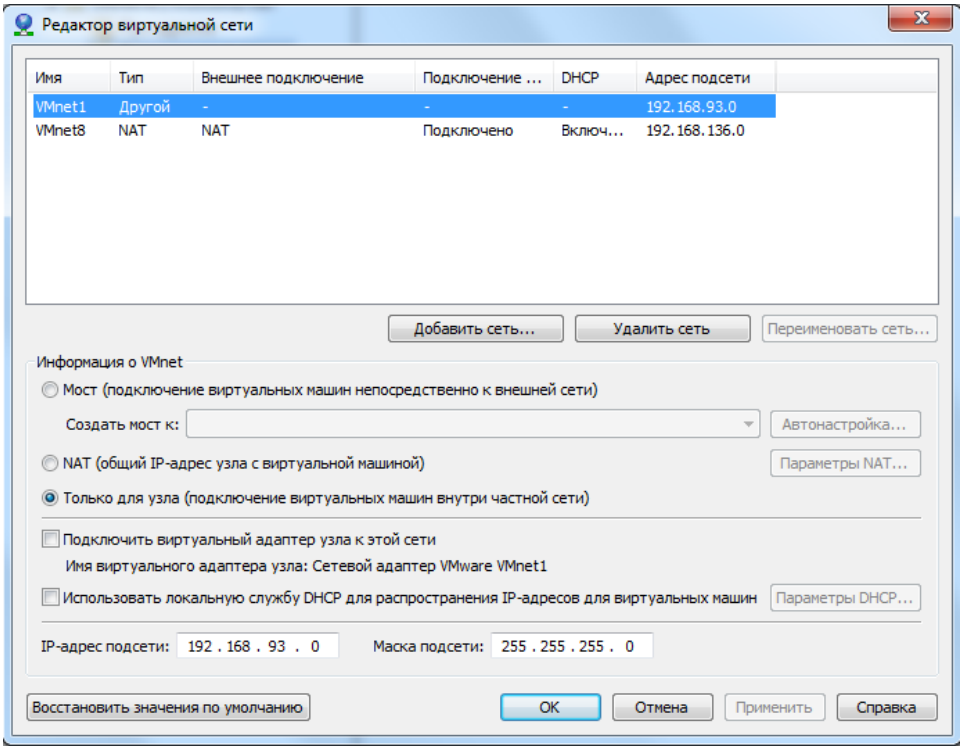
11. Подтвердить адрес – DNS. Затем активируйте область.
12. Проверьте параметры.



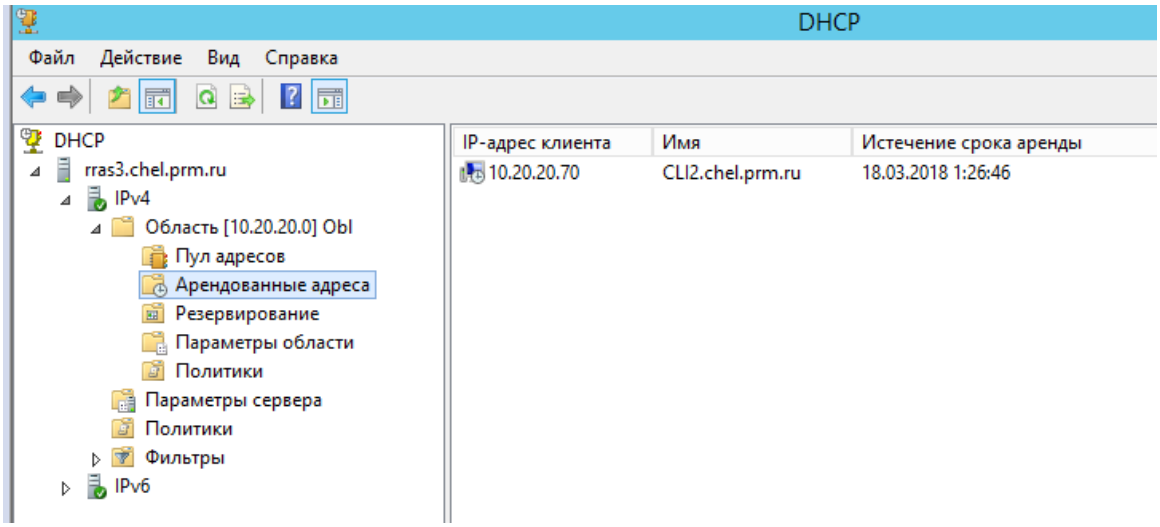
13. Аналогично настройте RRAS1.

Переведите клиентские компьютеры в обоих офисах в режим автоматического получения сетевых настроек. Убедитесь в правильности полученных настроек.

14. Настройте CLI2, если еще не настроили. Задайте имя добавьте, установите IP-адрес из той же подсети, в домен CHEL.
15. В VMWare открываем Правку → Редактор виртуальной сети снимаем галочки с нужных пунктов.

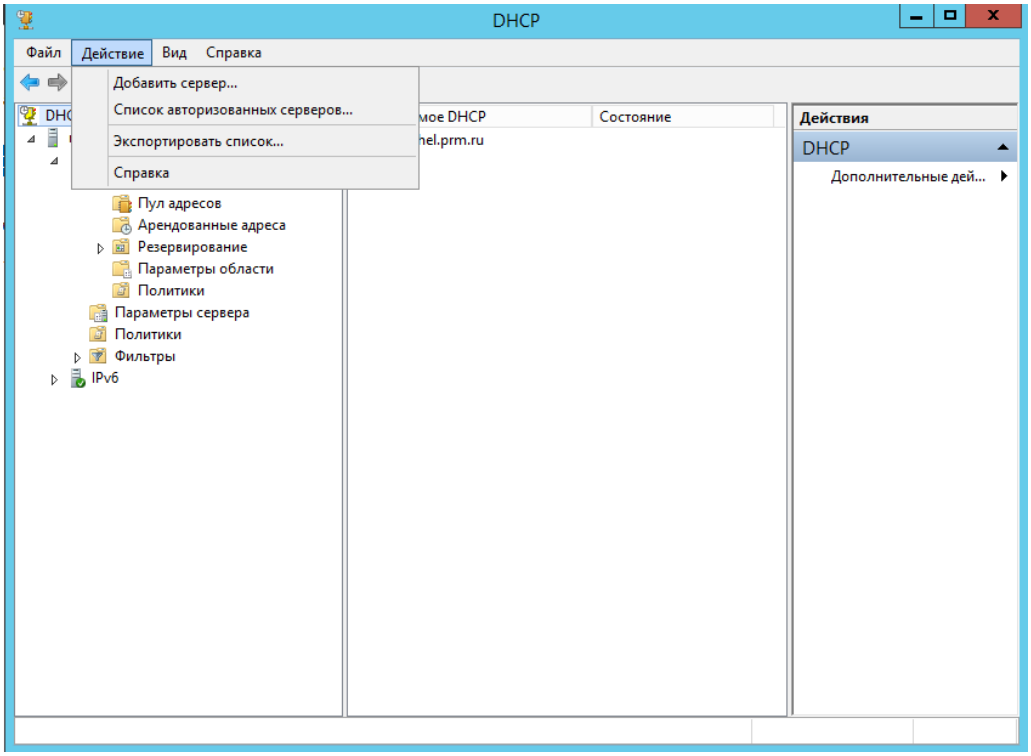


16. Зайдите в центр управления сетями → Изменение параметров адаптера → Свойство IPv4 → Свойство → Получать IP-адрес автоматически.
17. На сервере RRAS в DHCP сервере в арендованных адресах появится нажпись.

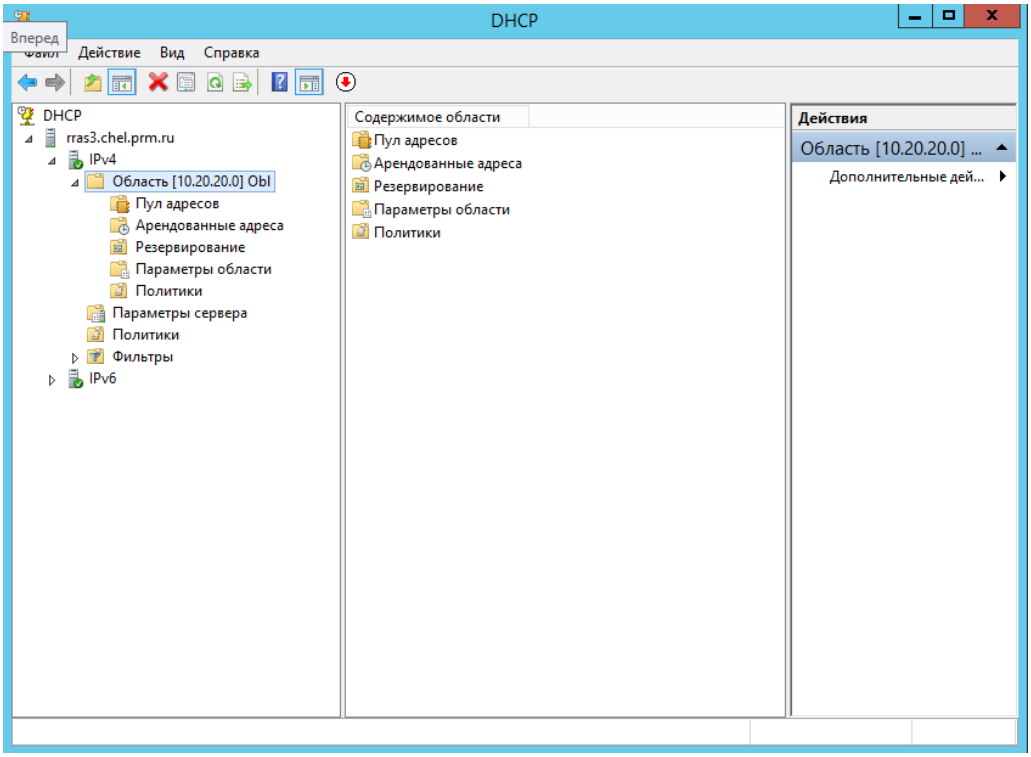


Авторизация сервера DHCP

Действие Список авторизованных серверов → Ввести Ip-адрес → Авторизовать



Выбираем область Деактивировать → Активировать.

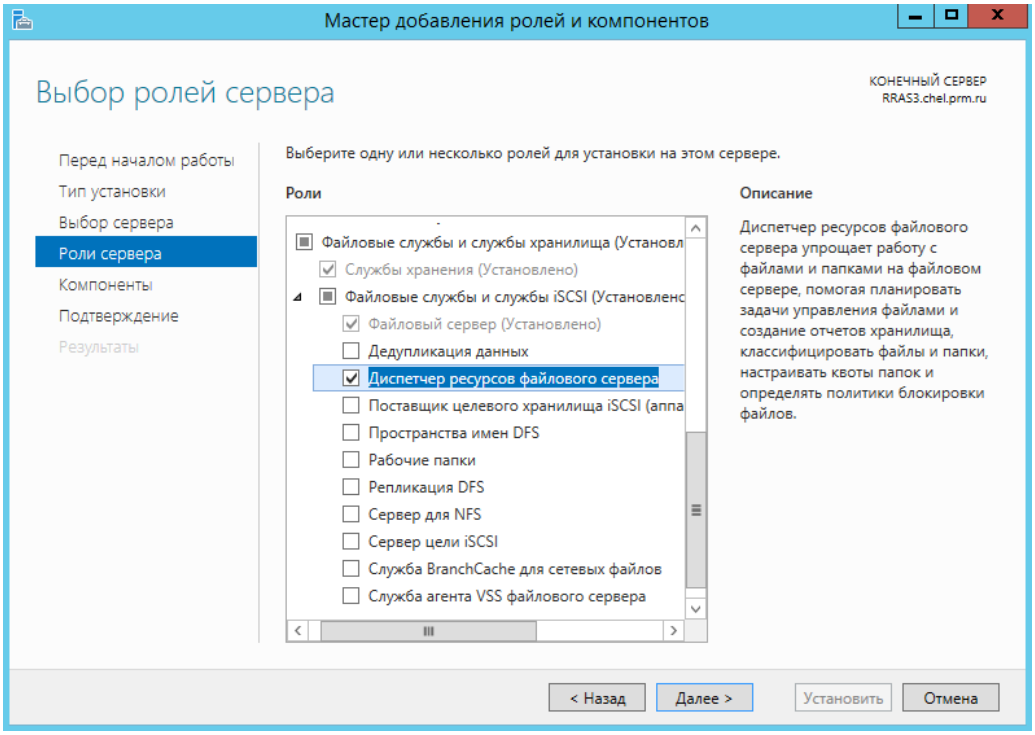


Перезапустить пользователя или компьютер.

Настройка служб управления файловыми хранилищами

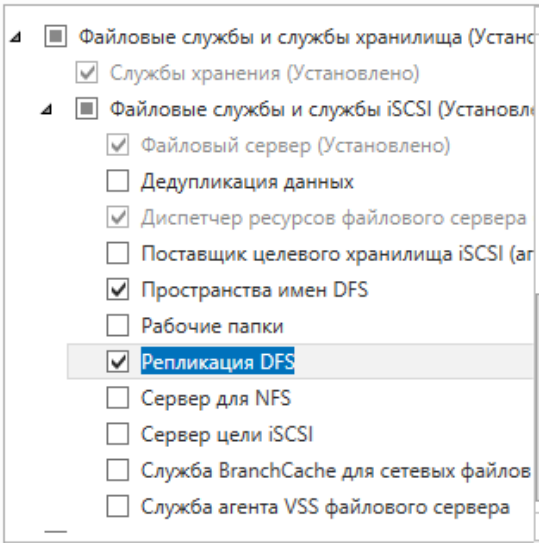
Установите роль файлового сервера на RRAS3.

1. ***Диспетчер серверов → Панель мониторинга → Добавить роли и компонент*** → Тип установки (***установка ролей или компонентов***) → Выбор сервера.
2. Выбираем роль – ***Файловые службы и службы хранилища***, а также ***Файловый сервер***, если он не установлен и ***Диспетчер ресурсов файлового сервера***.



В домене на серверах FS1 и FS2 установите соответствующие роли для организации распределенной файловой системы.

1. На сервере RRAS3 (FS1) откройте ***Диспетчер серверов → Панель мониторинга → Добавить роли и компонент*** → Тип установки (***установка ролей или компонентов***) → Выбор сервера.
2. Выбираем роль – ***Файловые службы и службы хранилища***, а также ***Пространство имен DFS*** и ***Репликация DFS***.

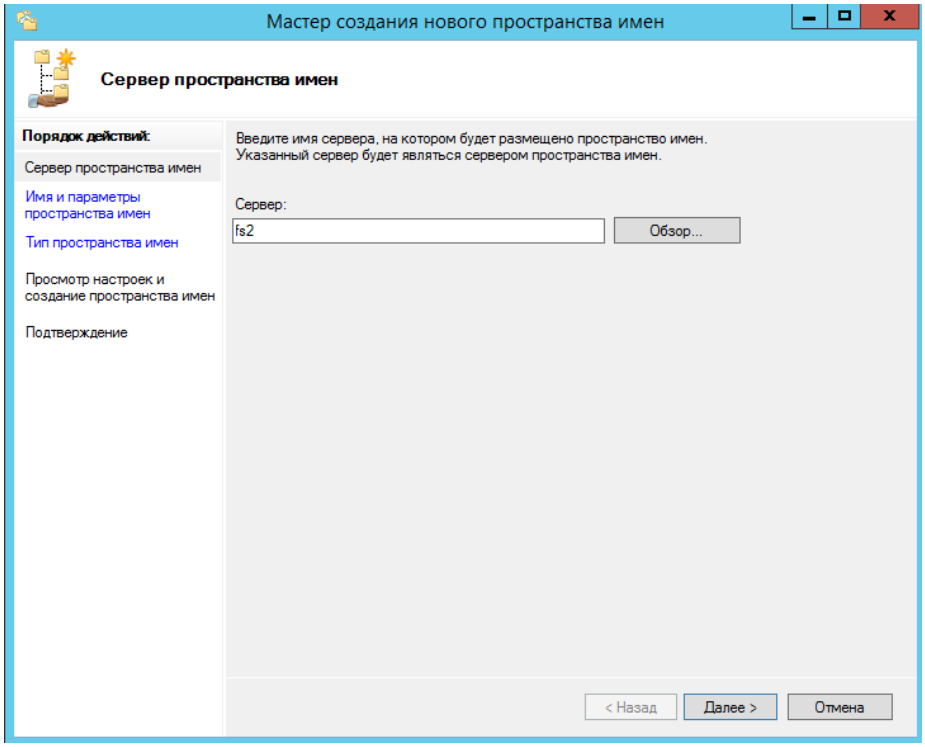


3. Два данных компонента установите на сервер FS2.

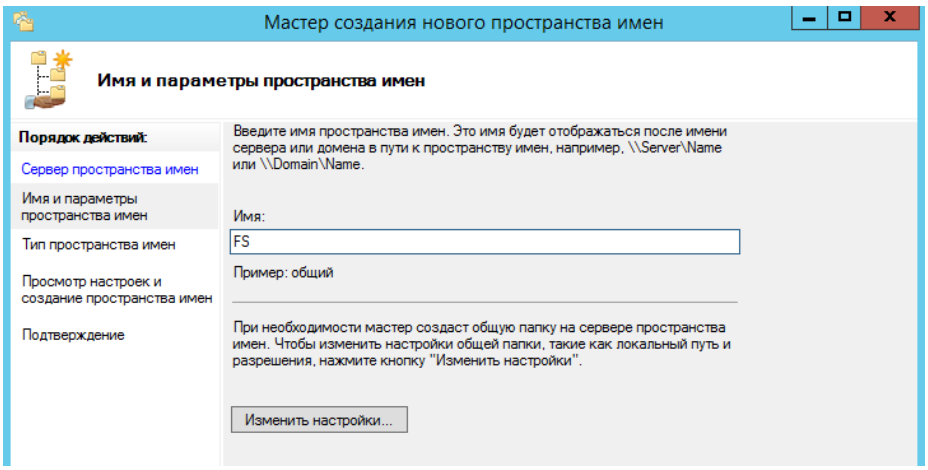
– *Создайте папку C:\Share на сервере FS1 и папку D:\Share на сервере FS2. Внутри созданных папок создайте папки Man_share и Work_share.*

– *Создайте корень DFS с именем FS. Данный корень должен поддерживаться обоими серверами. Создайте под этим корнем папку с именем Share, ссылающуюся на сетевые директории с тем же именем (Share) созданные вами ранее на каждом сервере. Обеспечьте всем пользователям домена доступ к этой папке на запись. Настройте репликацию между папками средствами DFS. Установите жесткое ограничение 1 Гб на размер папки FS\Share.*

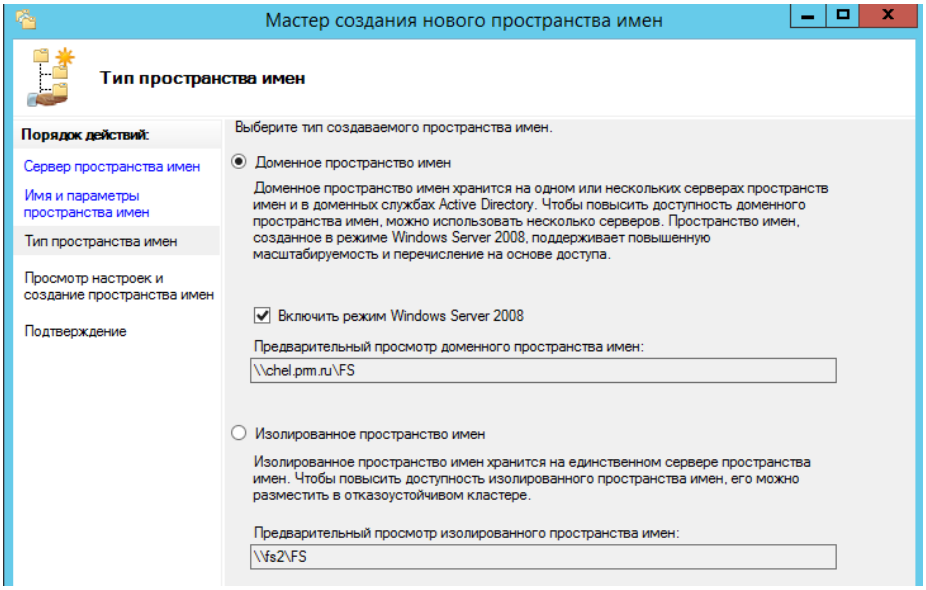
1. На сервере FS2 откроем ***Диспетчер серверов → Средства → Управление DFS → Пространства имен → Новое пространства имен***.
2. Введите имя сервера, на котором будет храниться пространства имен



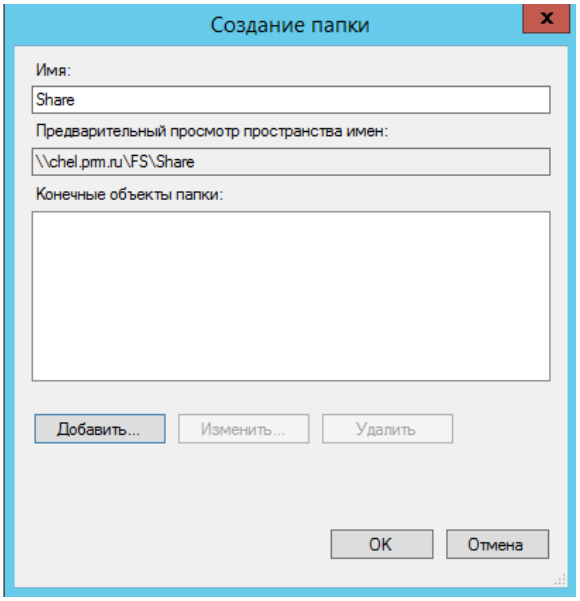
3. Введите имя пространства имен (создайте корень) – ***FS***.



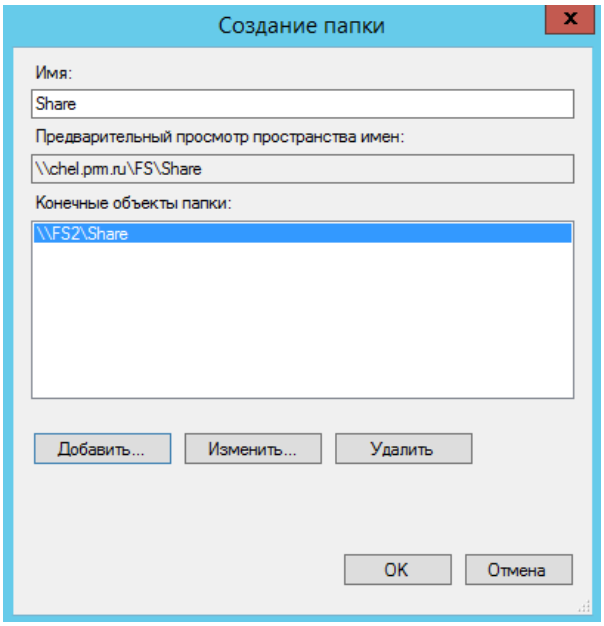
4. Выберете тип пространства имен – ***Доменное пространство имен***.



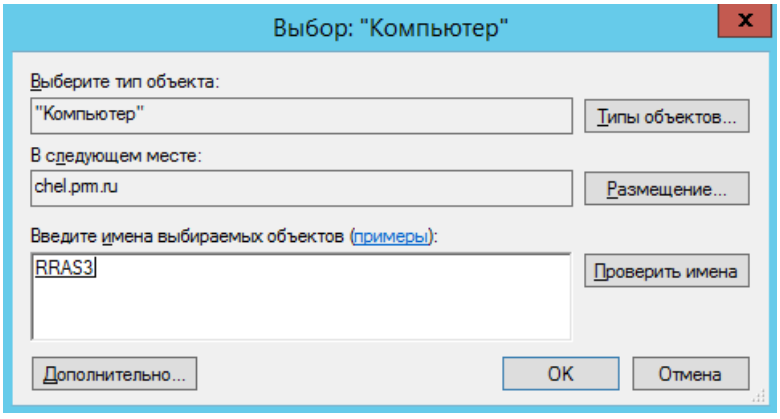
5. Выбираем пространства имен ***FS***.
6. Выбираем ***Создать папку. Вводим имя папки.***



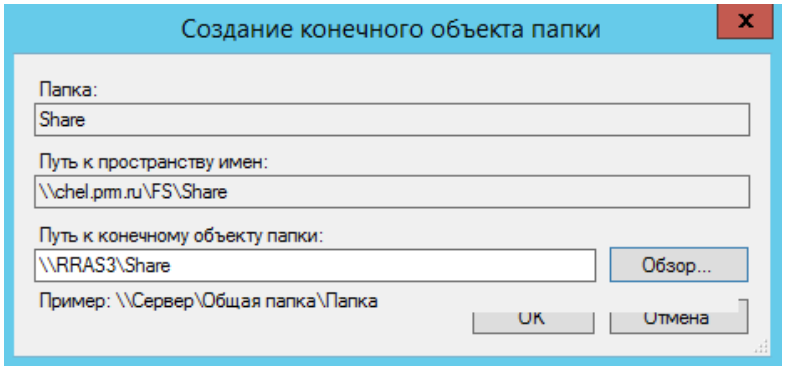
7. Добавим конечные объекты папки для этого нажмем на кнопку ***Создать***, нажмите на кнопку ***Обзор*** → Новая общая папка.
8. Вводим имя общего ресурса и локальный путь до папки, для этого требуется нажать на ***Обзор***. Подтвердите создание общих ресурсов. Затем добавим к данной папке еще одну конечную папку



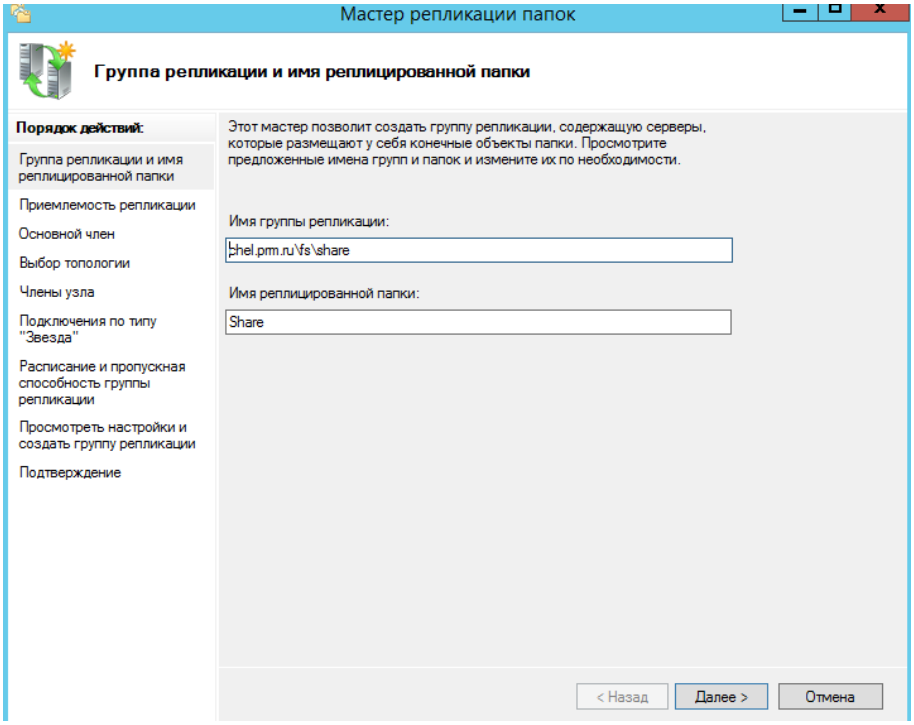
9. Сделаем ссылку на вторую директорию для этого щелкнем правой кнопкой мыши по папке и выберем ***Добавить конечный объект к папке***, нажмите на кнопку ***Обзор*** → ***Обзор*** для того чтобы выбрать другой сервер. Вводим имя сервера и подтверждаем выбор.



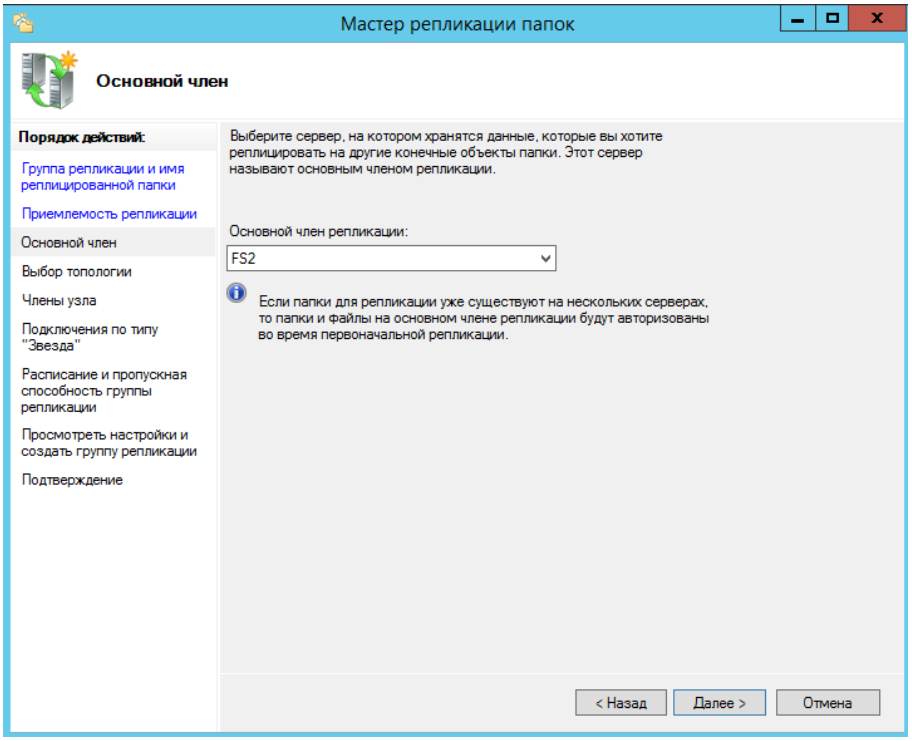
10. Нажать на кнопку Новая общая папка и вводим имя общего ресурса, локальный путь и права (как указано в задании запись для всех пользователей).
11. Подтверждаем создание нового конечного объекта.



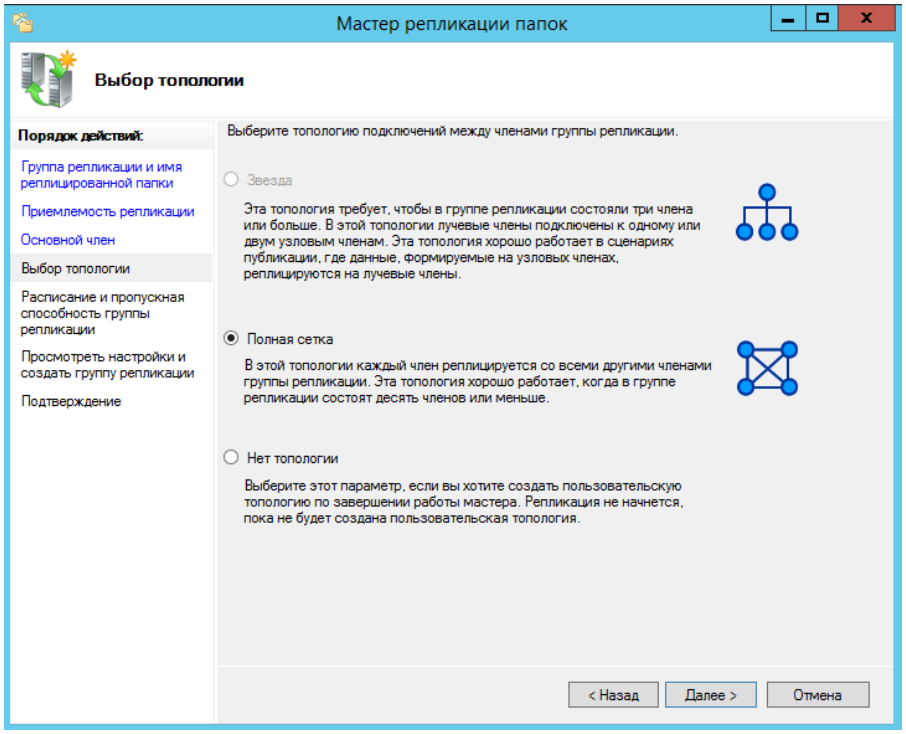
12. Подтвердите создание группы репликации.



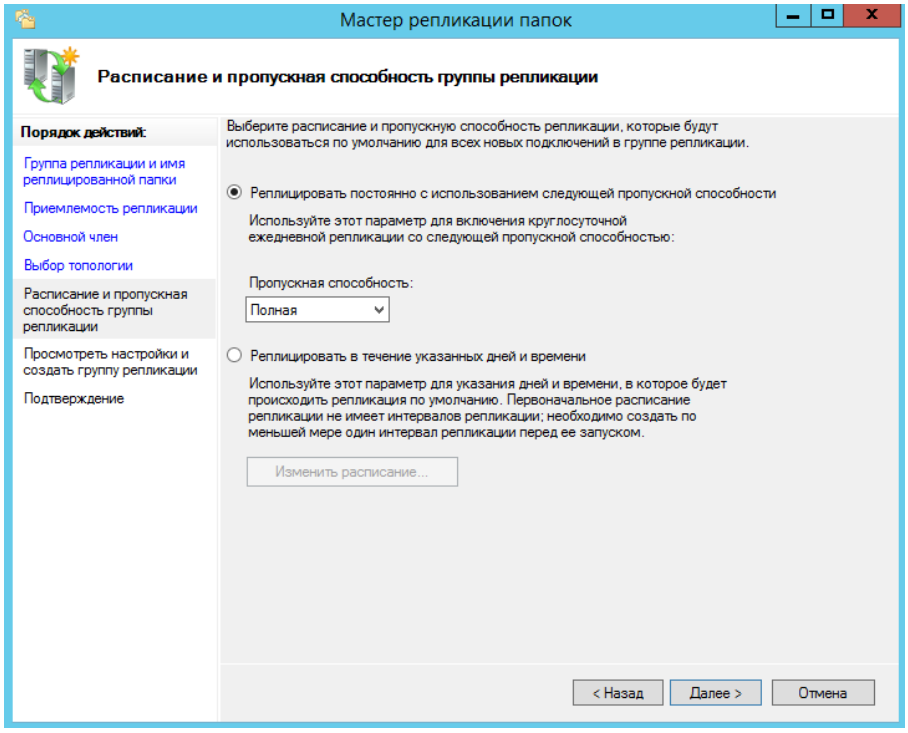
13. Выберете Основной член репликации (<u>в задании он не указан, по этому выбирается по желанию</u>).



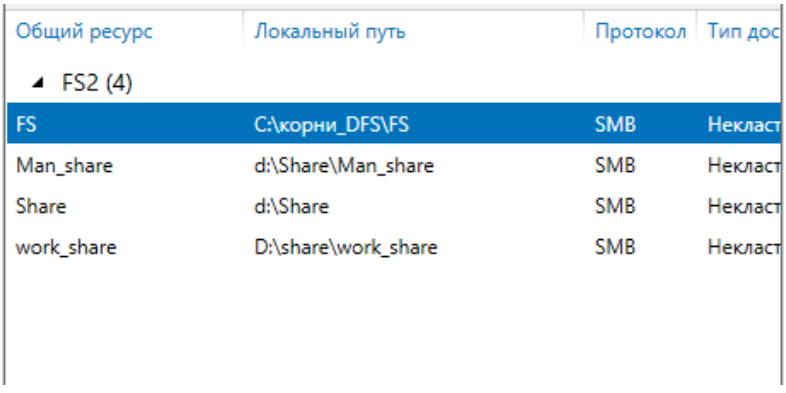
14. Выберете тип топологии



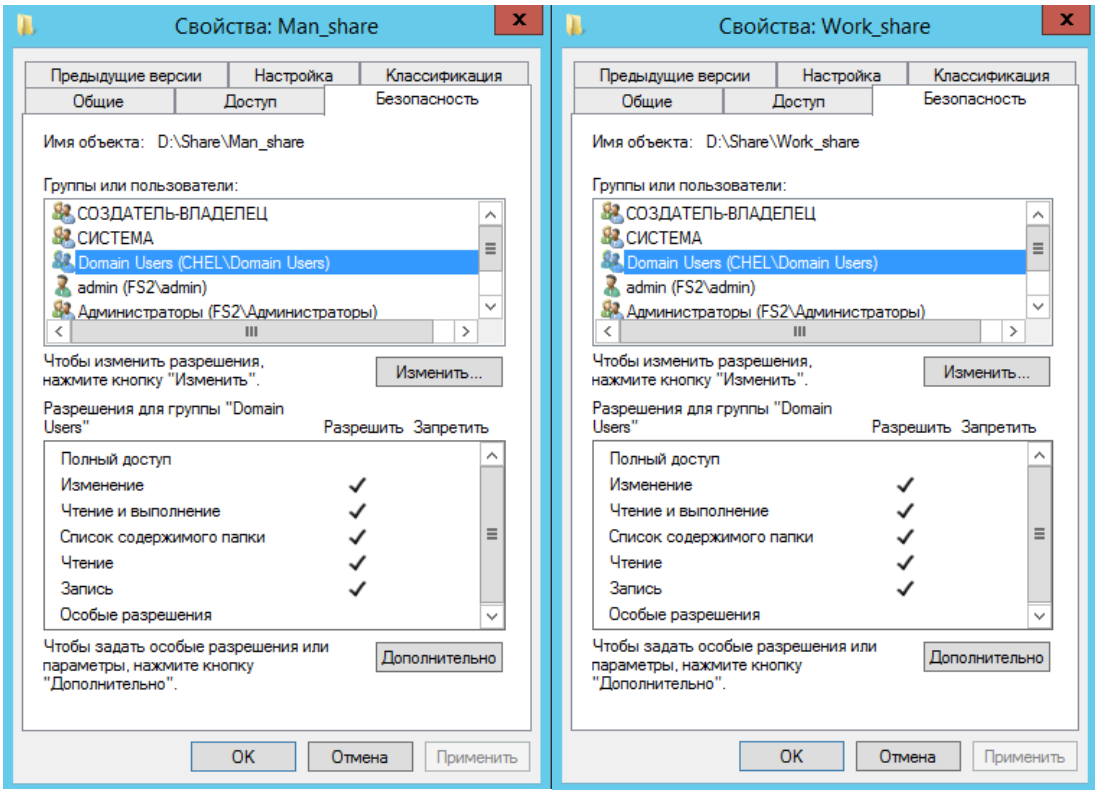
15. Выберете расписание и пропускную способность репликации и подтвердите создание.



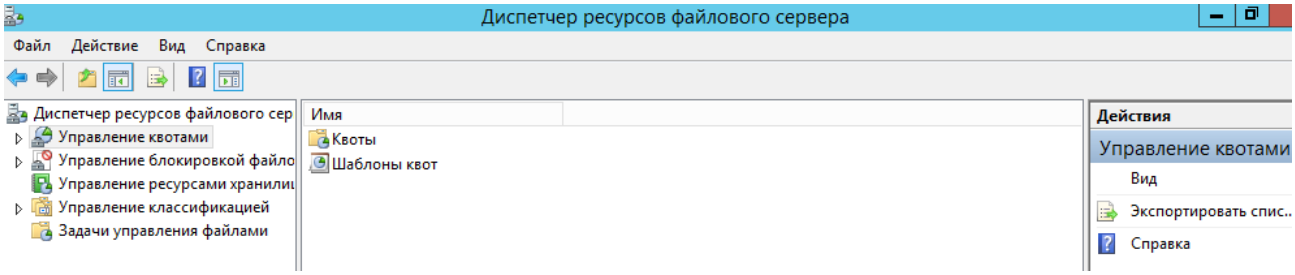
16. В созданной репликации выберете одну из папок, зайдите в свойства и на вкладку дополнительно.
17. Зайдите в ***Диспетчер серверов*** → Файловый сервер → Общие ресурсы.
18. Создайте в общей папки ресурсы Man_share и Work_share.



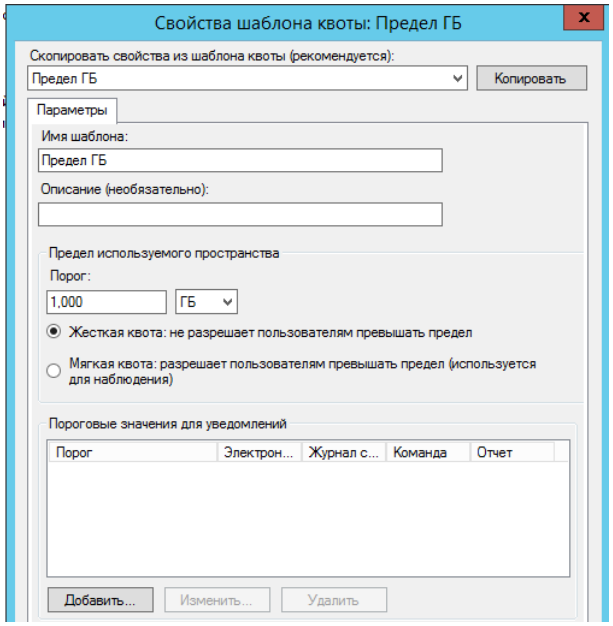
19. Добавьте права на эти папки у пользователей домена на каждом сервере для этого заходим в свойство папки и добавляем группу прав пользователи домена и выставляем права на запись.



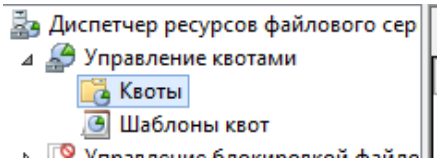
20. Зайдите в ***Диспетчер сервера***, откройте в ***Средства***, выберете ***Диспетчер ресурсов файлового сервера***.



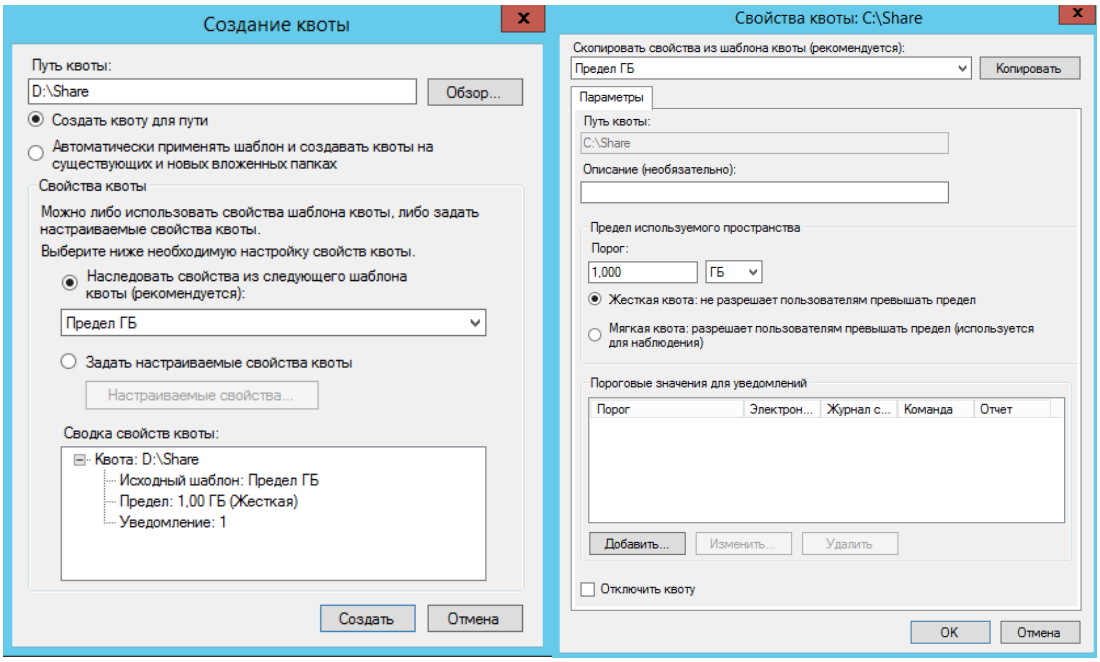
21. Откройте ***Управление квотами → Шаблоны квот → Создать шаблон квоты***.



22. Перейдите в квоты.

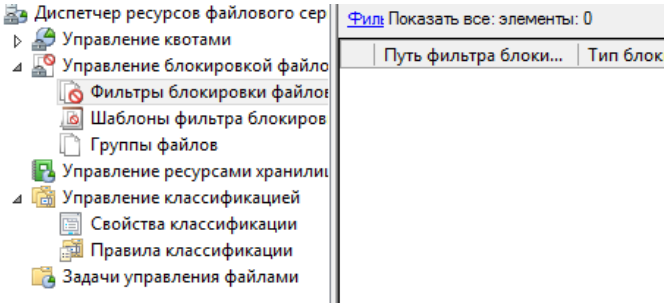


23. Выберете создать квоту. Аналогично создайте квоту на втором файловом сервере.

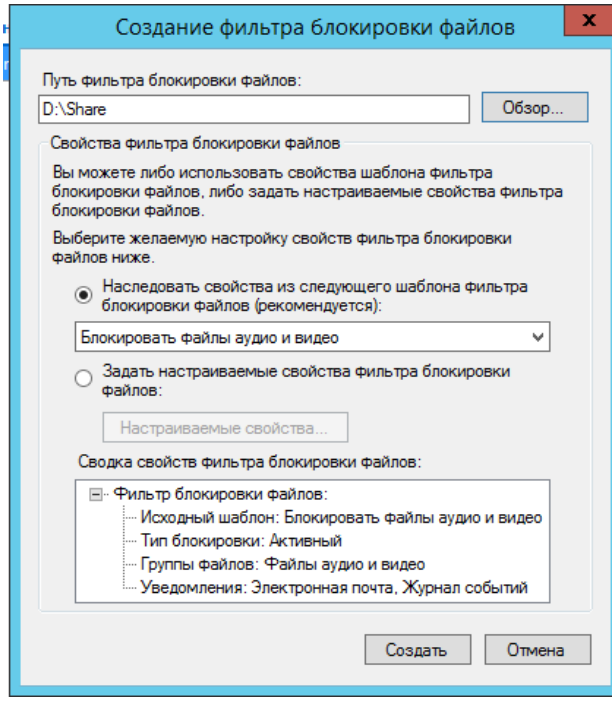


Запретите хранение аудио- и видео-файлов на серверах FS1 и FS2.

1. Зайти в фильтры блокировки файлов.



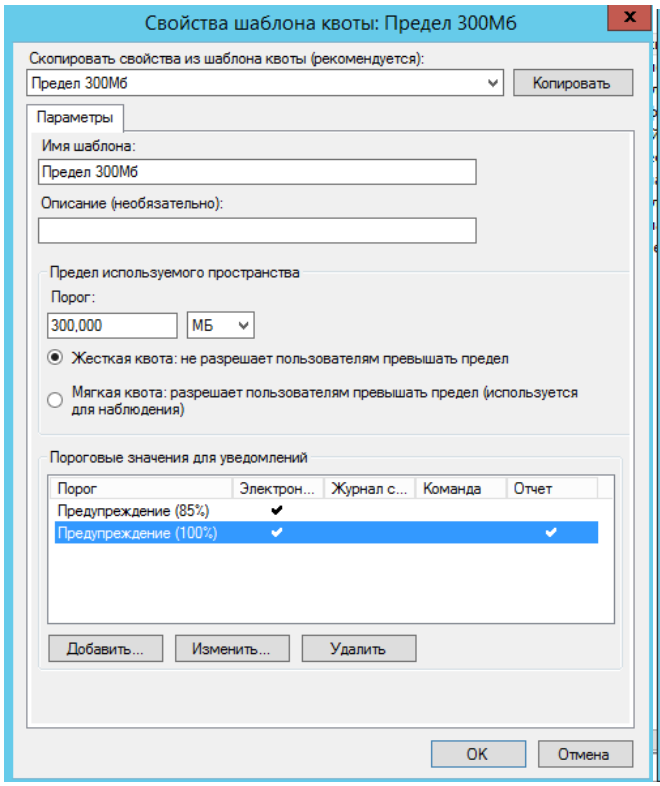
2. Создать новый фильтр.

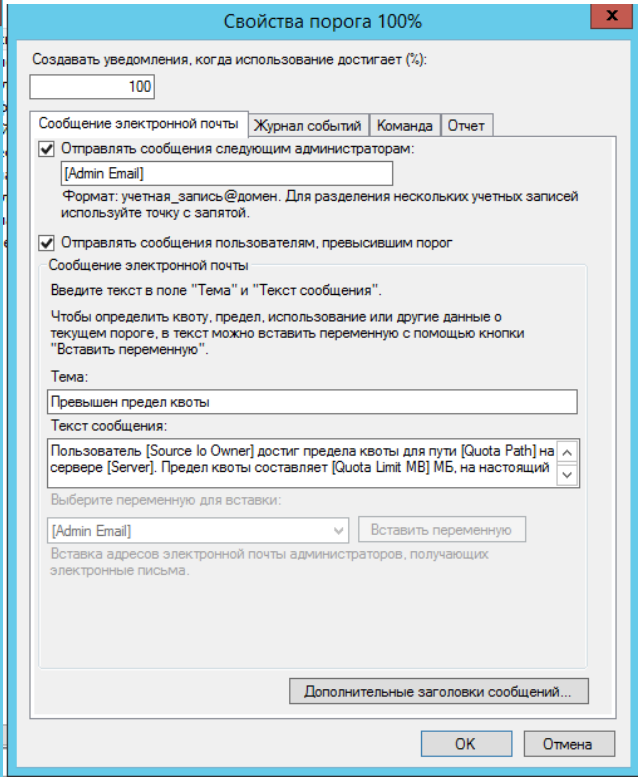


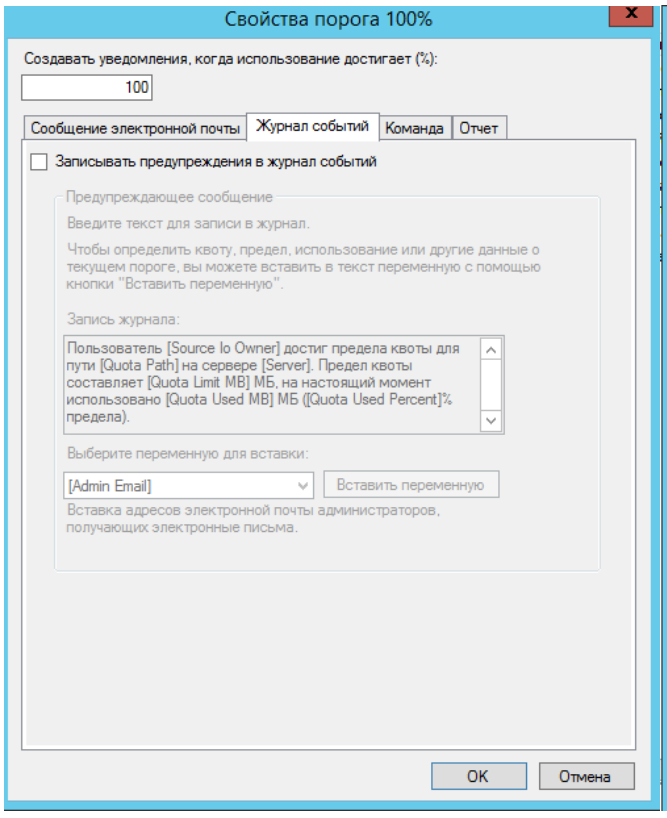
3. Аналогично настройте второй сервер.

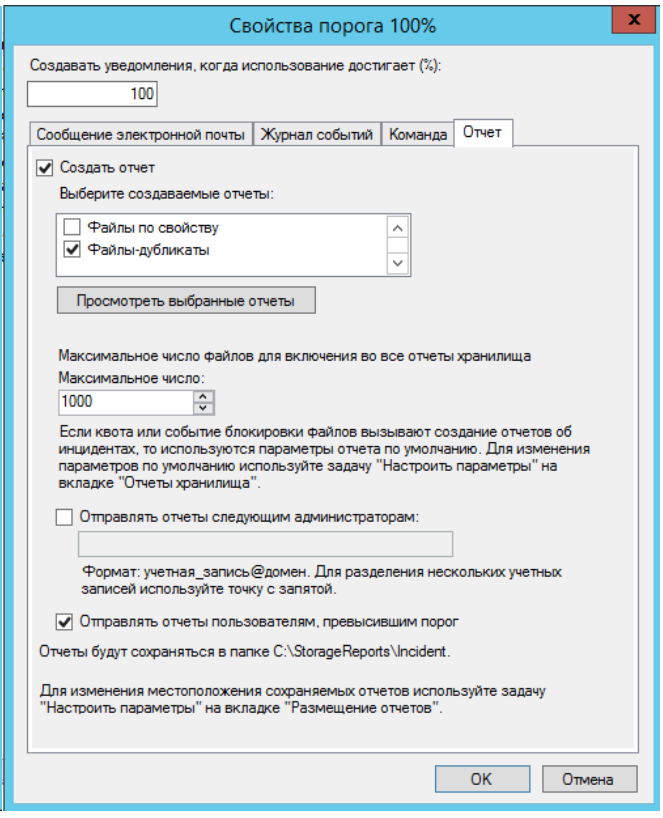
Установите на серверах FS1 и FS2 файловые квоты согласно таблице 4.

1. Зайдите в ***Шаблоны квот***.
2. Создайте жесткую квоту на 300 Мб.

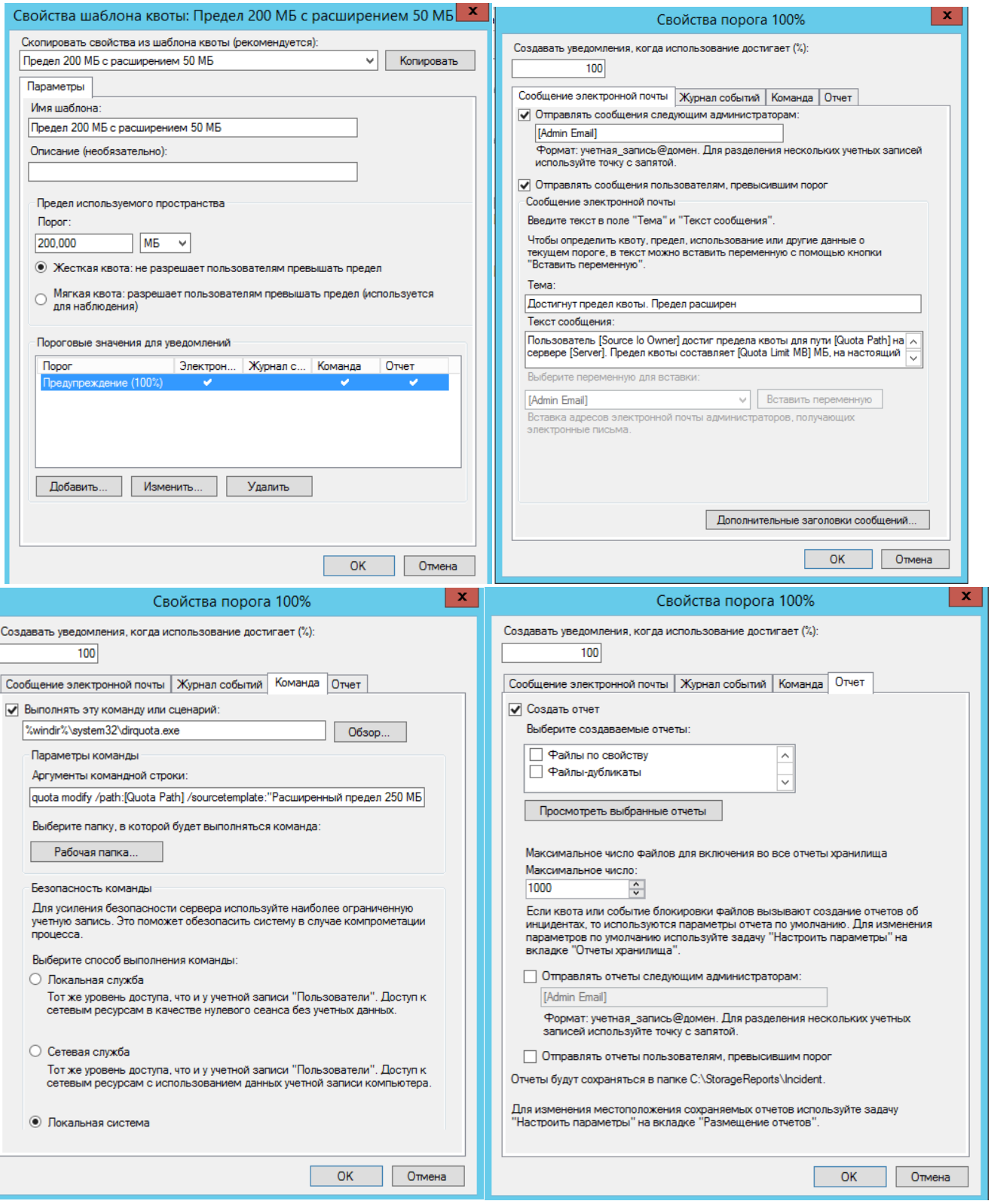




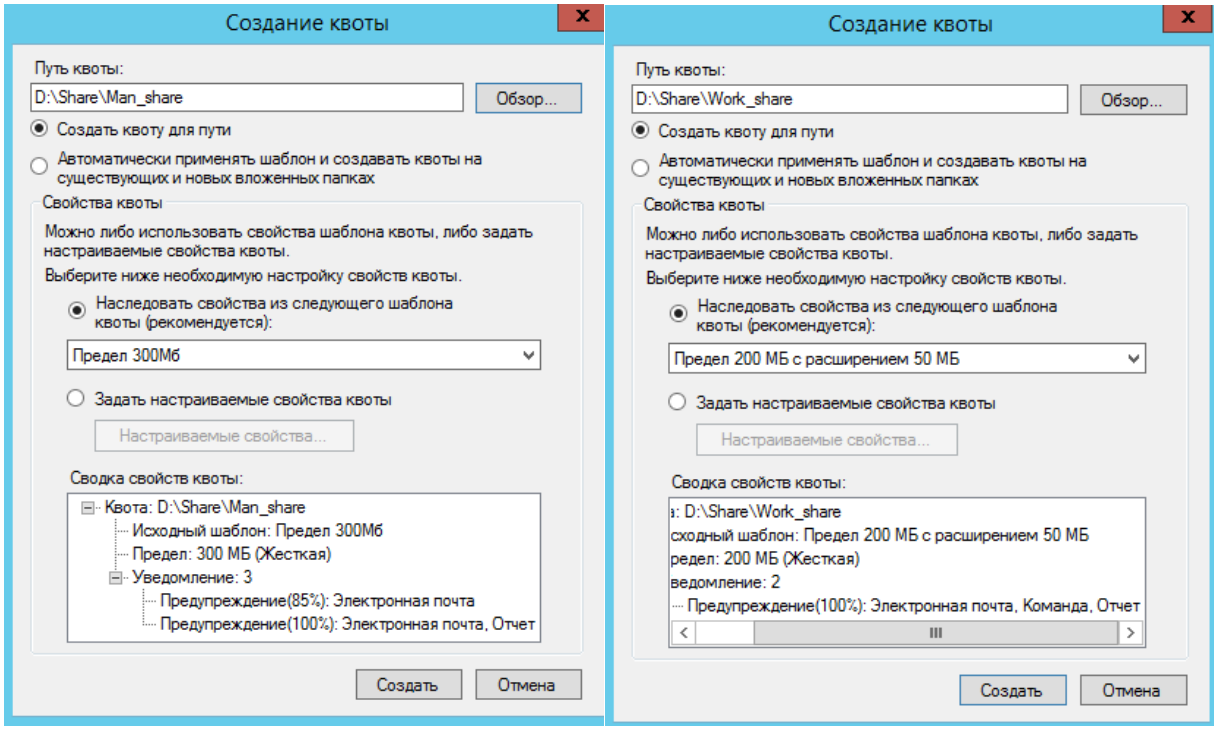




3. Измените квоту ***Предел 200Мб с расширением 50Мб***



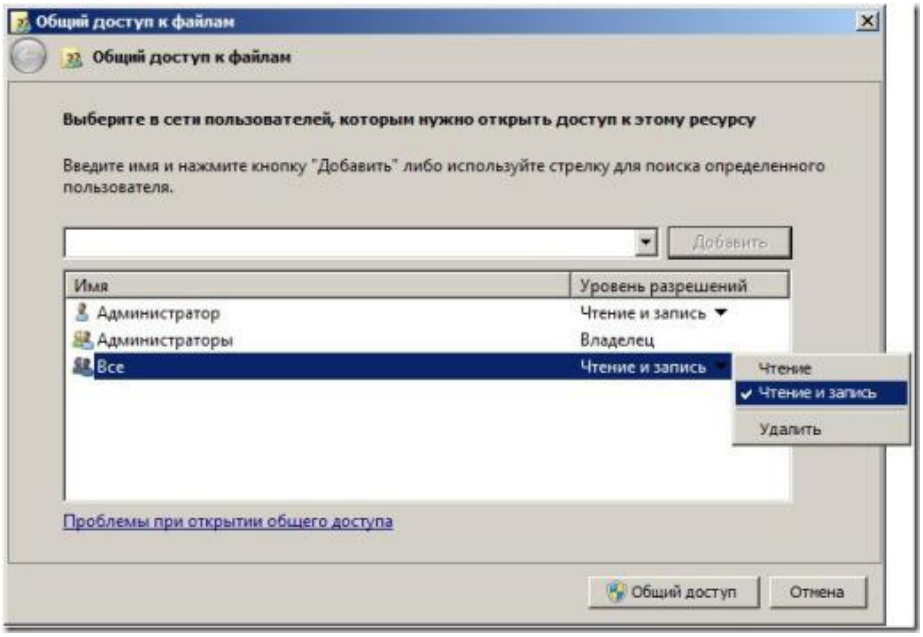
4. Зайдите в ***Квоты → Создать квоту*** и назначьте папкам соответствующие по таблицу квоты.



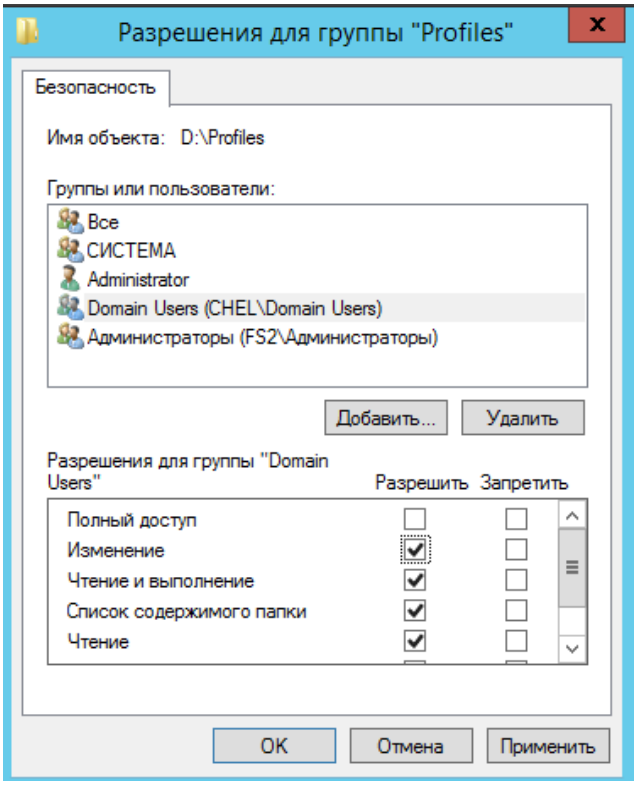
Профили в домене CHEL

В домене chel.prm.ru для членов группы Prepod настройте перемещаемые профили. Для хранения профилей создайте папку D:\Profiles на сервере FS2.
Проследите за тем, чтобы пользователь имел полный доступ к файлам своего профиля на сервере и не имел никакого доступа к файлам профилей других пользователей.

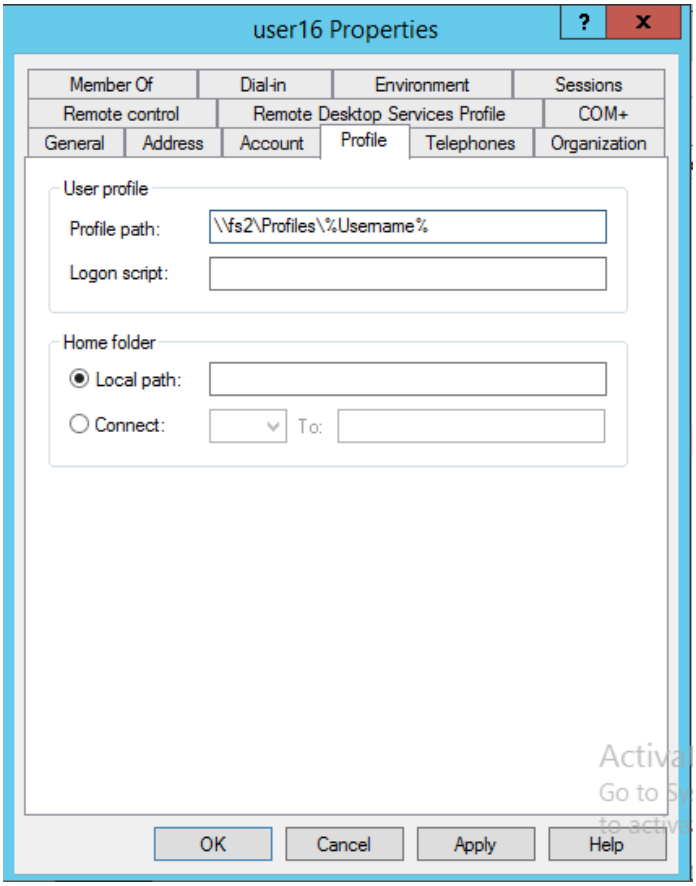
1. Создайте на файловом сервере FS2 папку D:\Profiles, в которой будут храниться перемещаемые профили. Следует предоставить папку в совместное использование и назначить сетевой папке разрешения на общий доступ и разрешения NTFS. Для этого, находясь в Проводнике, щелкните правой кнопкой мыши по созданной папке, в контекстном меню выберите *Свойства*, перейдите на закладку *Доступ* и щелкните кнопку *Общий доступ.*



2. В появившемся окне выберите группу *Все*, нажмите на кнопку *Добавить*, в поле *Уровень разрешений* выберите пункт контекстного меню *Чтение и запись* и нажмите на кнопку *Общий доступ*. Закончите настройку, щелкнув кнопку *Готово*.
3. Далее перейдите на вкладку Безопасность и установите разрешения NTFS, так чтобы доменная группа *Пользователи домена* имела разрешения на запись, как показано на рисунке.



4. Теперь все готово для настройки перемещаемых профилей для учетных записей пользователей. Находясь в консоли *Active Directory – пользователи и компьютеры*, откройте свойства учетной записи пользователя, перейдите на закладку *Профиль* и в поле *Путь к профилю* введите сетевой путь к подпапке пользователя, которая будет создана в папке, хранящей перемещаемые профили.
   Профиль нужно прописать для пользователей группы Prepod, то есть для user16-user30.

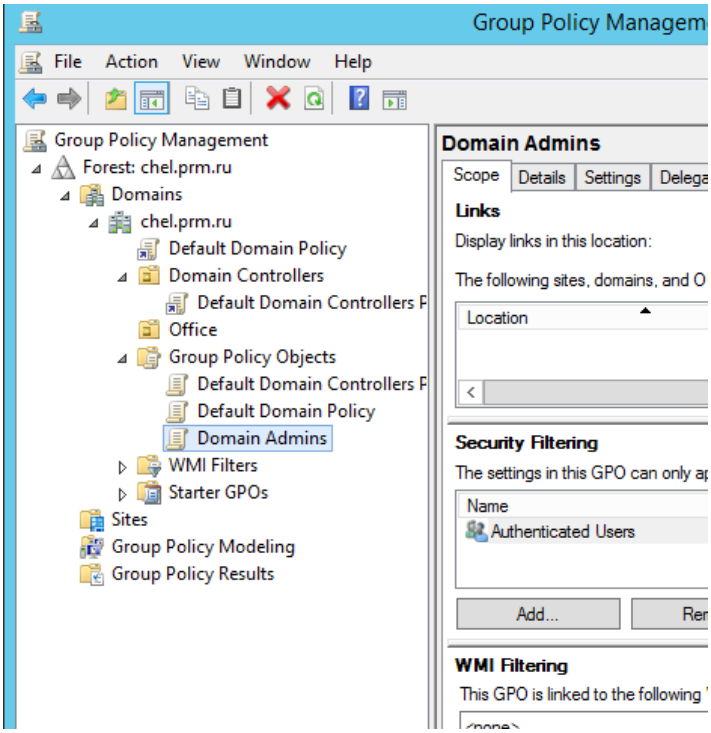


Групповая политика

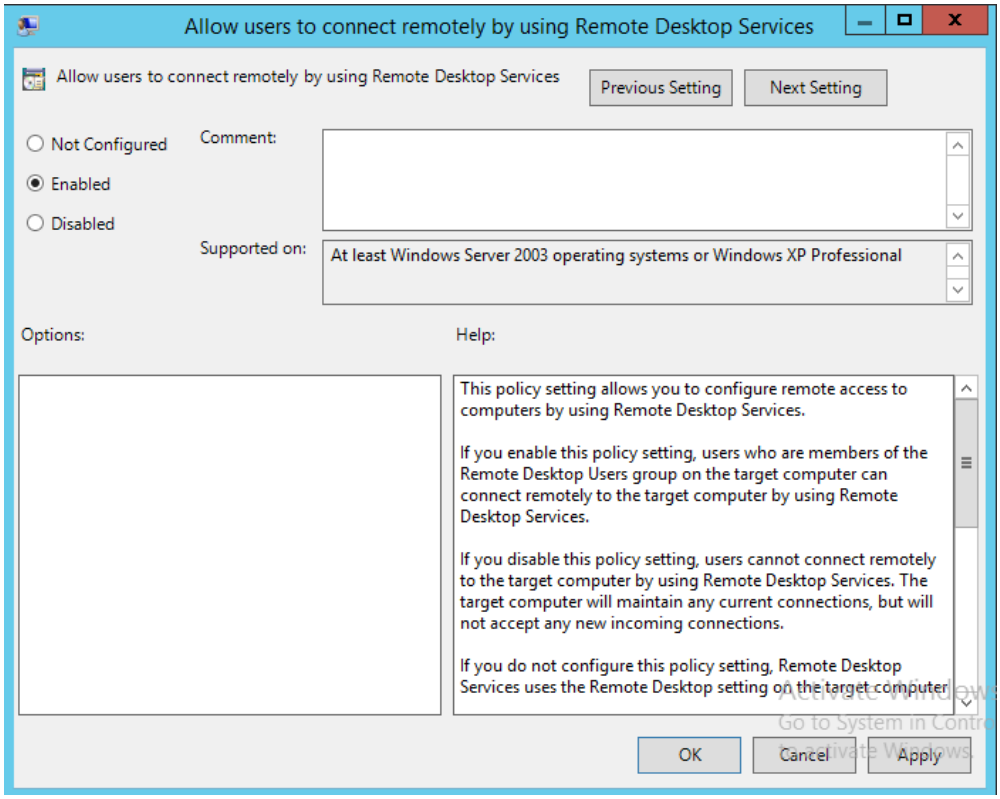
В домене chel.prm.ru настройте групповые политики, обеспечивающие выполнение следующих условий:

а) удаленный рабочий стол включен на всех компьютерах домена и доступен для администраторов домена;

1. ***На сервере 2 Диспетчер серверов → Менеджер групповой политики*** → Открываем сервер CHEL затем выбираем групповую политику Администраторов домена

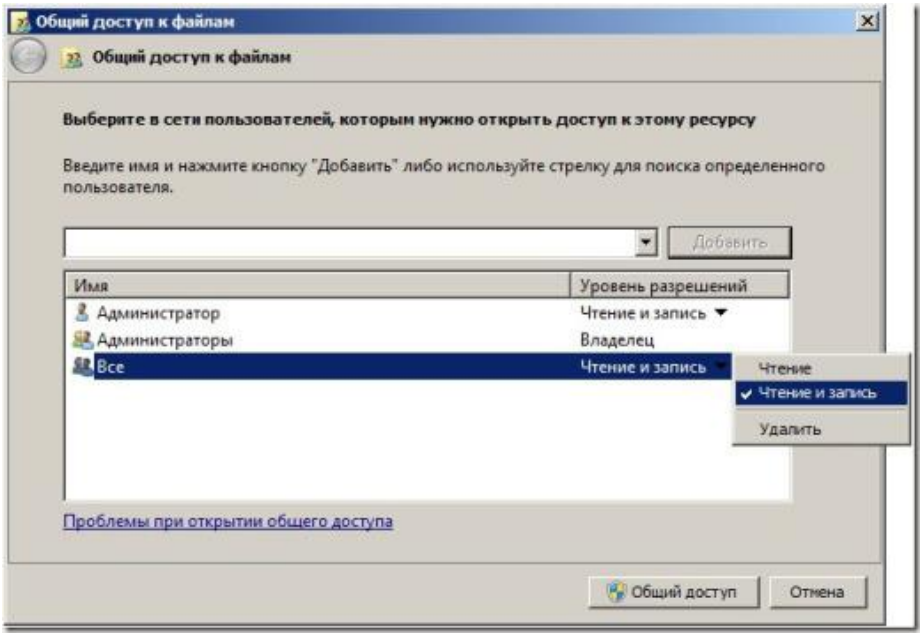


2. Из контекстного меню выбрать изменить → ***Конфигурация компьютера*** (Computer configuration) → ***Политики*** (Policies) → ***Административные шаблоны*** (Administrative Templates) → ***Компоненты Windows*** (Windows Components) → ***Службы удаленных рабочих столов*** (Remote desktop settings) → ***Узел сеансов удаленных рабочих столов*** (Remote desktop session host) → ***Подключения*** (Connections) → ***Разрешать удаленное подключение с использованием служб удаленных рабочих столов*** (Allow users to connect remotely using Remote Desktop Services) → Включить

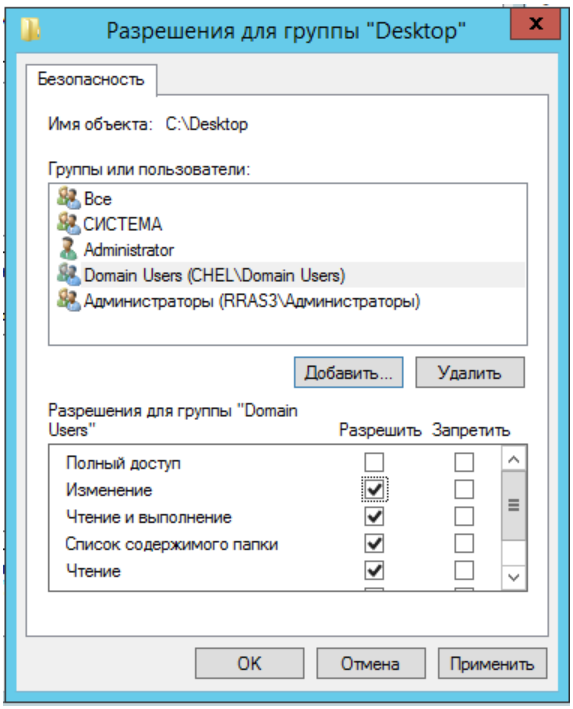


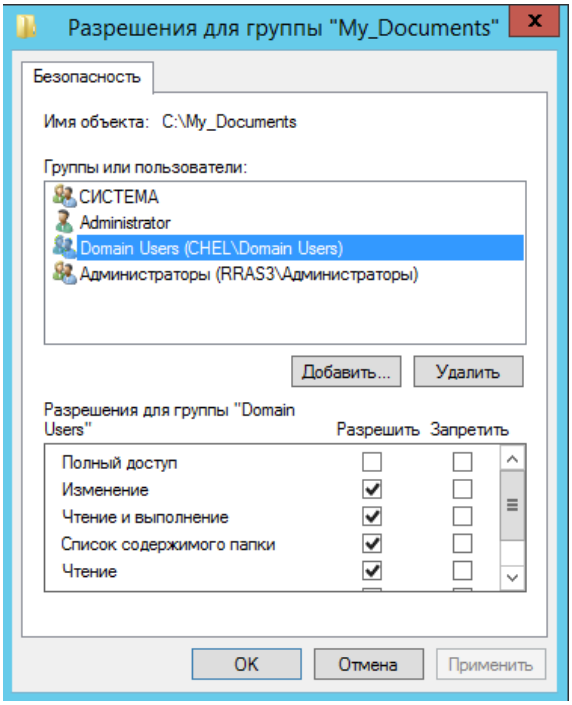
б) для всех пользователей домена включено перенаправление папок Desktop и My Documents на файловый сервер FS1 в специально созданные для этого папки;

1. На сервере FS1 создать папки Desktop и My_Documents.
2. Находясь в Проводнике, щелкните правой кнопкой мыши по созданной папке, в контекстном меню выберите *Свойства*, перейдите на закладку *Доступ* и щелкните кнопку *Общий доступ.*

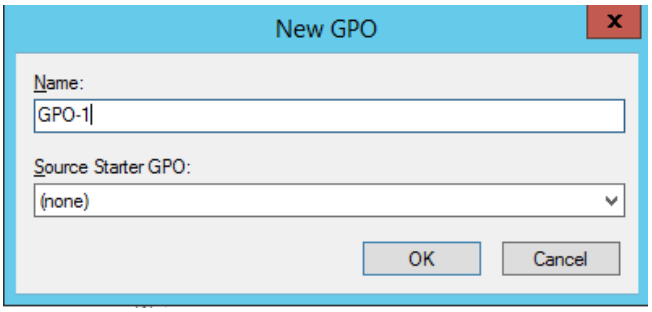


3. В появившемся окне выберите группу *Все*, нажмите на кнопку *Добавить*, в поле *Уровень разрешений* выберите пункт контекстного меню *Чтение и запись* и нажмите на кнопку *Общий доступ*. Закончите настройку, щелкнув кнопку *Готово*.
4. Далее перейдите на вкладку Безопасность и установите разрешения NTFS, так чтобы доменная группа *Пользователи домена* имела разрешения на запись, как показано на рисунке.

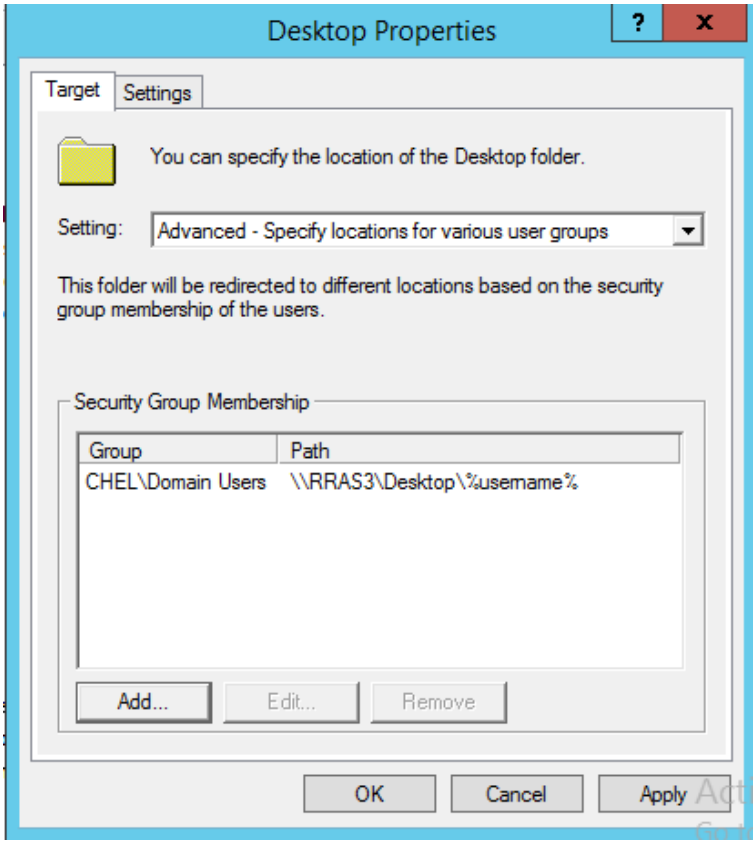




5. На сервере DC2 ***Диспетчер серверов*** → ***Менеджер групповой политики*** выбираем домен CHEL из контекстного меню выбираем ***Создать GPO в домене и связать их***.
6. Задать имя групповой политики.



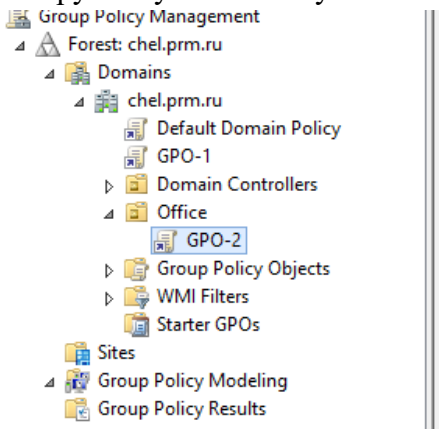
7. В контекстном меню выбрать ***Изменить***.
8. ***Конфигурация пользователя*** (User Configuration) → ***Политики*** (Policies) → ***Настройка Windows*** (Windows Settings) → ***Перенаправление папок*** (Folder Redirection) → Desktop → Свойства



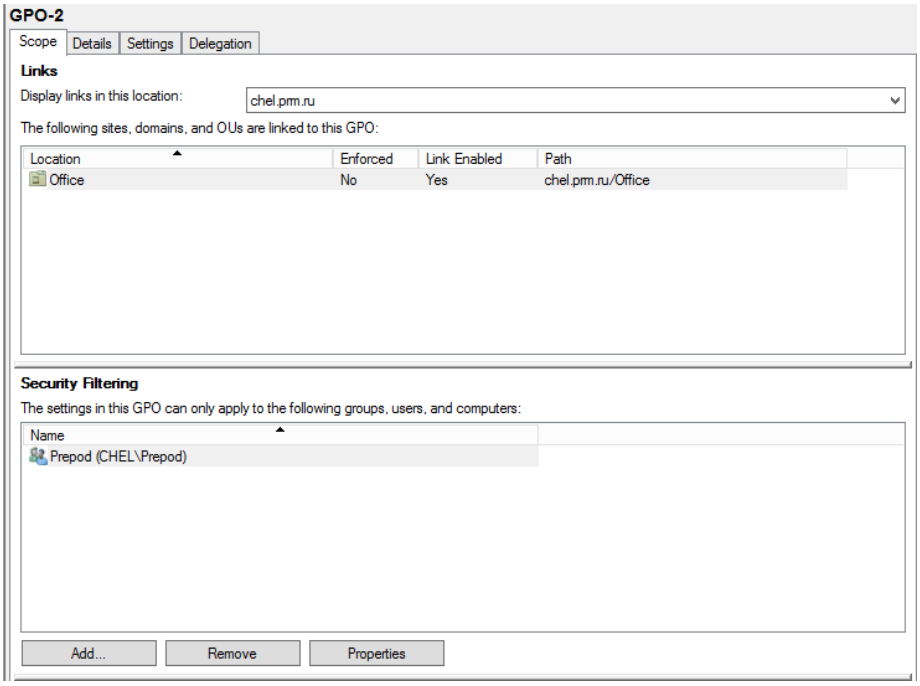
9. Аналогично перенастройте папку Документы.

в) сетевые папки Man_share и Work_share с файлового сервера FS2 подключены как сетевые диски (Z:\) для пользователей групп Prepod и Workers соответственно;

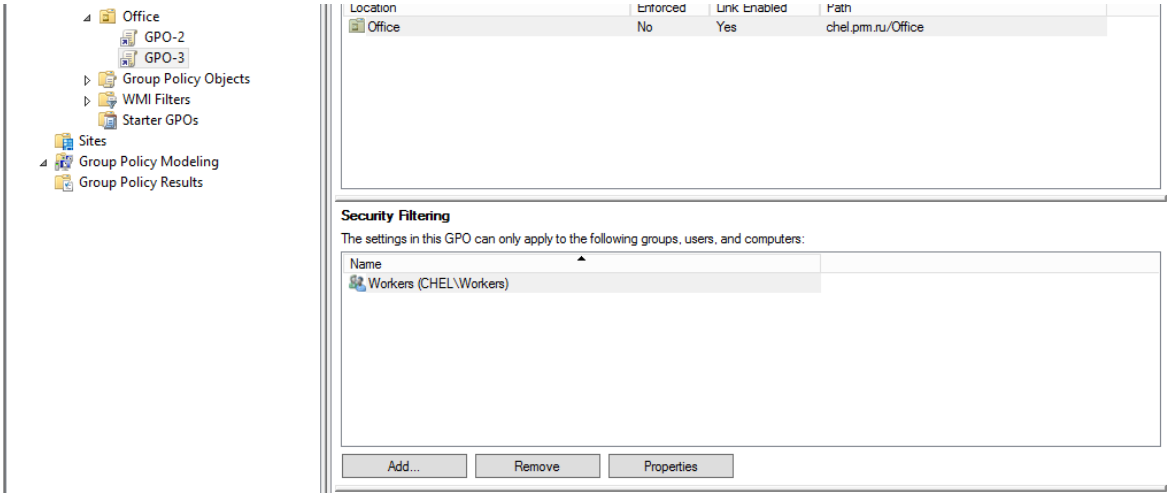
1. В подразделении Office создаем групповую политику GPO-2.



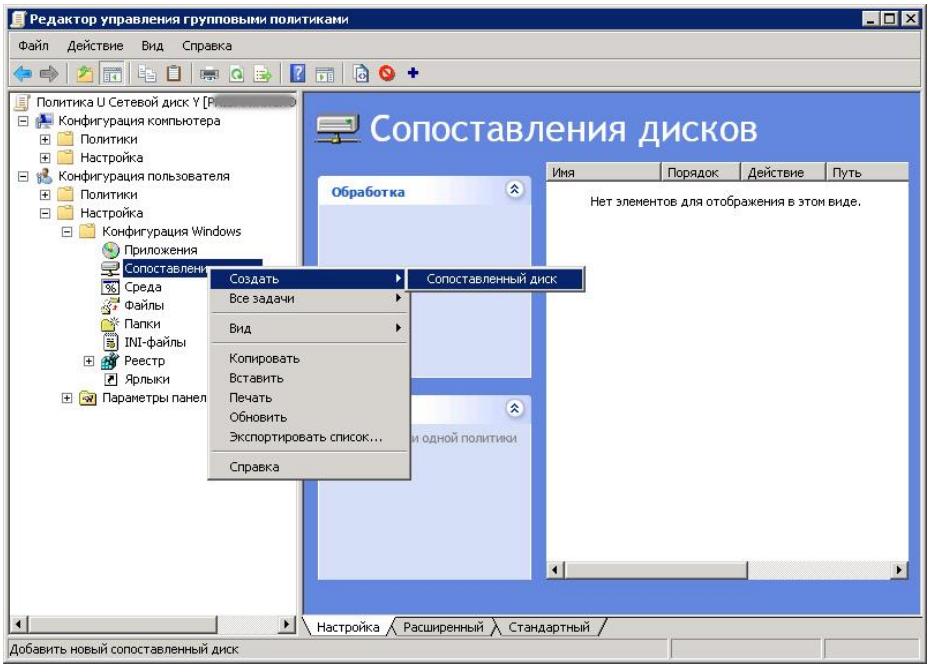
2. Выделяем политику GPO-2 и из области ***Security Filtering*** удаляем запись для всех пользователей и добавляем группу Prepod.



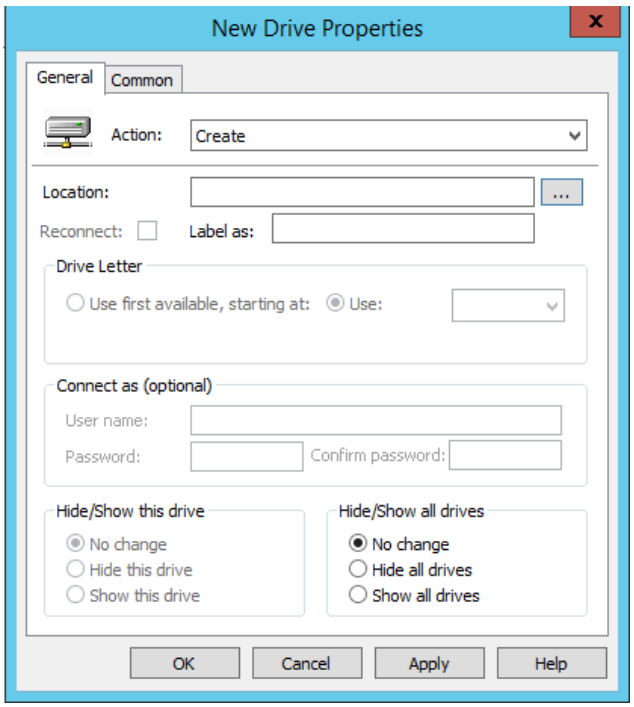
3. Аналогично создаем и настраиваем политику GPO-3 для группы Workers.



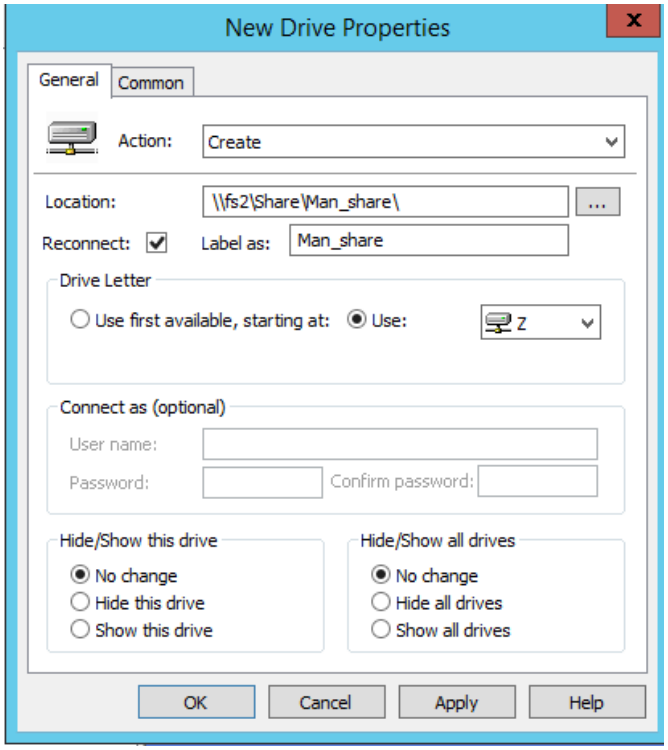
4. Изменяем политику GPO-2.
5. Редактор управления групповыми политиками выбираем последовательно: ***Конфигурация пользователя → Настройка → Конфигурация Windows → Сопоставления дисков***. В открывшемся окне Новые свойства диска на вкладке Общие в выпадающем списке Действие: необходимо выбрать Создать:



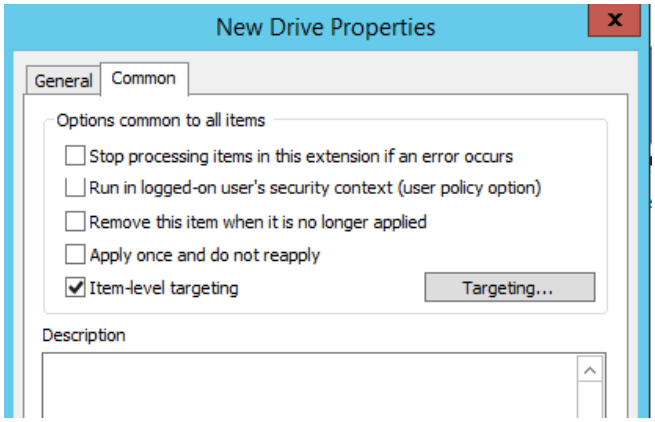
6. В открывшемся окне Новые свойства диска на вкладке Общие в выпадающем списке Действие: необходимо выбрать Создать:



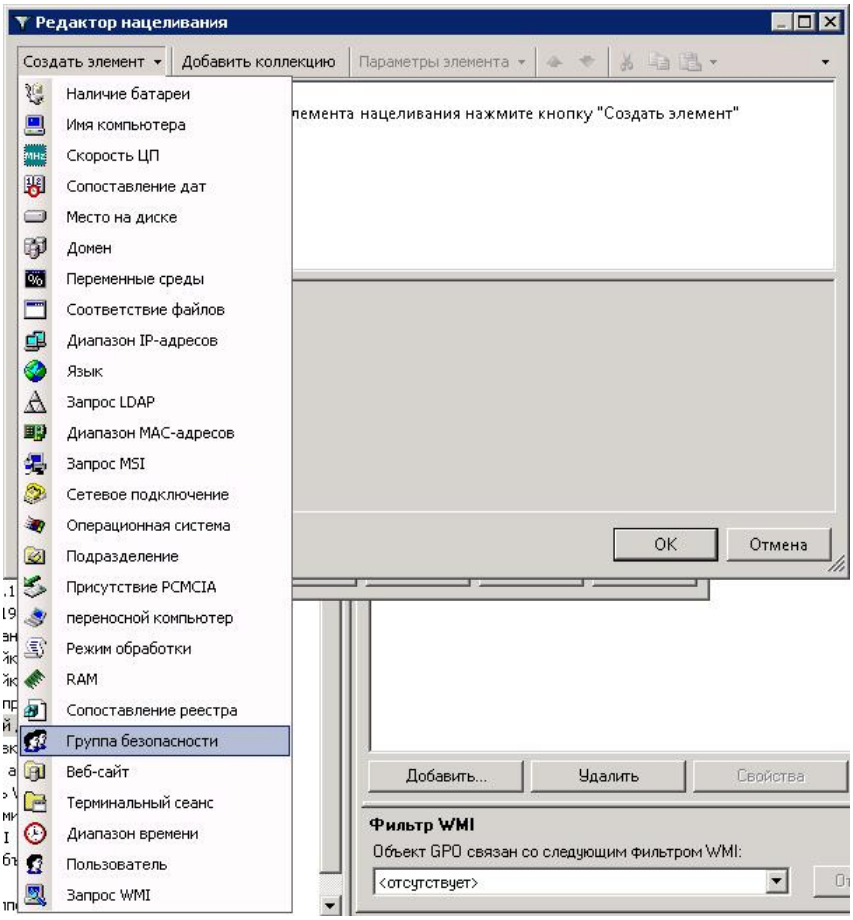
7. В открывшемся окне Новые свойства диска на вкладке Общие в выпадающем списке Действие: необходимо выбрать Создать:



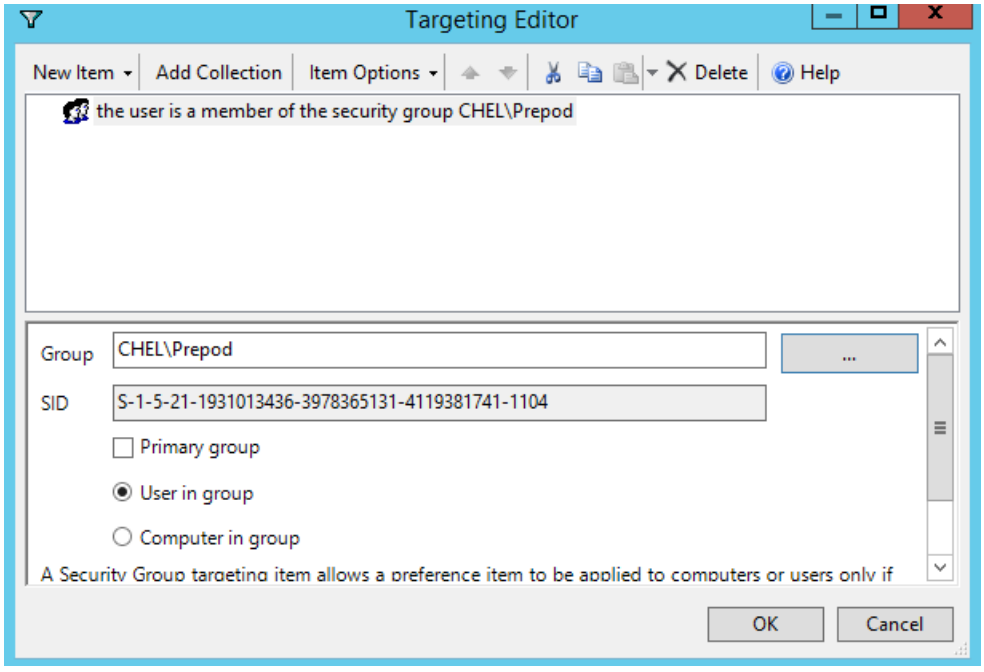
8. Заходим в кнопку Нацеливание...



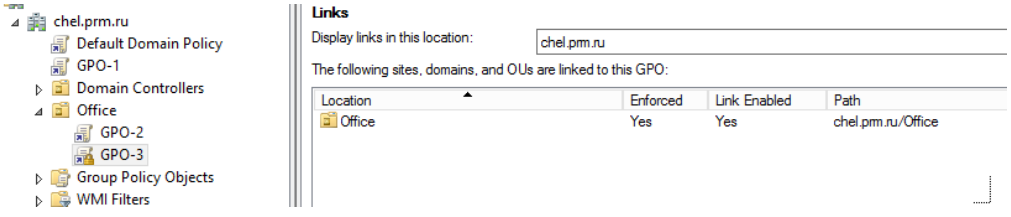
9. В Редакторе нацеливания щелкаем выпадающий список Создать элемент и Группа безопасности:



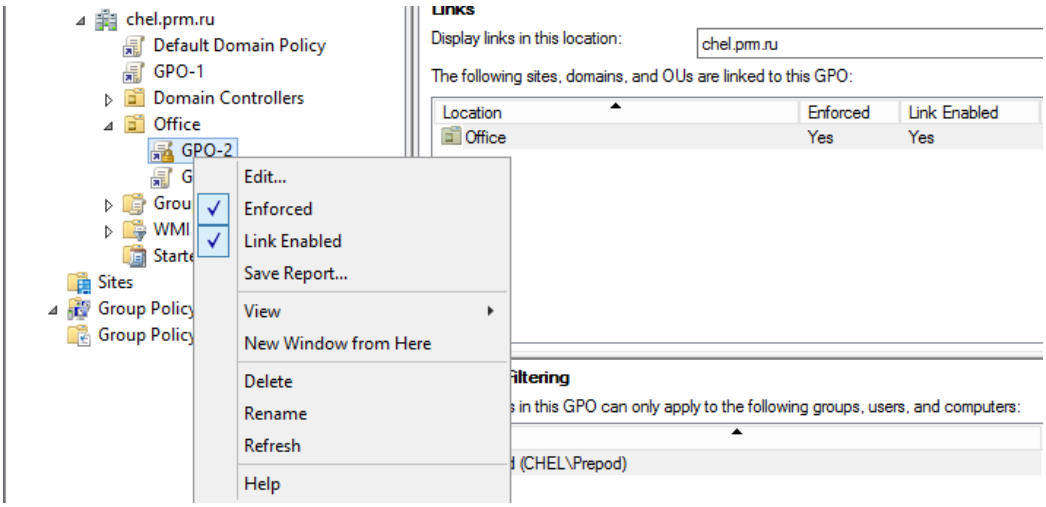
10. Выбираем радиокнопку Пользователь в группе и щелкаем кнопку ...:



11. Попадаем снова в окно Новые свойства диска и нажимаем Ok:
12. Теперь связываем новую политику с подразделением (OU) - желательно сначала протестировать работу новой политики.



13. Проверяем, что связь включена и добавляем галочку Принудительный:



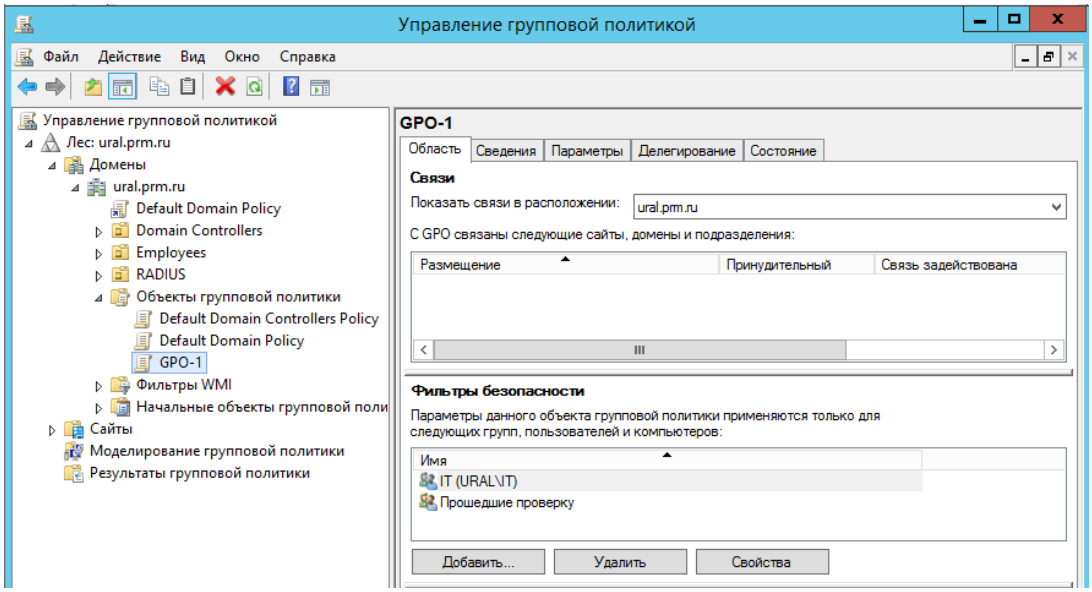
14. Теперь нужно залогиниться в тестовую машину и проверить, что сетевой диск появился у пользователя:

15. Аналогично требуется настроить вторую политику.

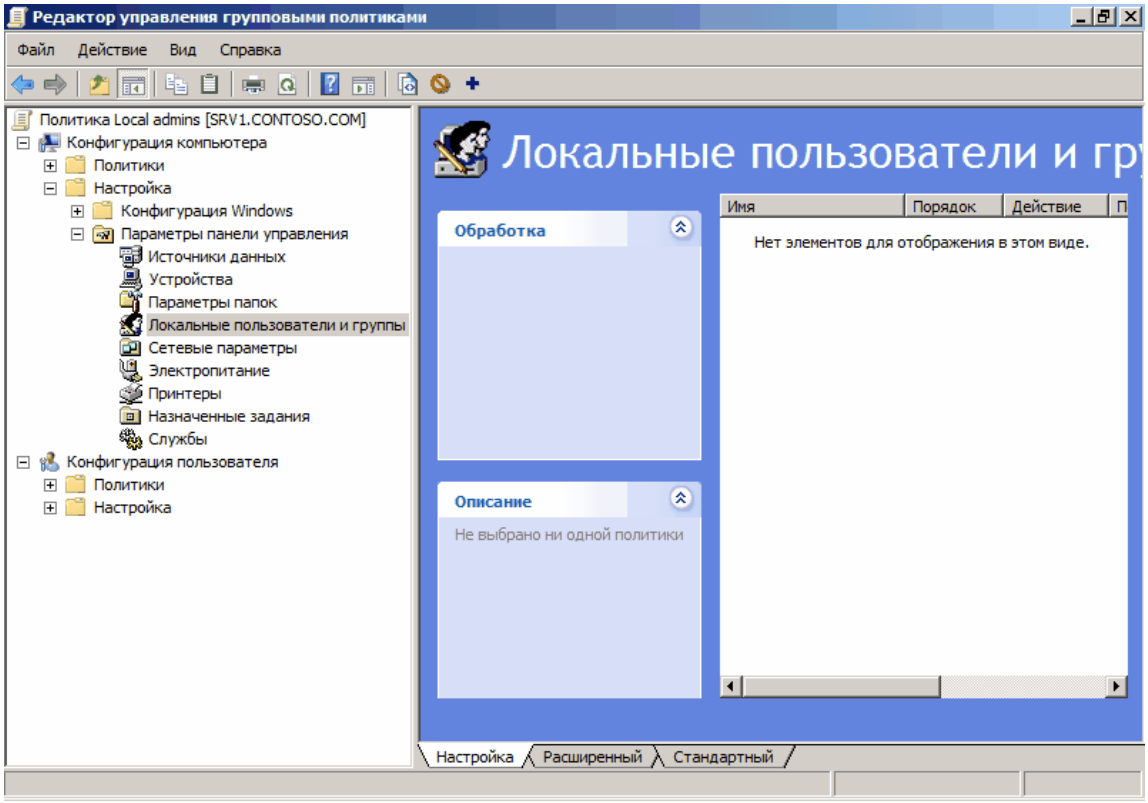
В домене ural.prm.ru настройте групповые политики, обеспечивающие выполнение следующих условий:

– *пользователи группы IT должны быть членами локальных групп администраторов на всех компьютерах данного домена;*

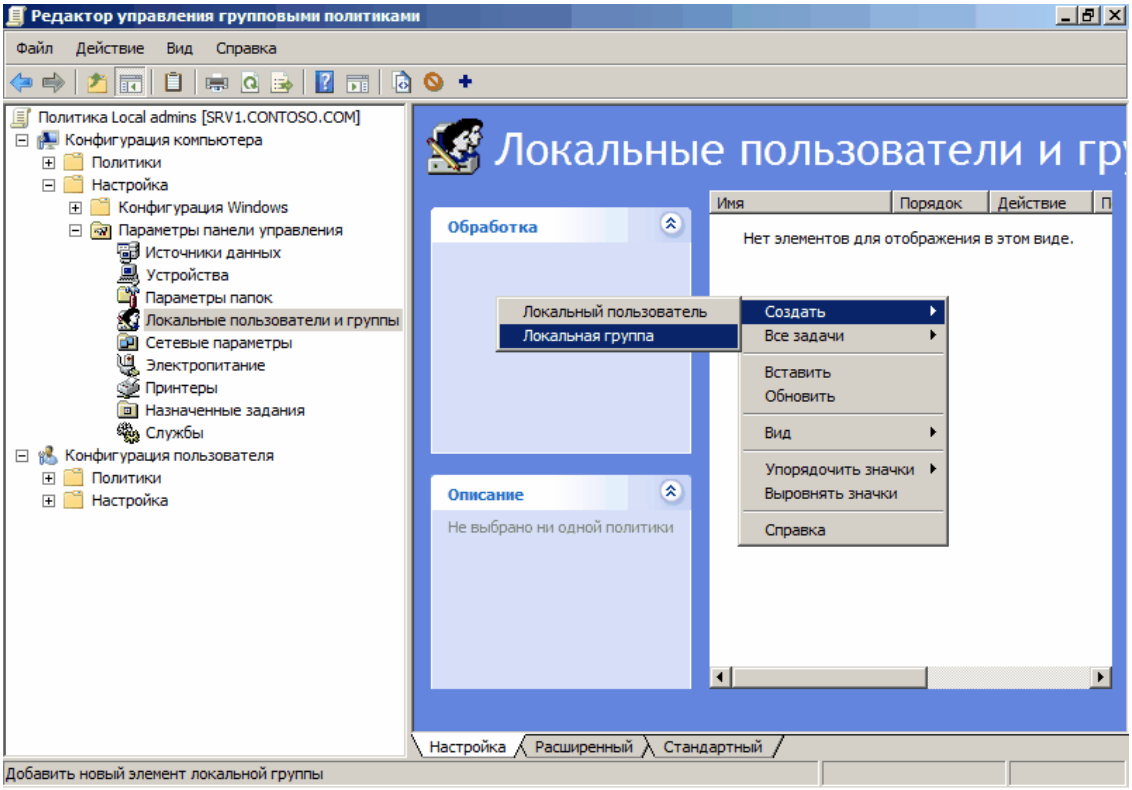
1. Создаем групповую политику



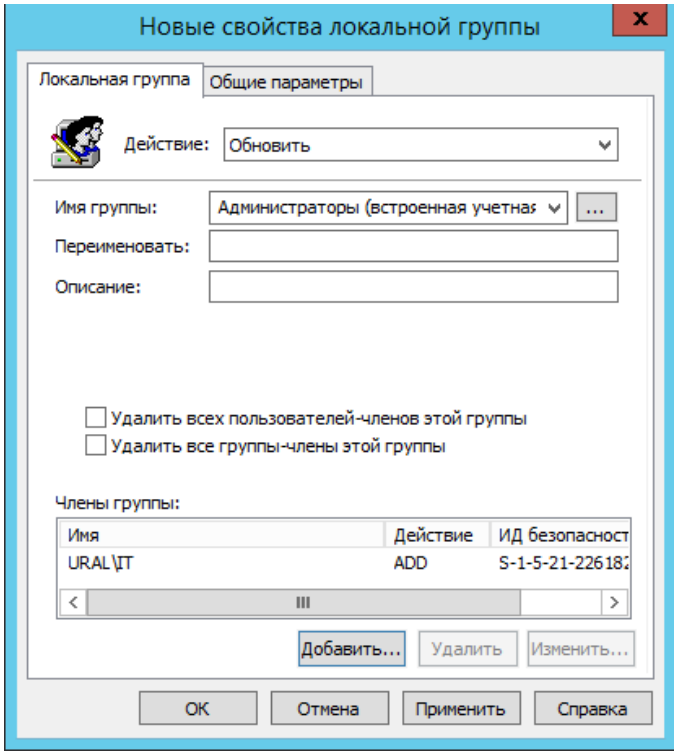
2. Для добавления пользователей в локальные группы с помощью предпочтений идем в раздел Конфигурация компьютера\Настройка\Параметры панели управления (*Computer Configuration\Preferences\Control Panel Settings*) и выбираем пункт Локальные пользователи и группы (*Local User and Groups*)



3. Щелкаем правой клавишей мыши на пустом поле, и в контекстном меню выбираем пункт Создать — Локальная группа

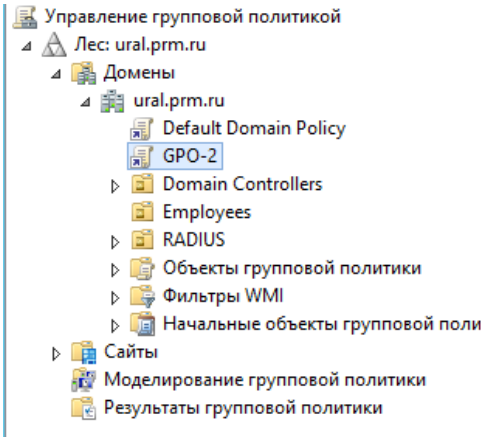


4. В поле имя группы выбираем Администраторы (встроенная учетная запись), это выберет группу локальных администраторов, даже если она была переименована. Затем жмем на кнопку Добавить и в качестве членов группы выбираем доменную группу IT. Теперь осталось нажать ОК, и наша группа IT будет добавлена в группу локальных админов на всех рабочих станциях домена.

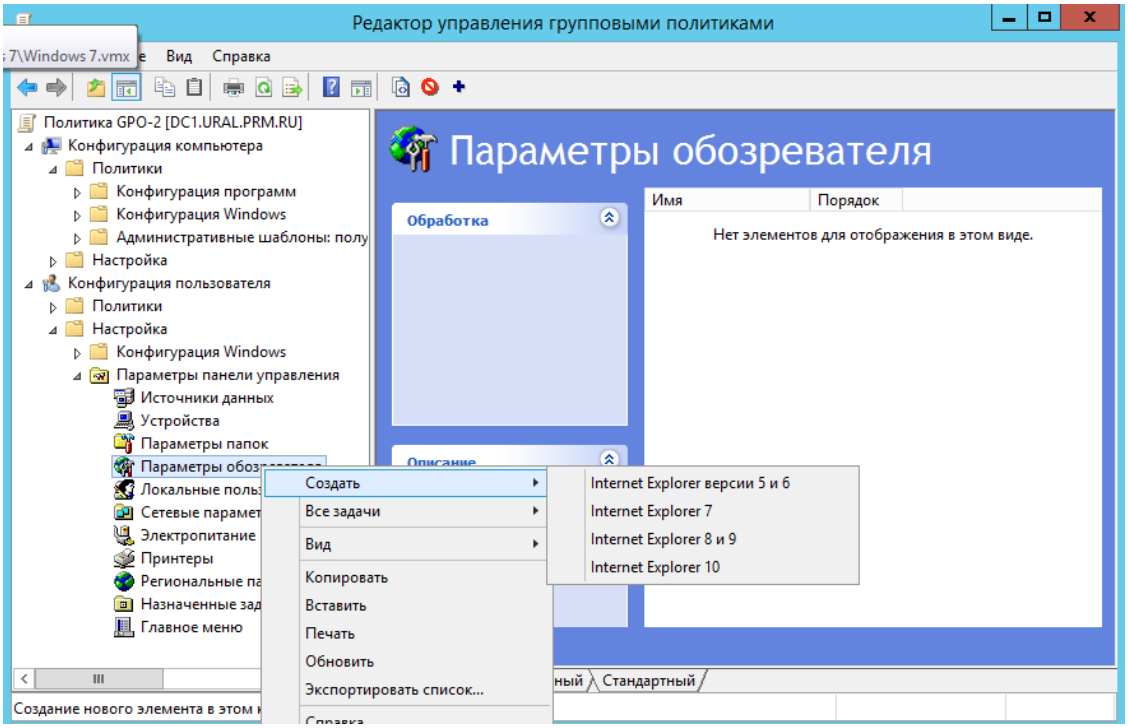


– *для всех пользователей домена при открытии браузера IE должна открываться стартовая страница терминального сервера;*

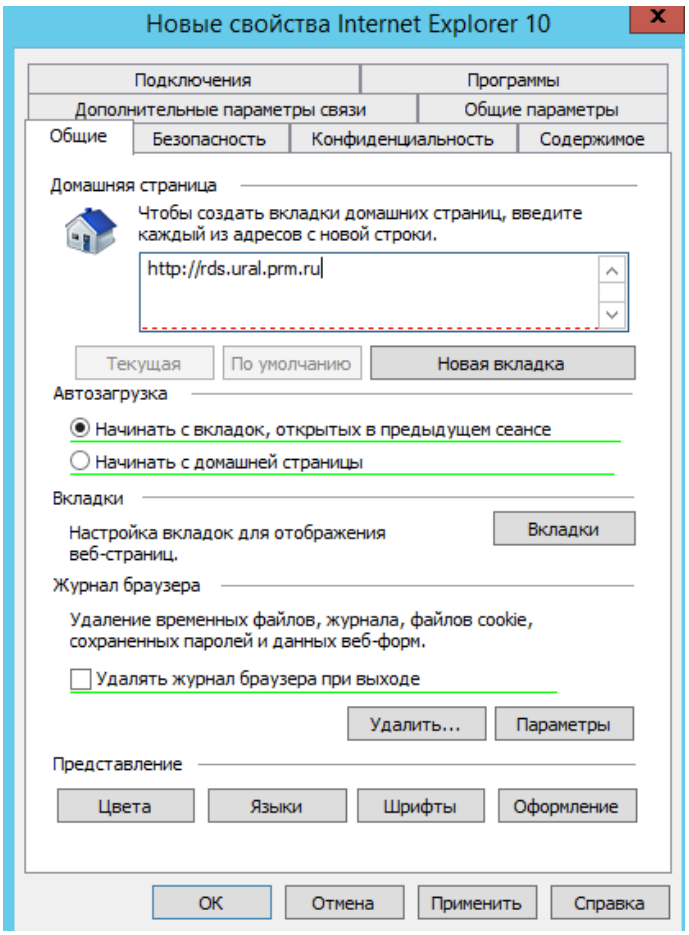
1. Создать групповую политику GPO-2, после этого выберете Изменить ГП



2. Выберем соответствующий параметр групповой политики, выберем версию IE 10/



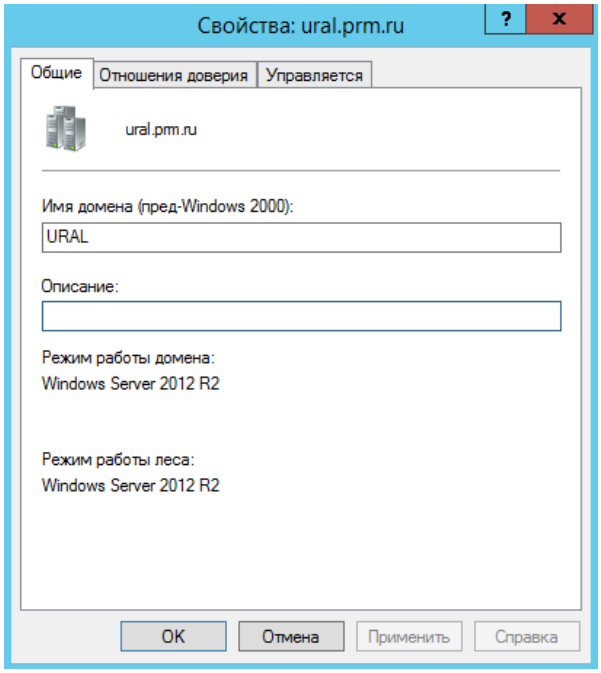
3. Настройте стартовую страницу браузера.



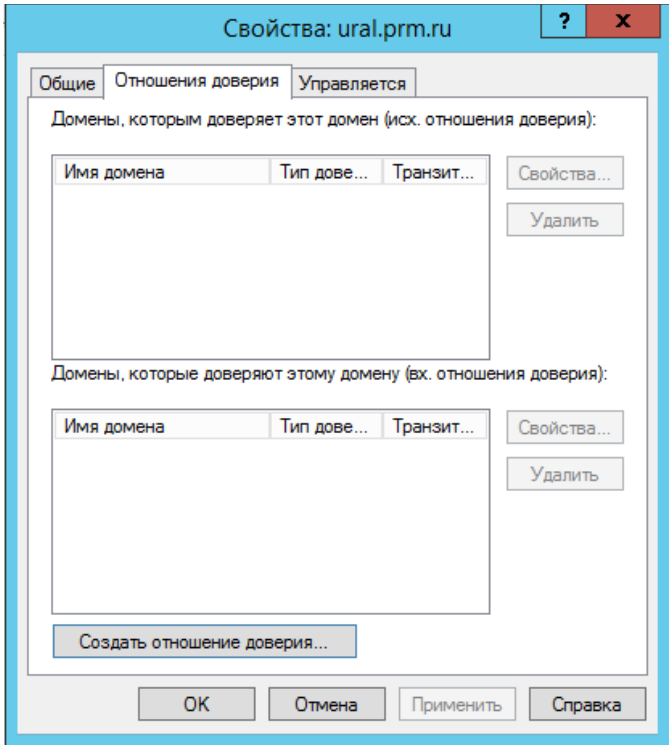
Доверительные отношения

Между доменами ural.prm.ru и chel.prm.ru установите односторонние доверительные отношения: пользователи домена ural.prm.ru должны иметь доступ к ресурсам домена chel.prm.ru (без дополнительных настроек в AD и DNS), но не наоборот.

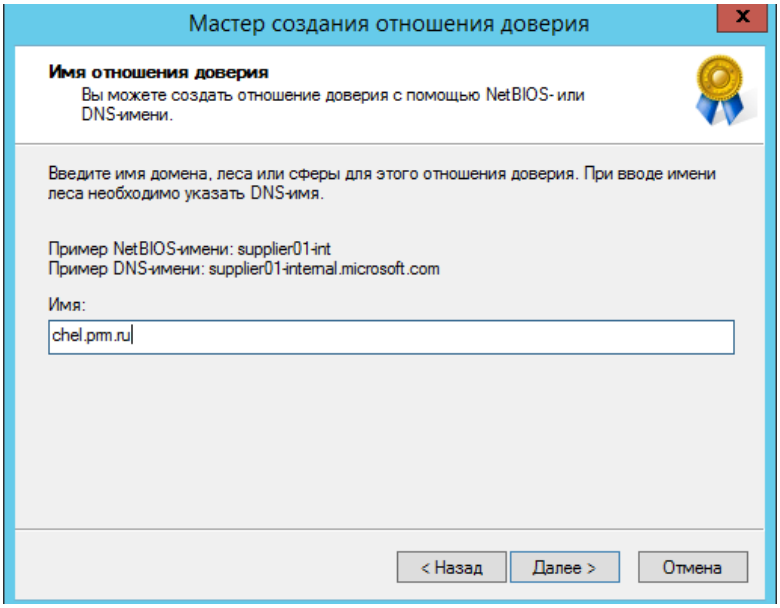
1. В домене DC1 заходим в средства ***AD – домены и доверие***, заходим к контекстное меню домен и выбираем Свойства.



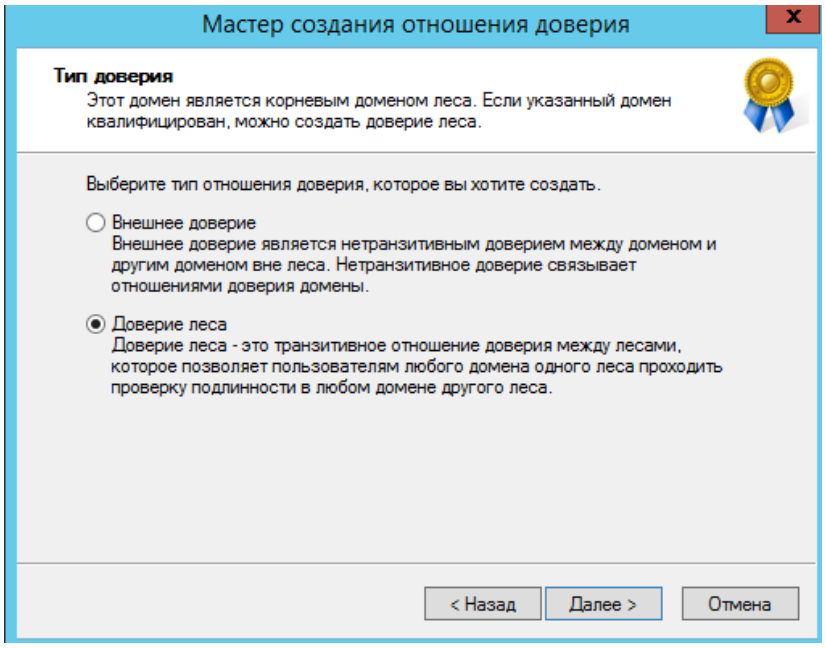
2. Переходим на вкладку ***Отношения доверия*** и нажимаем на кнопку ***Создать отношение доверия***.

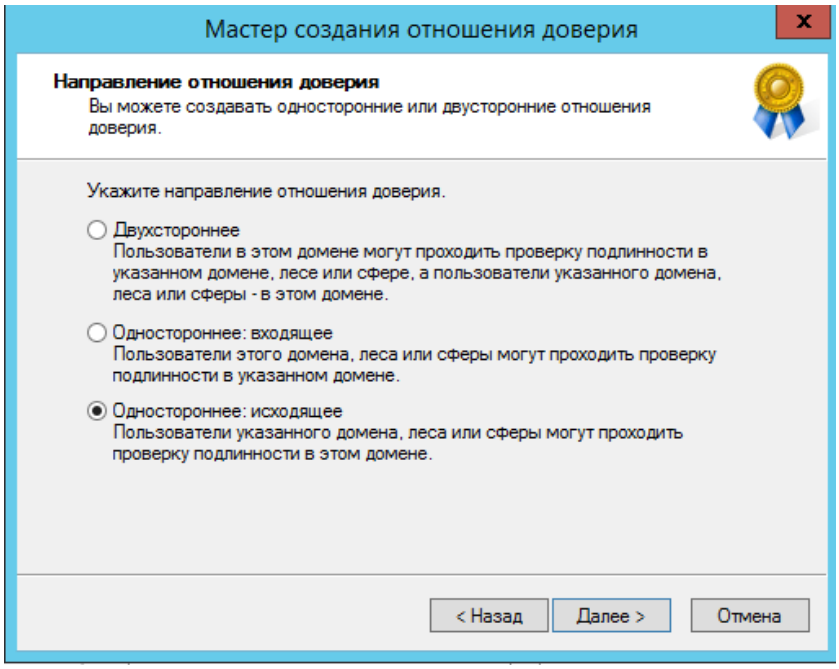


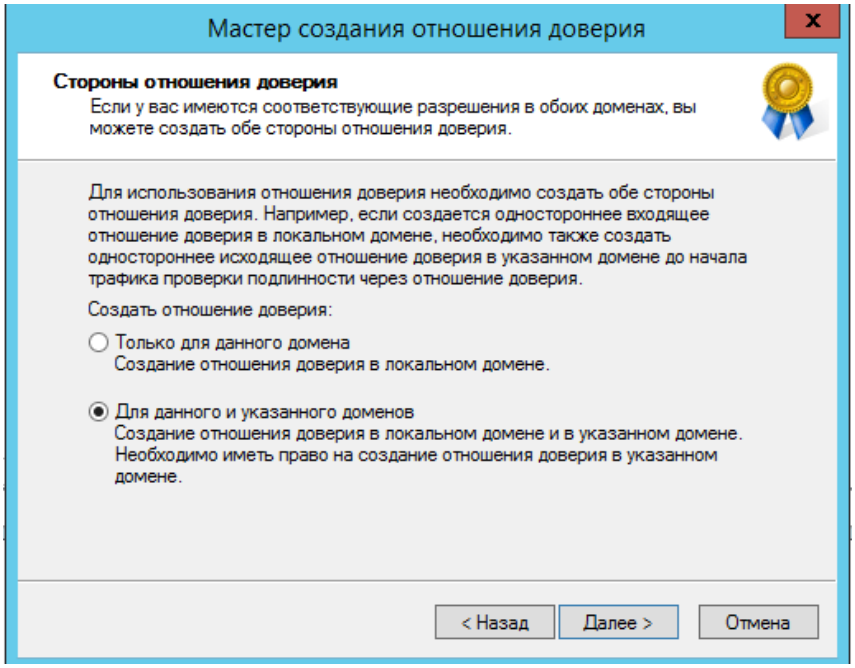
3. Вводим имя домена с которым нужно установить доверительные отношения

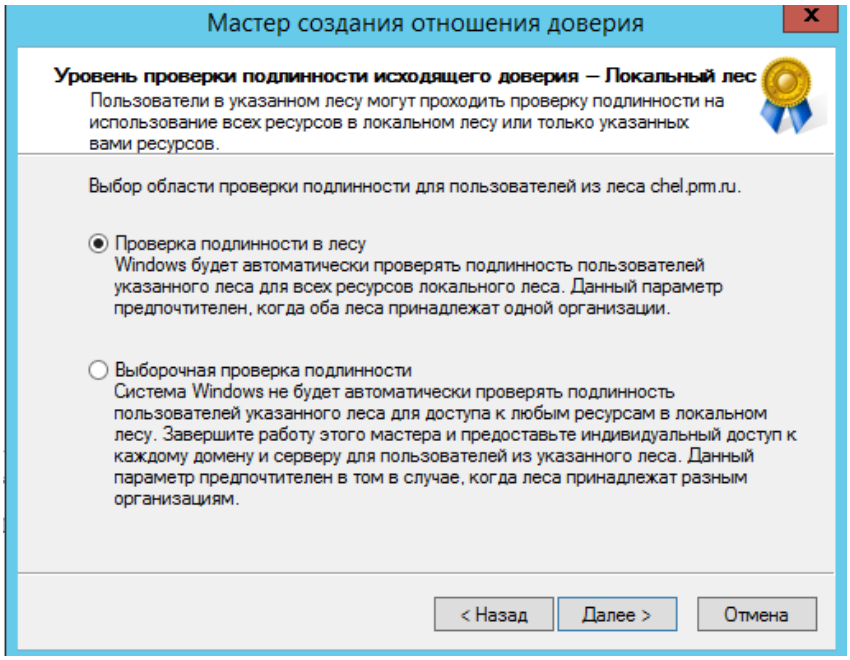


4. Выберете тип доверия

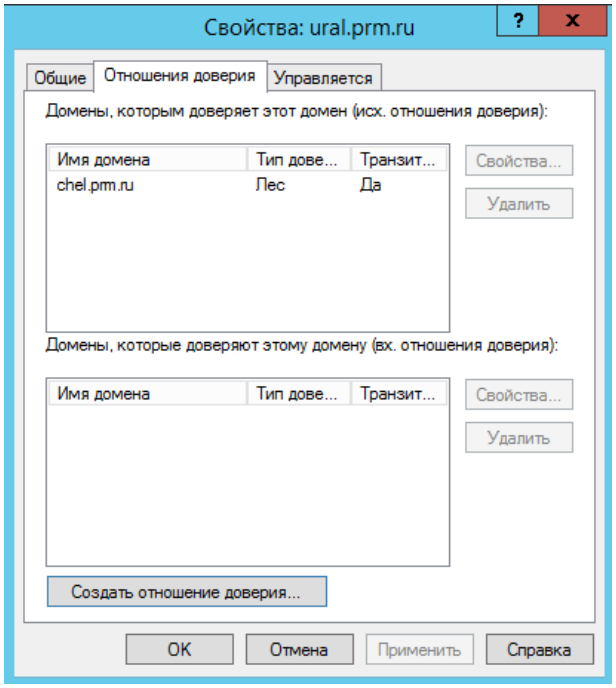






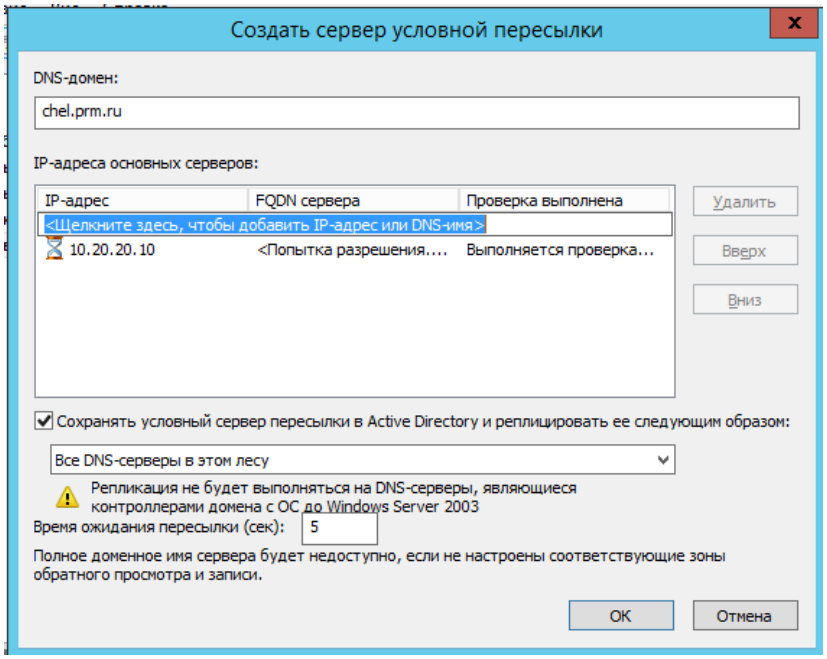


5. Завершите настройку доверительного отношения. При необходимости следует удалить доверие из поля ***Домены, которые доверяют этому домену (вх. отношения доверия)***



На серверах DC1 и DC2 настройте пересылку DNS-запросов между доменами ural.prm.ru и chel.prm.ru. При появлении новых DNS-серверов они должны получать соответствующие настройки автоматически.

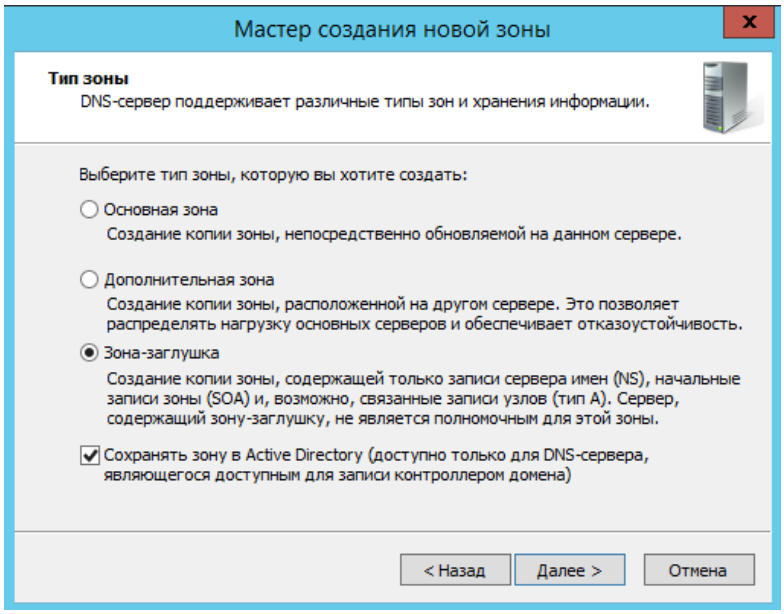
1. В консоли ***Диспетчер DNS*** (DNS Manager) щелкните правой кнопкой папку ***Серверы условной пересылки*** (Conditional Forwarders). В контекстном меню выберите команду ***Создать условную пересылку*** (Conditional Forwarder).
2. В диалоговом окне ***Создать сервер условной пересылки*** (New Conditional Forwarder) введите имя домена, в который следует пересылать запросы.
3. Щелкните список ***IP-адрес*** (IP Address), введите IP-адрес полномочного DNS-сервера в указанном домене и нажмите Enter.
4. Установите флажок ***Сохранять условную пересылку в Active Directory*** (Store This Conditional Forwarder In Active Directory) и выберите стратегий репликации.
5. Аналогично настройте второй DNS.



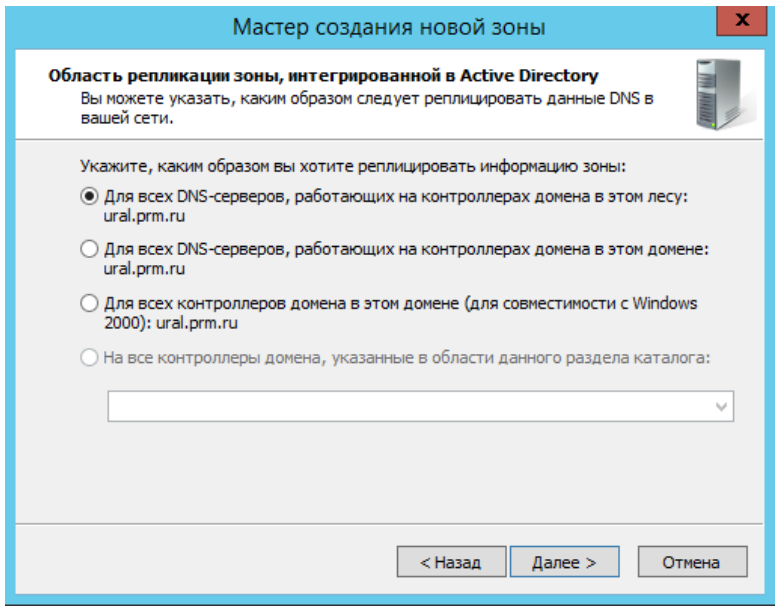
6. На сервере DC1 откройте PowerShell и проверьте пересылку DNS-запросов.

Настройка одностороннего доверия DNS

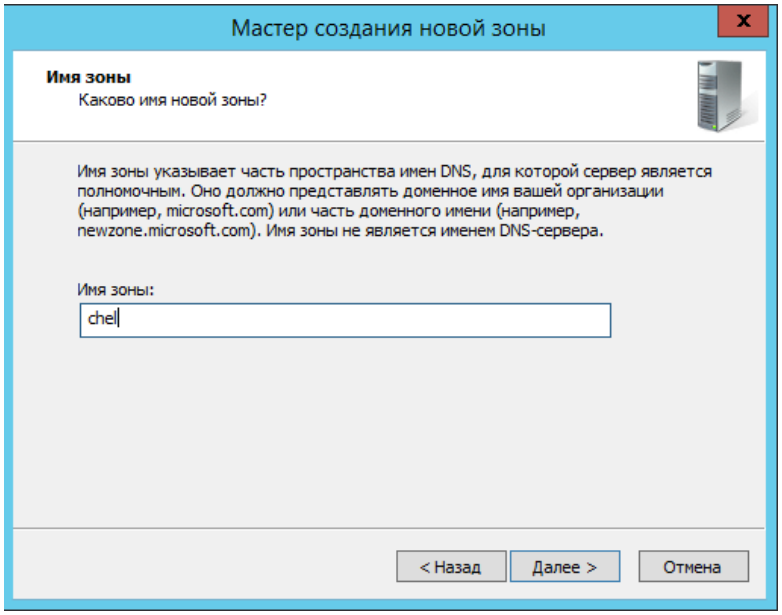
1. Открываем службу DNS на сервере DC1, выбираем зону прямого просмотра → ***Создать новую зону*** → Выбираем тип зоны.



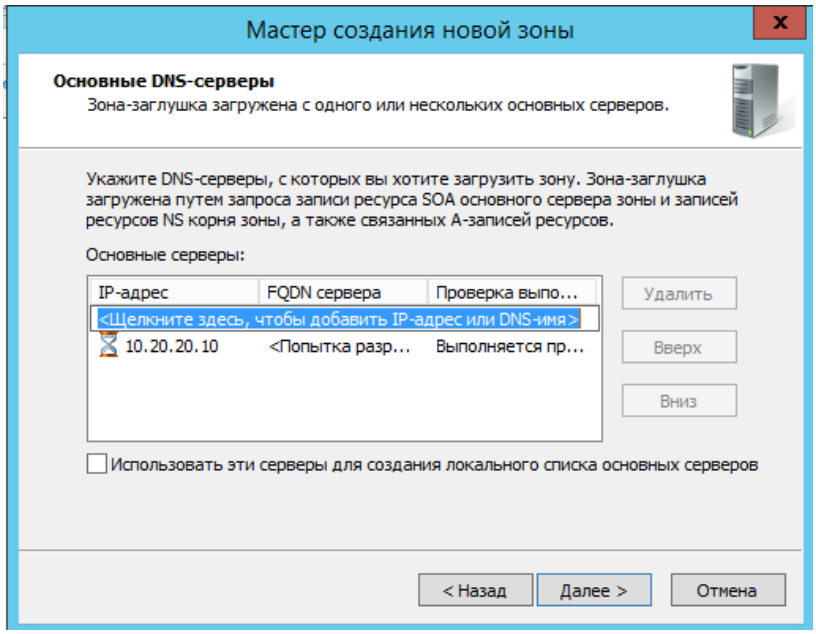
2. Область репликации зоны



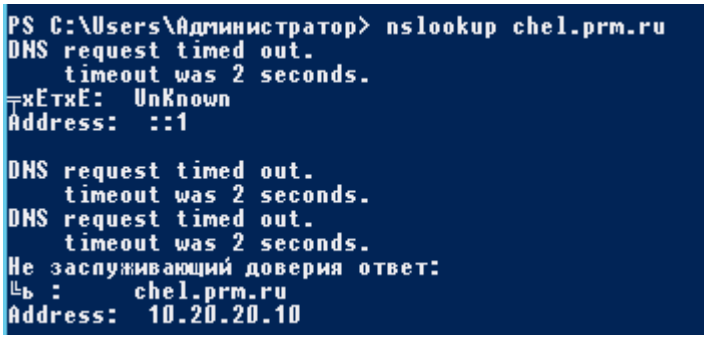
3. И имя зоны создаваемой зоны



4. Ip адрес DNS сервера



5. Аналогично настройте второй DNS сервер.

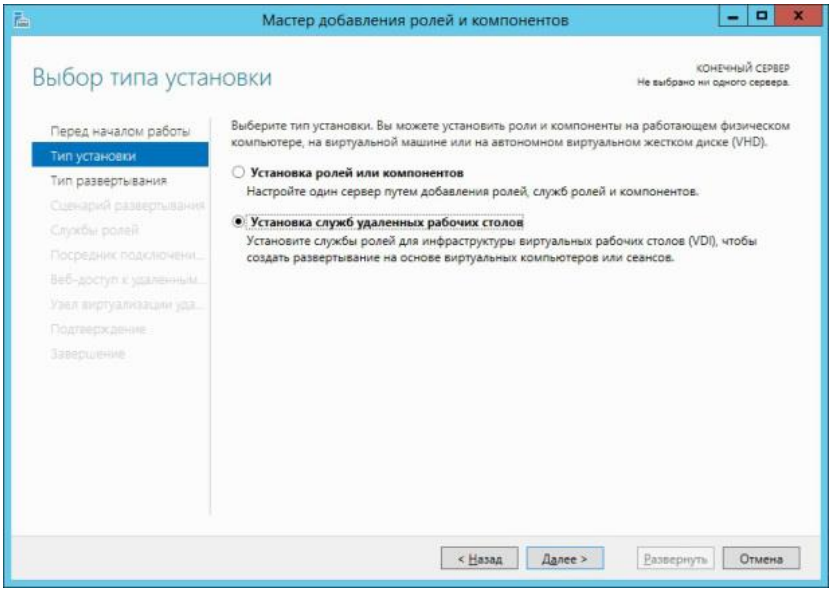


Установка роли RDS

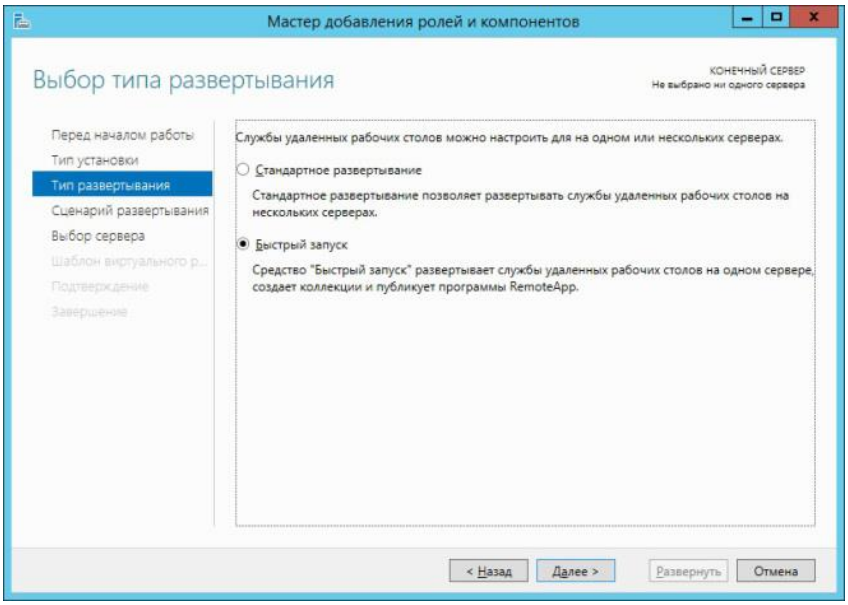
На сервере RRAS1 установите роль RDS.

На сервере RDS установите и настройте роль терминального сервера.

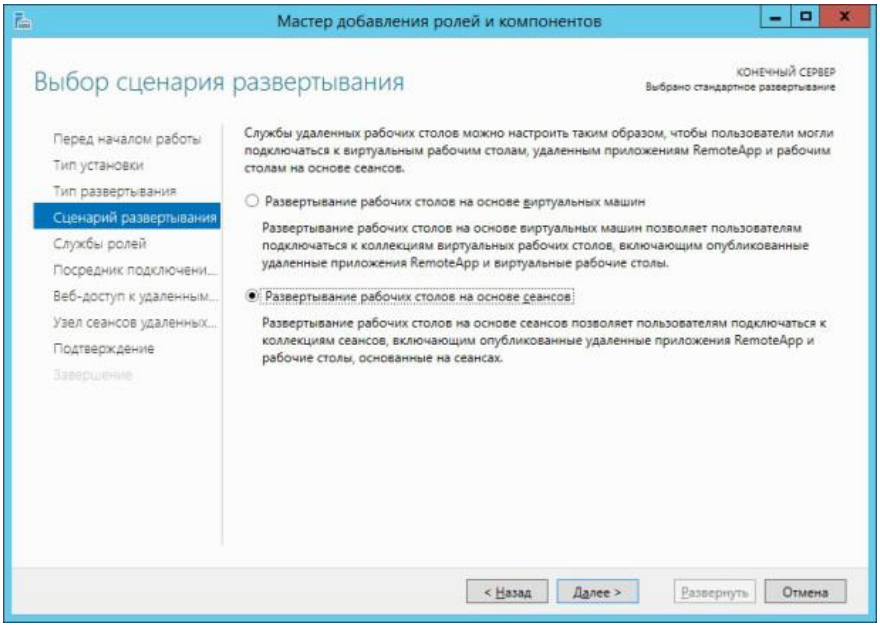
1. Диспетчер серверов → Панель мониторинга → Добавить роли и компонент.
2. В следующем окне предлагается выбрать тип установки. Отмечаем пункт ***Установка служб удалённых рабочих столов***.



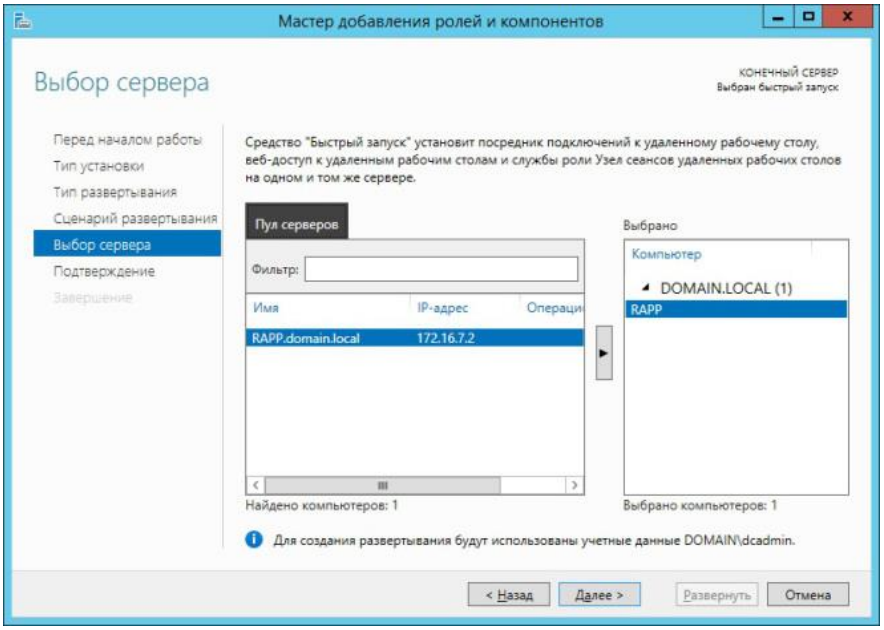
3. Так как мы производим установку всех служб RDS на один сервер, то целесообразно в следующем окне мастера выбрать ***Быстрый запуск***.



4. Далее выбираем сценарий развертывания RDS. Создание среды удалённых рабочих столов на основе сеансов. Поэтому выбираем соответствующую опцию и жмём ***Далее***.



5. В следующем окне мастера предлагается выбрать сервер, на котором будут развернуты службы RDS. В нашем случае это сервер RASS1.ural.prm.ru. После того, как выбор сделан, жмём ***Далее***.



После выбора сервера мы увидим окно с подтверждением выбранных служб и именем сервера, на который будут установлены эти службы. Тут же необходимо согласиться с тем, что сервер будет перезагружен, поставив соответствующую галочку и нажать кнопку ***Развернуть***, после чего откроется окно в котором будет отображен процесс развёртывания ролей RDS. В процессе выполнения установки сервер будет перезагружен. После перезагрузки сервера, необходимо зайти под той же учётной записью, под которой был начат процесс установки (Administrator) и спустя некоторое время откроется окно мастера и развёртывание возобновится автоматически (при необходимости это следует запустить занового вручную).

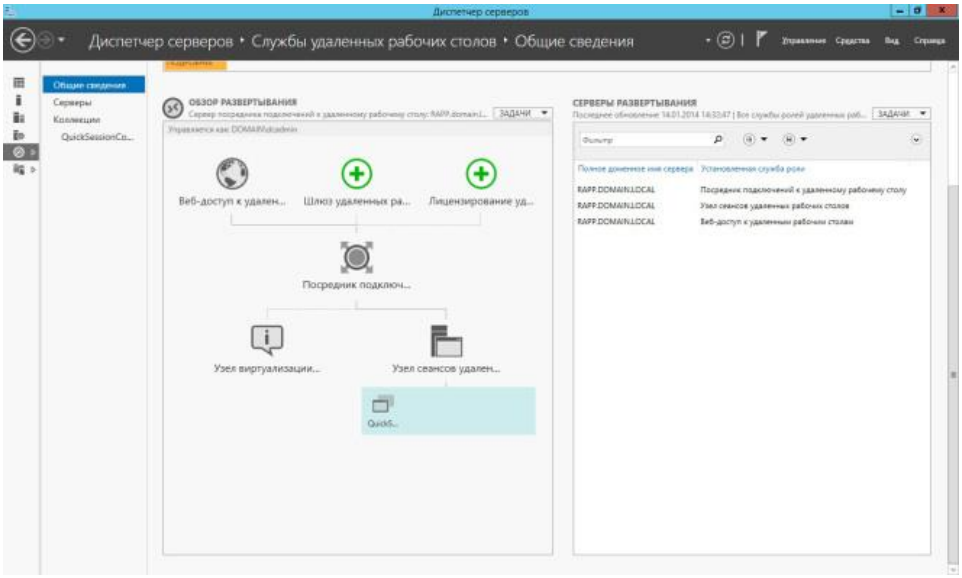
```
PS C:\Users\Администратор.URAL> Set-Service WinRM
PS C:\Users\Администратор.URAL>
```

```
PS C:\Users\Администратор.URAL> enable-PSRemoting

Быстрая настройка WinRM
Запуск команды "Set-WSManQuickConfig" для включения удаленного управления этим компьютером с помощью службы WinRM.
 Это подразумевает:
    1. Запуск или перезапуск (если она уже запущена) службы WinRM.
    2. Изменение типа запуска службы WinRM на автозапуск.
    3. Создание прослушивателя для приема запросов на любом IP-адресе.
    4. Настройку исключений брандмауэра Windows для трафика службы WS-Management (только для протокола http).

Вы хотите продолжить?
[Y] Да - Y  [A] Да для всех - A  [N] Нет - N  [L] Нет для всех - L  [S] Приостановить - S  [?] Справка
(значением по умолчанию является "Y"):Y
Служба WinRM уже настроена для приема запросов на этом компьютере.
Служба WinRM уже настроена для удаленного управления на этом компьютере.
```

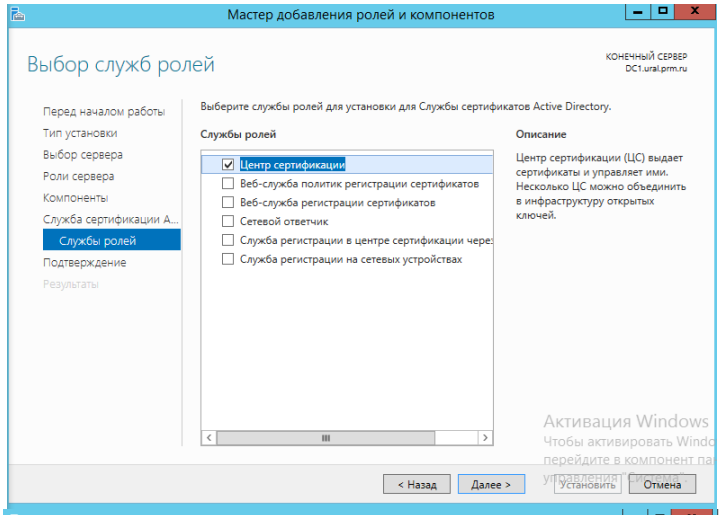
6. После завершения установки, мастер отрапортует о состоянии всех служб и сообщит ссылку для организации веб-доступа к удалённым рабочим столам.
7. Когда мастер завершит развёртывание RDS, можно будет посмотреть какие роли установлены. Для этого заходим в диспетчер серверов и выбираем в левой панели пункт ***Службы удалённых рабочих столов***. На вкладке ***Общие сведения*** мы можем увидеть, что сервер RAPP в данном развёртывании будет выступать в роли посредника подключений к удалённому рабочему столу, узла сеансов удалённых рабочих столов и узла веб-доступа к удалённым рабочим столам.

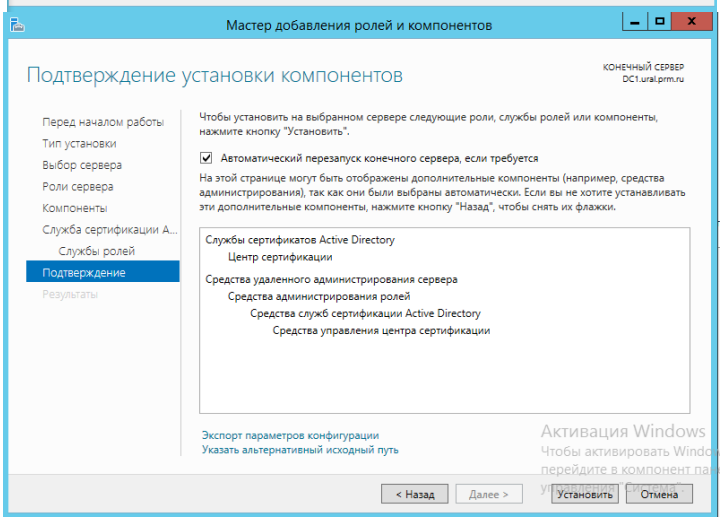


Установка службы сертификации

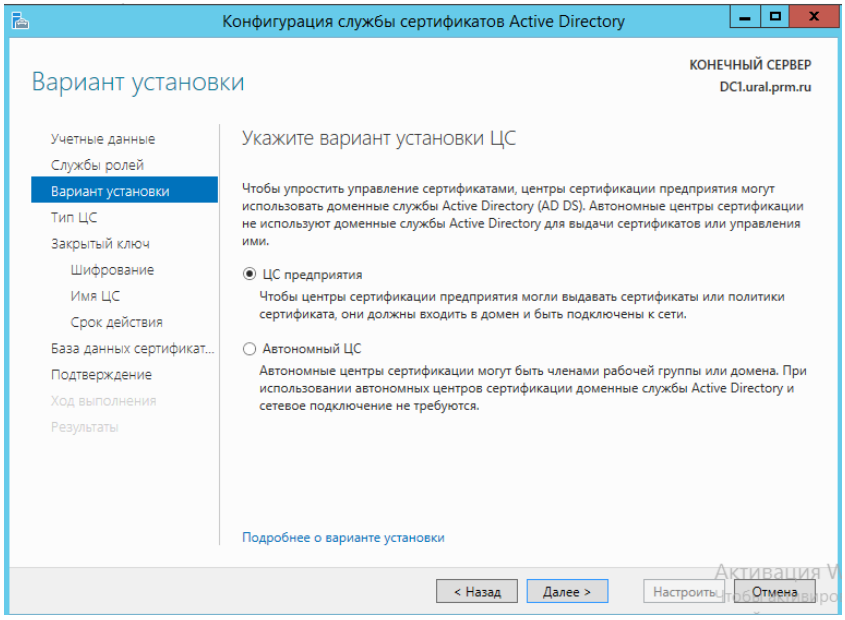
На сервере DC1 установите и настройте роль удостоверяющего центра с названием MainCA.

1. Заходим в ***Диспетчер серверов*** DC1 → ***Добавить роли и компоненты*** → ***Установление ролей и компонентов*** → Выбрать сервер → ***Служба сертификации AD***

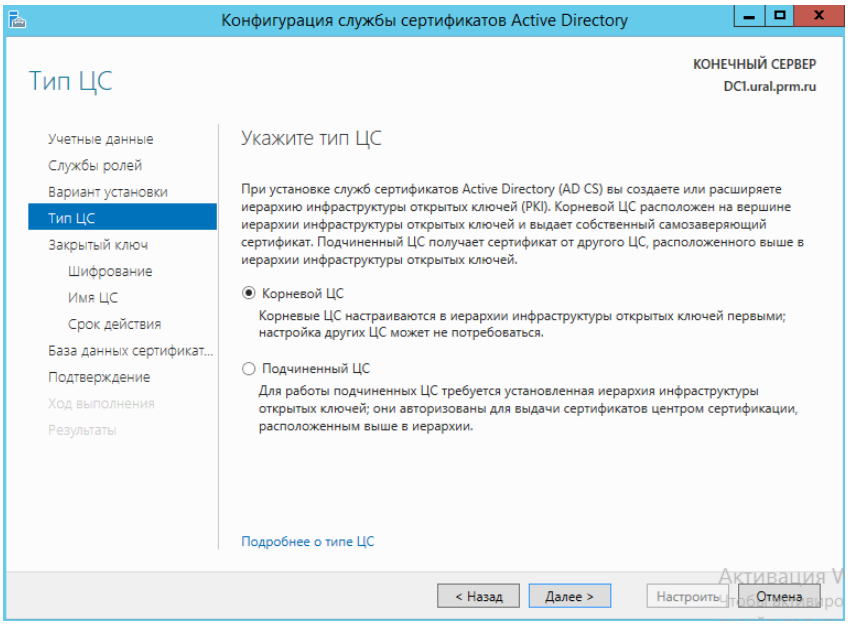




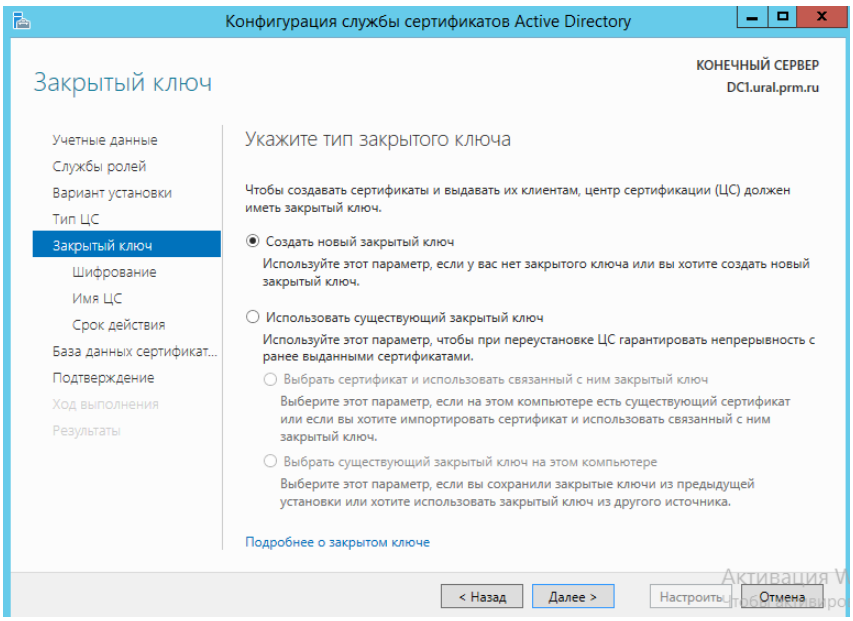
2. Далее осуществите конфигурирование центра сертификации → Учетные данные для настройки службы роли стандартные → Выбор для настройки службы роли (Центр сертификации) → Вариант для настойки – ***ЦС предприятия***.



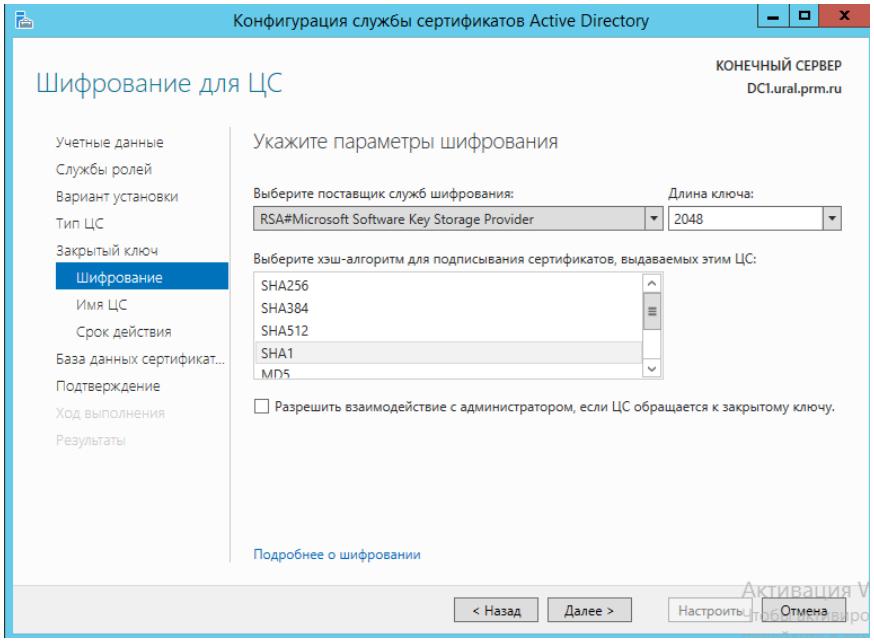
3. Укажите тип – ***Корневой ЦС***.



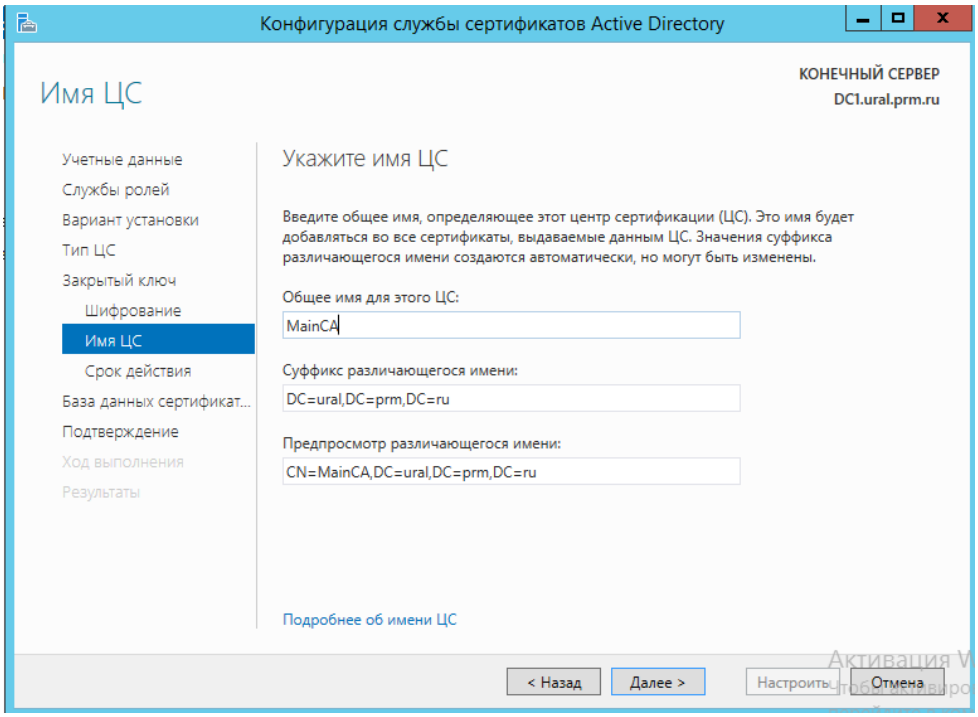
4. Выбор типа закрытого ключа – ***Создать новый закрытый ключ***.



5. Выбор параметров шифрования – ***SHA1***.



6. Имя ЦС – ***MainCA***.

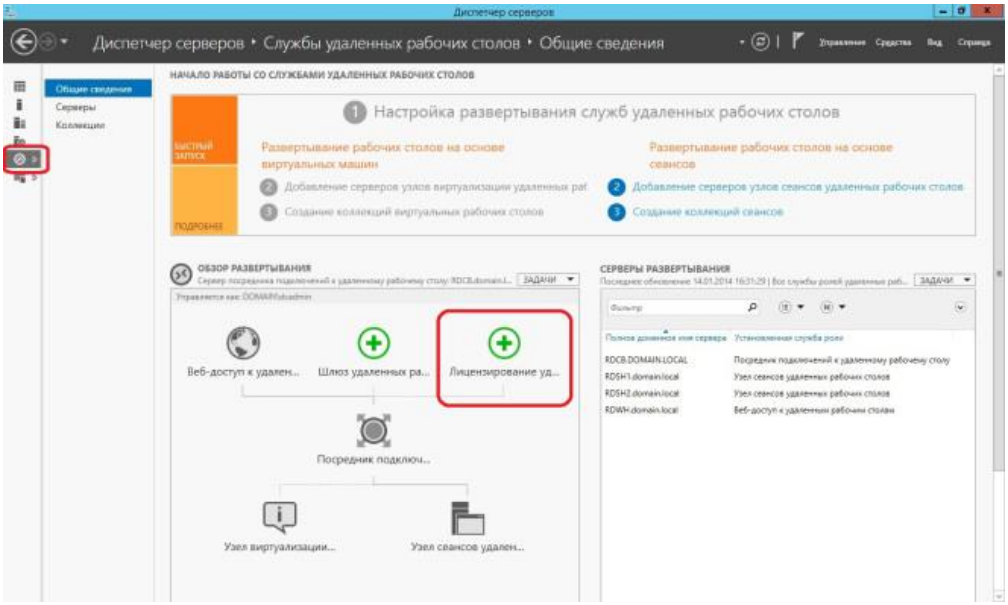


7. Подтвердите период и место расположения базы и закончите настраивать службу.

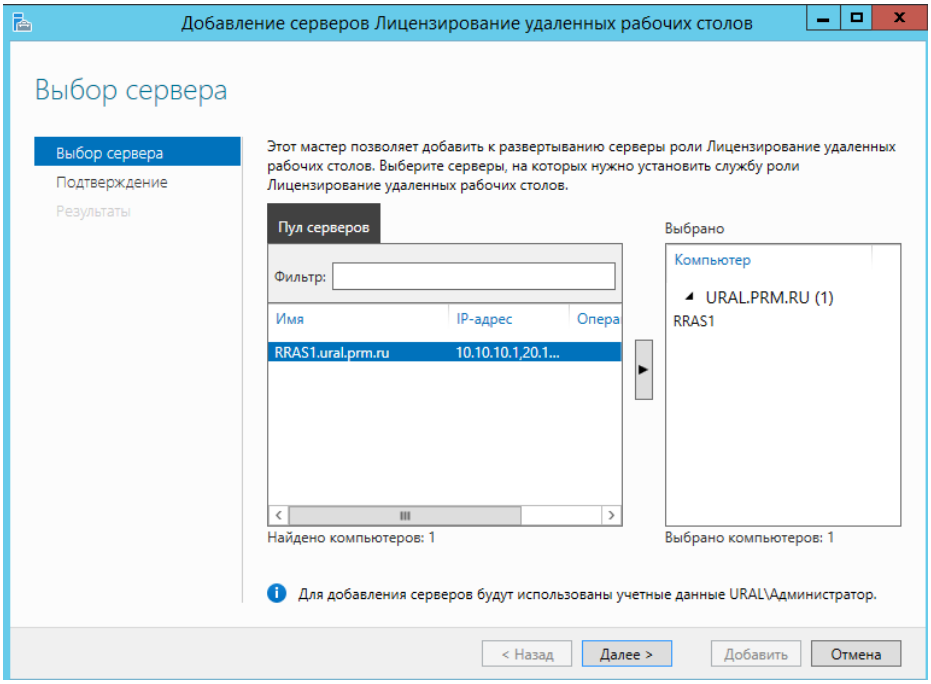
Терминальный сервер со службой лицензирования

Разверните терминальный сервер с лицензированием по компьютерам (используйте временную лицензию).

1. Запустите Диспетчер серверов, и перейдите в консоль управления удалёнными рабочими столами, кликнув на соответственную ссылку слева. Для запуска необходимого мастера кликнем на зелёную кнопку с плюсом и подписью ***Лицензирование удалённых рабочих столов*** на панели Обзор развёртывания.



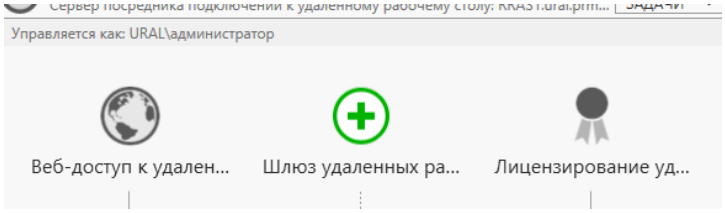
2. Выбираем сервер, который будут отвечать за лицензирование удалённых рабочих столов. И подтвердите его правильность.



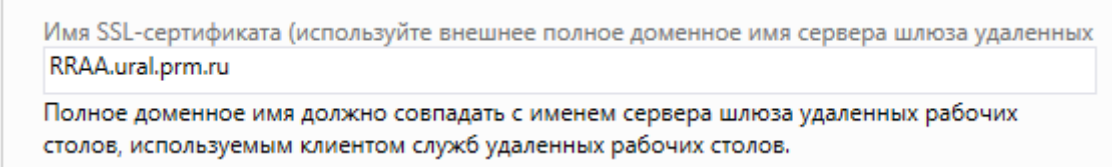
3. В окне с результатами работы мастера можно перейти по ссылке Посмотреть свойства лицензирования удалённых рабочих столов для развёртывания и настроит базовые параметры серверов лицензирования.

Сконфигурируйте web-доступ RemoteApp к службам терминалов сервера.

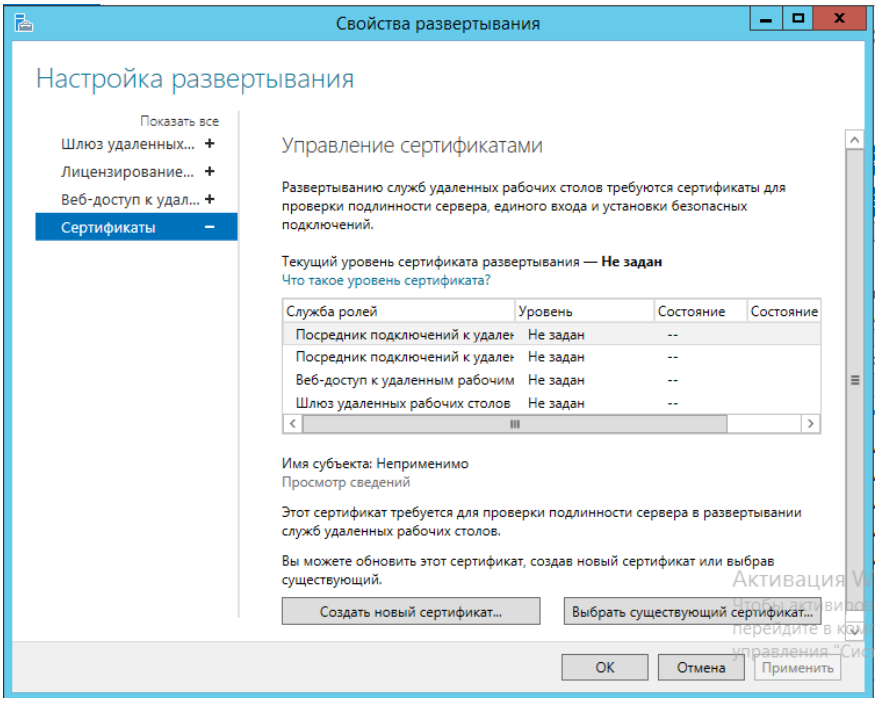
1. Настроим на терминальном сервере шлюз удаленных рабочих столов и выберем сервер.



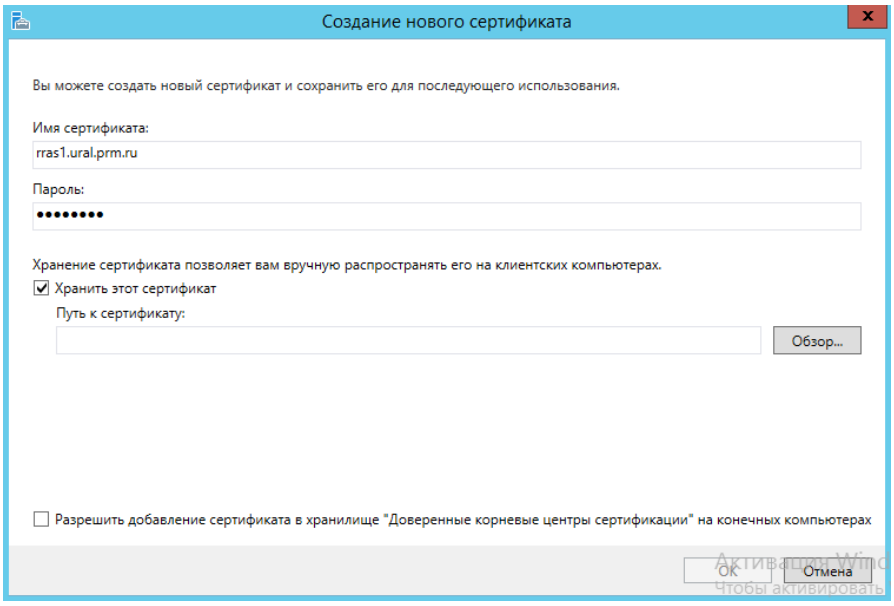
2. Введите имя сертификата.



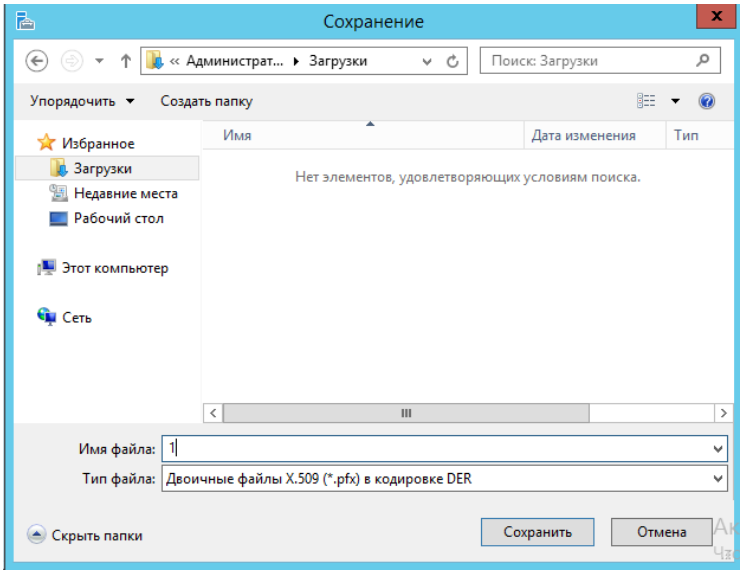
3. Закончите настройку.
4. Настройка сертификатов ***Задачи → Изменить настройку развертывания → Сертификаты***.



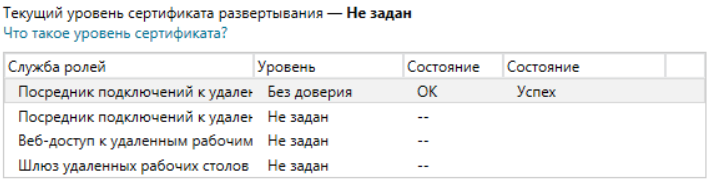
5. ***Выбрать посредник подключения к удаленному рабочему столу: включение единого входа → Создать сертификат***.



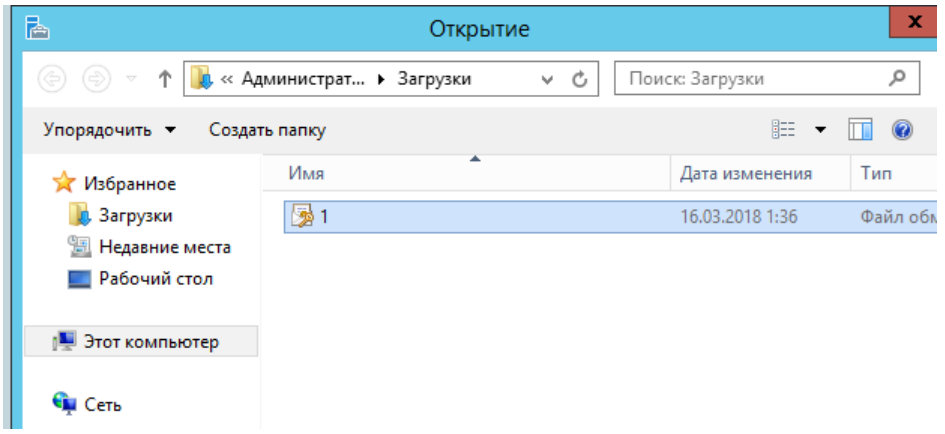
6. Нажать ***Обзор*** и выбрать место хранения сертификата (Документы).



7. Выбрать галочку ***Разрешить добавление сертификата в хранилище.*** После создания сертификата нажмите на кнопку ***Применить***.



8. Требуется назначить сертификат на все служба, выберете службу нажмите Выбрать существующий сертификат и выберете ране созданный сертификат.



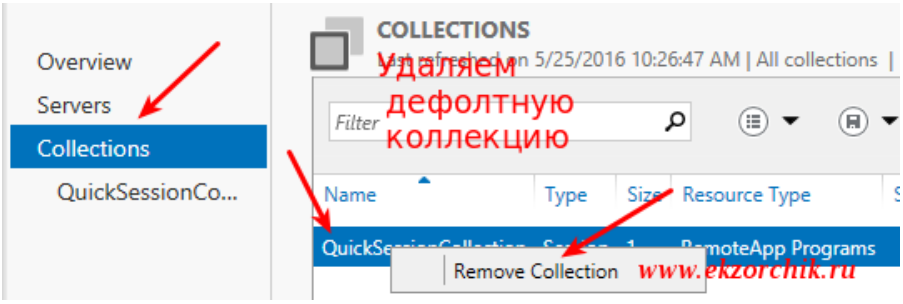
9. Нажмите на кнопку ***Применить***. Аналогично сделайте для остальных служб и нажмите OK.

Текущий уровень сертификата развертывания — **Без доверия**
Что такое уровень сертификата?

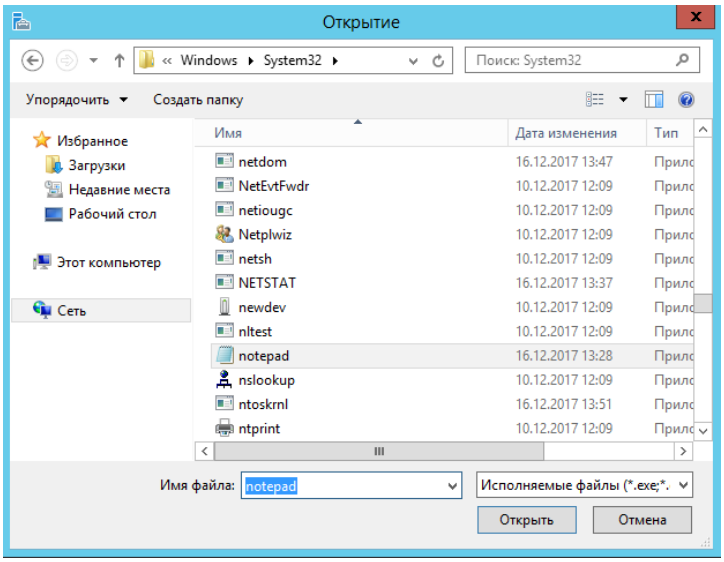
Служба ролей	Уровень	Состояние	Состояние
Посредник подключений к удален	Без доверия	OK	Успех
Посредник подключений к удален	Без доверия	OK	Успех
Веб-доступ к удаленным рабочим	Без доверия	OK	Успех
Шлюз удаленных рабочих столов	Без доверия	OK	Успех

Опубликуйте программу Блокнот на web-портале RemoteApp для членов группы Sales.

1. Удалить коллекцию по умолчанию Collections и в правой части через выделение дефолтной коллекции по правом клику нажимаем Remove Collection — Yes.



2. Удаляю дефолтную коллекцию опубликованных приложений.
3. Коллекции → Задачи → Создать коллекцию → Вводим имя IT → Выберем сервер. Убираем галочку ***Включит дисковые профили*** и завершаем создавать коллекцию.
4. Заходим в коллекцию в удаленном приложении выбираем Задачи → Опубликовать приложение → на диске с Windows\System32 выбираем notepad. И завершаем публикацию.



5. Выберете Блокнот и нажмите ПКМ → Изменить свойства → Переходим в назначение пользователей → Только указанные пользователи и группы → Выбрать нужную группу.

Опубликуйте программу Paint на web-портале RemoteApp для членов группы IT.

1. Аналогично добавить приложение и настроить приложение Paint и настроить группу.

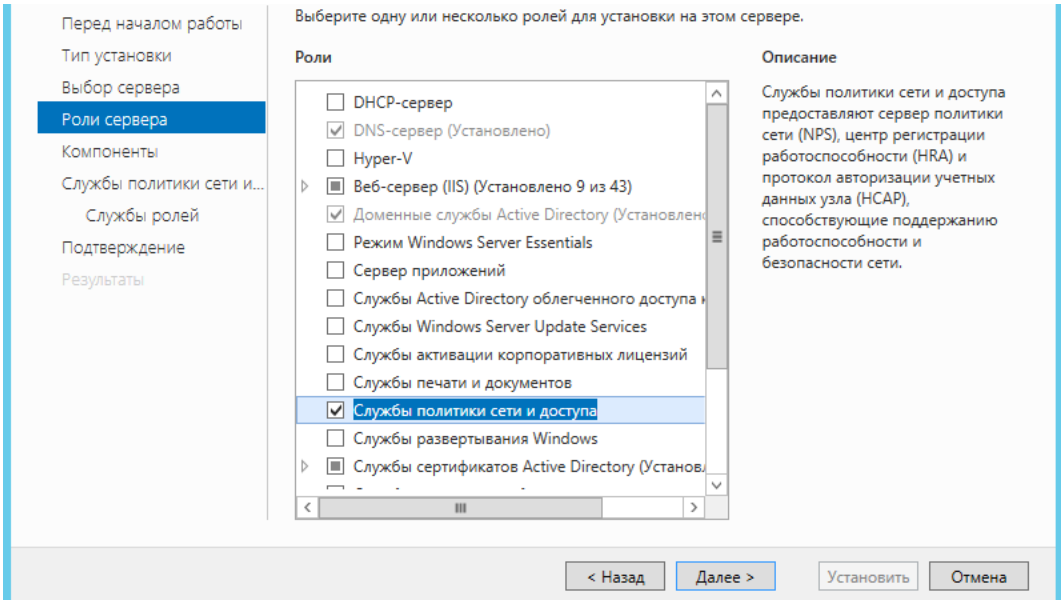
Web-интерфейс сервера должен быть настроен таким образом, чтобы пользователи могли автоматически получать доступ к форме входа на web-интерфейс удаленных рабочих столов при указании адресов http://rds.ural.prm.ru и https://rds.chel.prm.ru.

1. На сервере веб-доступ к удаленным рабочим столам запустите Диспетчер служб IIS. Для этого нажмите кнопку ***Пуск***, выберите пункт ***Администрирование*** и выберите команду ***Диспетчер Internet Information Services (IIS)***.
2. В левой области разверните имя сервера, узел узлы, разверните узел веб-узел по умолчанию, разверните узел RDWeb и нажмите кнопку страницы
3. В средней панели, под ASP.NET, дважды щелкните параметры приложения.
4. Чтобы изменить параметры веб-подключения к удаленному рабочему столу, измените значения на панели ***Параметры приложения***.
5. Чтобы настроить сервер шлюз удаленных рабочих столов по умолчанию, дважды щелкните DefaultTSGateway, введите полное доменное имя сервера в поле значение (например, server1.contoso.com) и нажмите кнопку ОК.

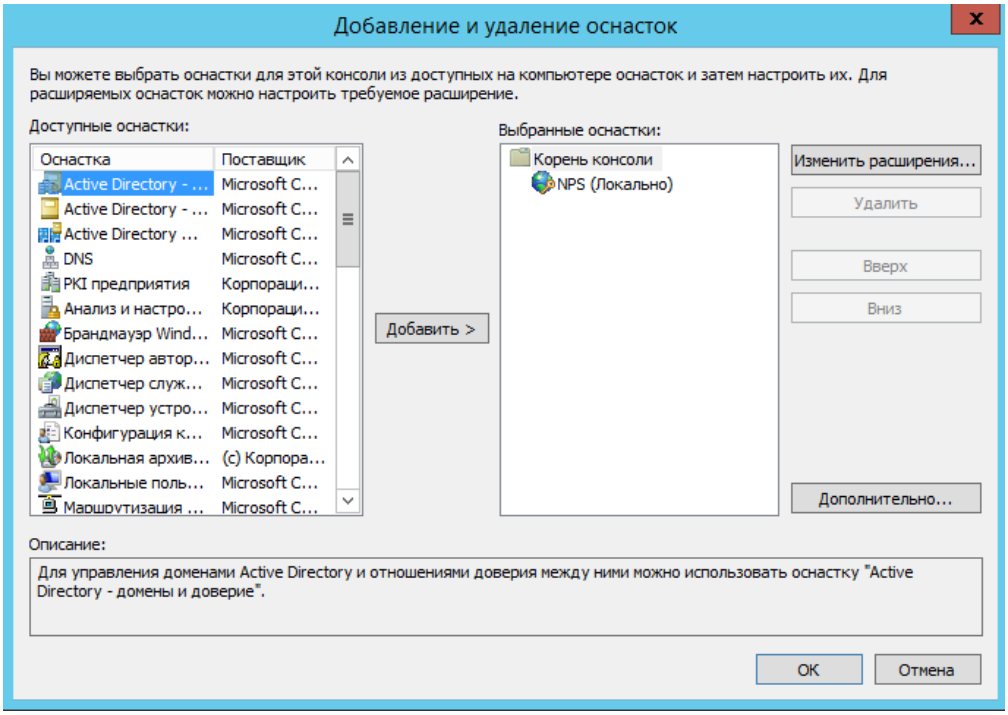
Службы политики сети и доступа

На сервере DC1 в офисе ural.prm.ru установите роль Службы политики сети и доступа.

1. Установить ***Службы политики сети и доступа*** (Откройте консоль Server Manager и установите роль ***Network Policy Server*** (находится в разделе ***Network Policy and Access Services***)).

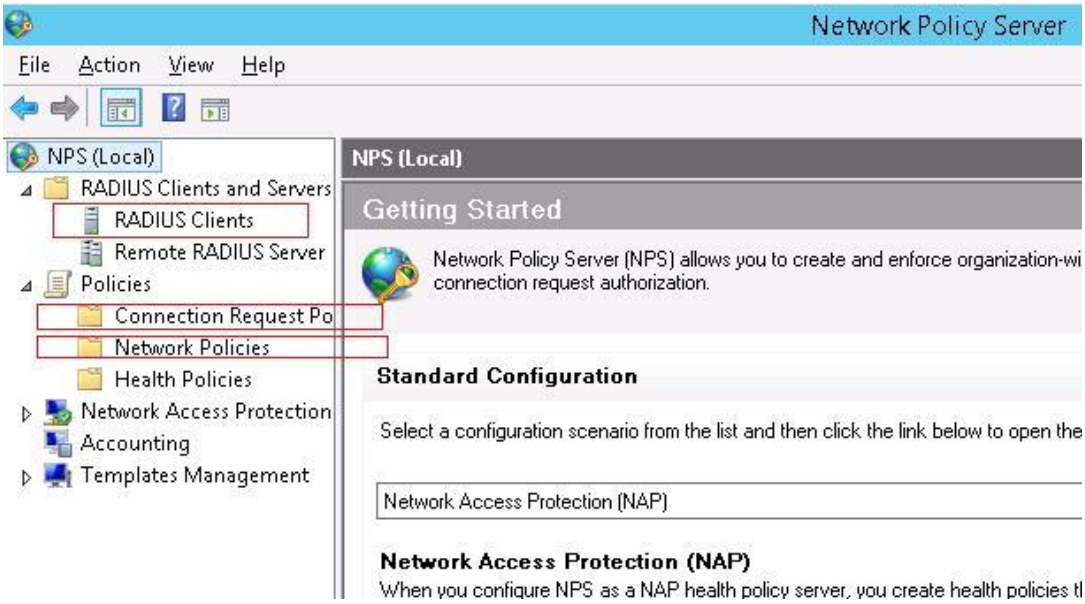


2. После окончания установки запустите mmc-консоль и добавьте консоль управления ***Network Policy Server***.



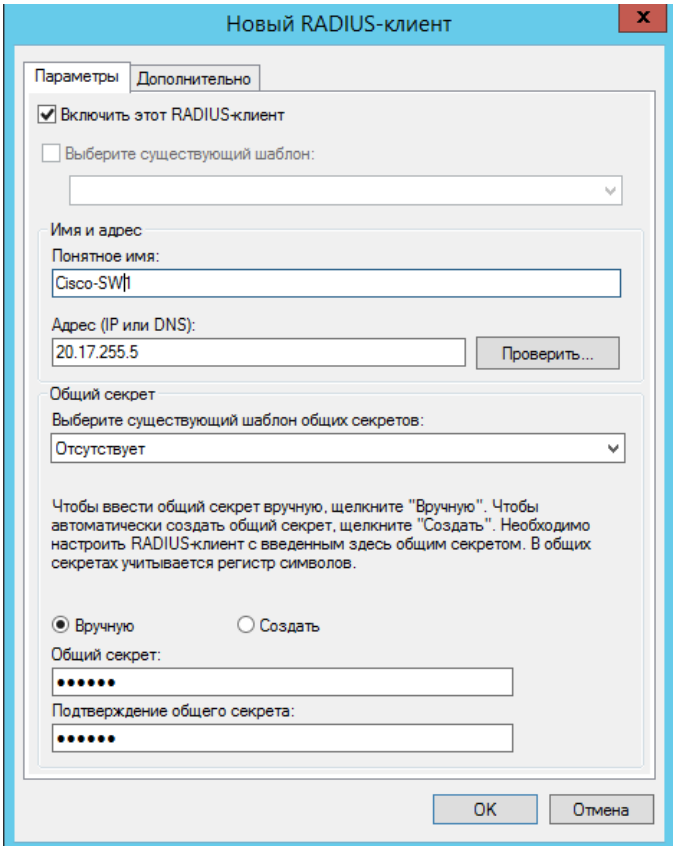
Нас интересуют три следующих раздела консоли:

- ***RADIUS Clients*** — содержит список устройств, которые могут аутентифицироваться на сервере
- ***Connection Request Policies*** – определяет типы устройств, которые могут аутентифицироваться
- ***Network Polices*** – правила аутентификации



3. Добавьте нового клиента RADIUS, щелкнув ПКМ по разделу ***RADIUS Clients*** и выберете ***New***. Укажите:

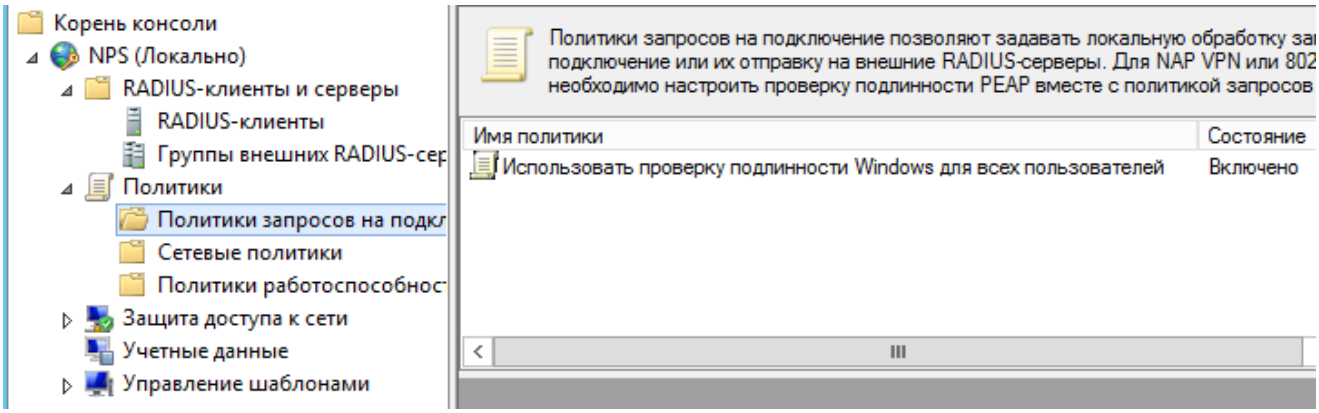
- Friendly Name: Cisco-SW1
- Address (IP or DNS): 20.17.255.5
- Shared secret (пароль/секретный ключ): пароль можно указать вручную (он должен быть достаточно сложным), либо сгенерировать с помощью специальной кнопки (сгенерированный пароль необходимо скопировать, т.к. в дальнейшем его придется указать на сетевом устройстве).



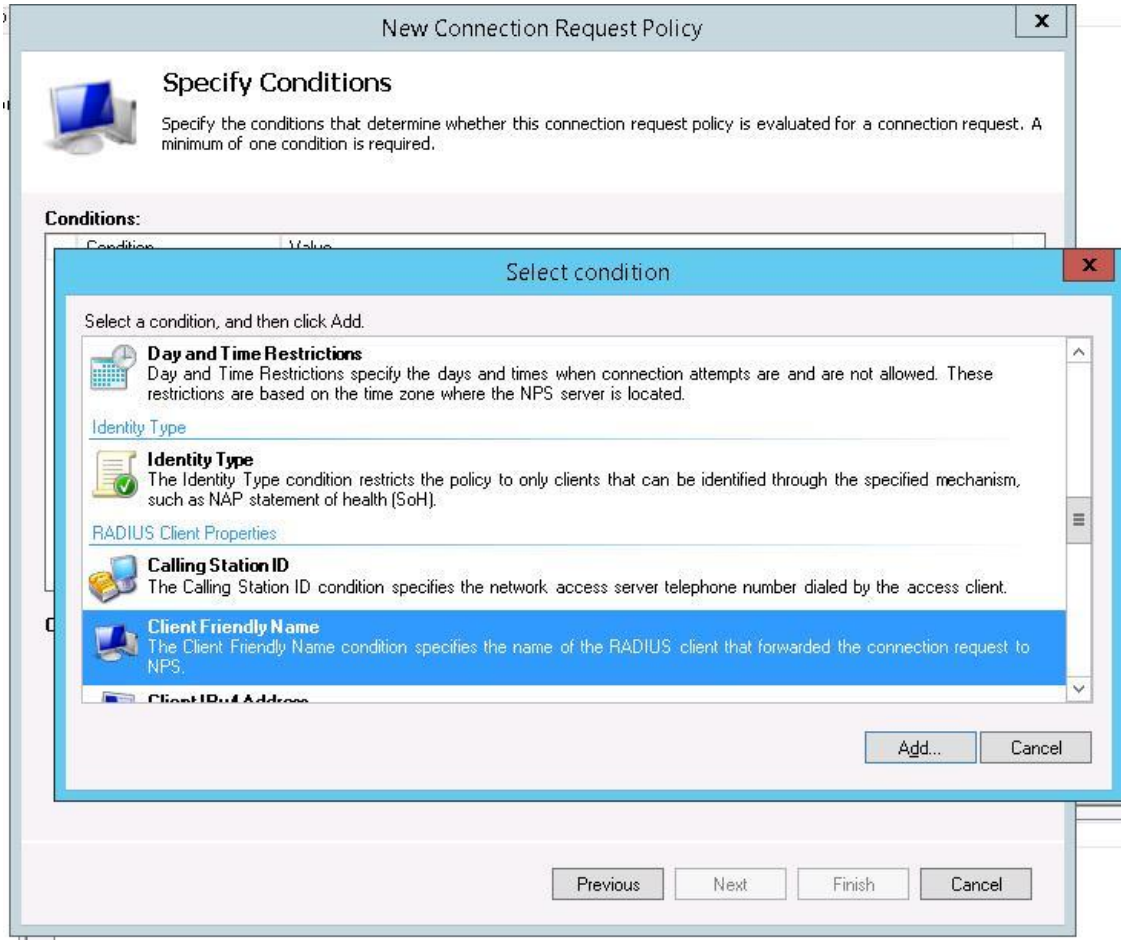
4. Создайте оставшихся пользователей.

Создайте новую политику доступа с названием CiscoTools для клиентов RADIUS. Действовать должна только созданная вами политика.

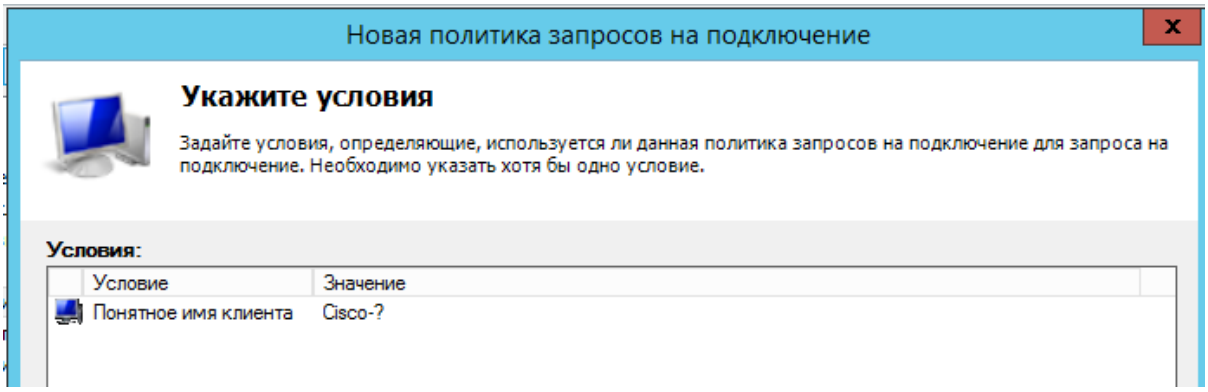
1. Отключим стандартную политику (***Use Windows authentication for all users***) в разделе ***Connection Request Policies***, щелкнув по ней ПКМ и выбрав ***Disable***.



2. Создадим новую политику с именем ***CiscoTools*** и нажимаем далее. В разделе ***Condition*** создадим новое условие. Ищем раздел ***RADIUS Client Properites*** и выбираем **Client Friendly Name**.

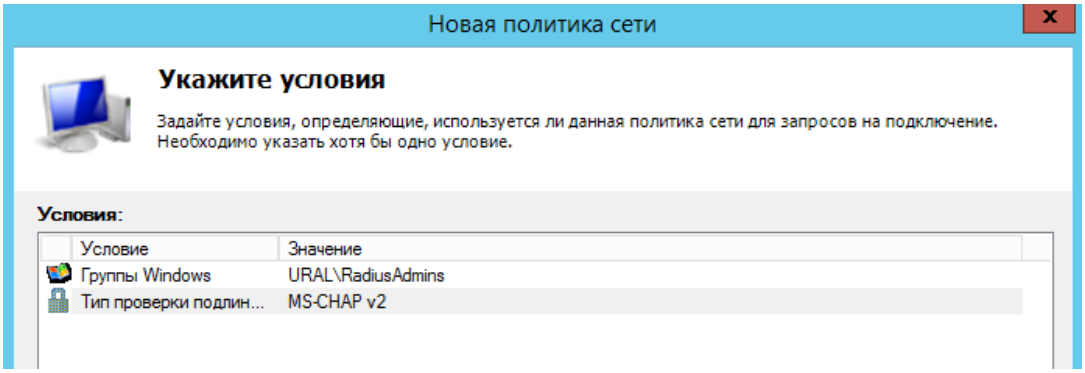


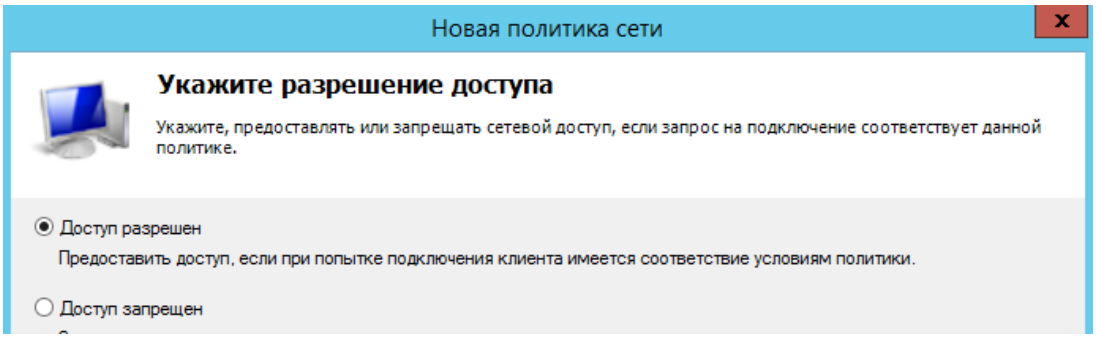
3. В качестве значения укажем **Cisco-?**. Т.е. условие будет применяться для всех клиентов RADIUS, начинающийся с символов :"Cisco -". Жмем Next->Next-> Next, соглашаясь со всеми стандартными настройками.



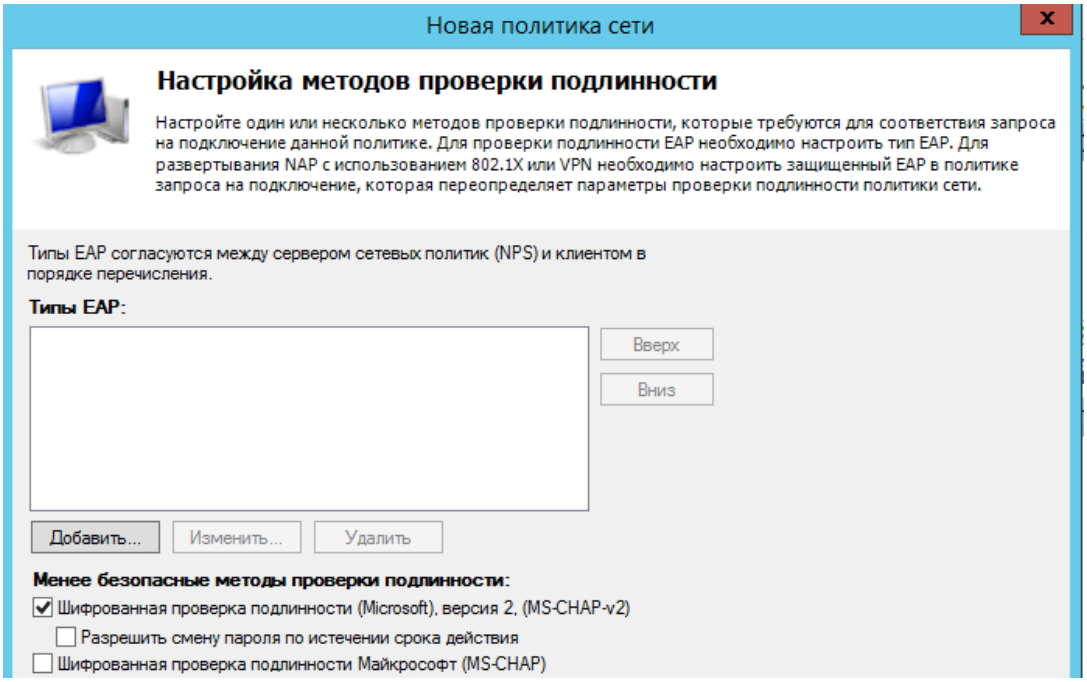
Создайте новую административную политику аутентификации с названием NewAuthPol в соответствии с которой члены доменной группы RadiusAdmins смогут аутентифицироваться по протоколу MSCHAP v2.

1. Далее в разделе ***Network Policies*** создадим новую политику аутентификации. Укажите ее имя ***NewAuthPol***. Создадим два условия: в первом условии ***Windows Groups***, укажем доменную группу, члены которой могут аутентифицироваться учетные записи сетевых администраторов в включённых в группу AD ***RadiusAdmins***, второе условие ***Authentication Type***, выбрав в качестве протокола аутентификации ***MSCHAP v2***.

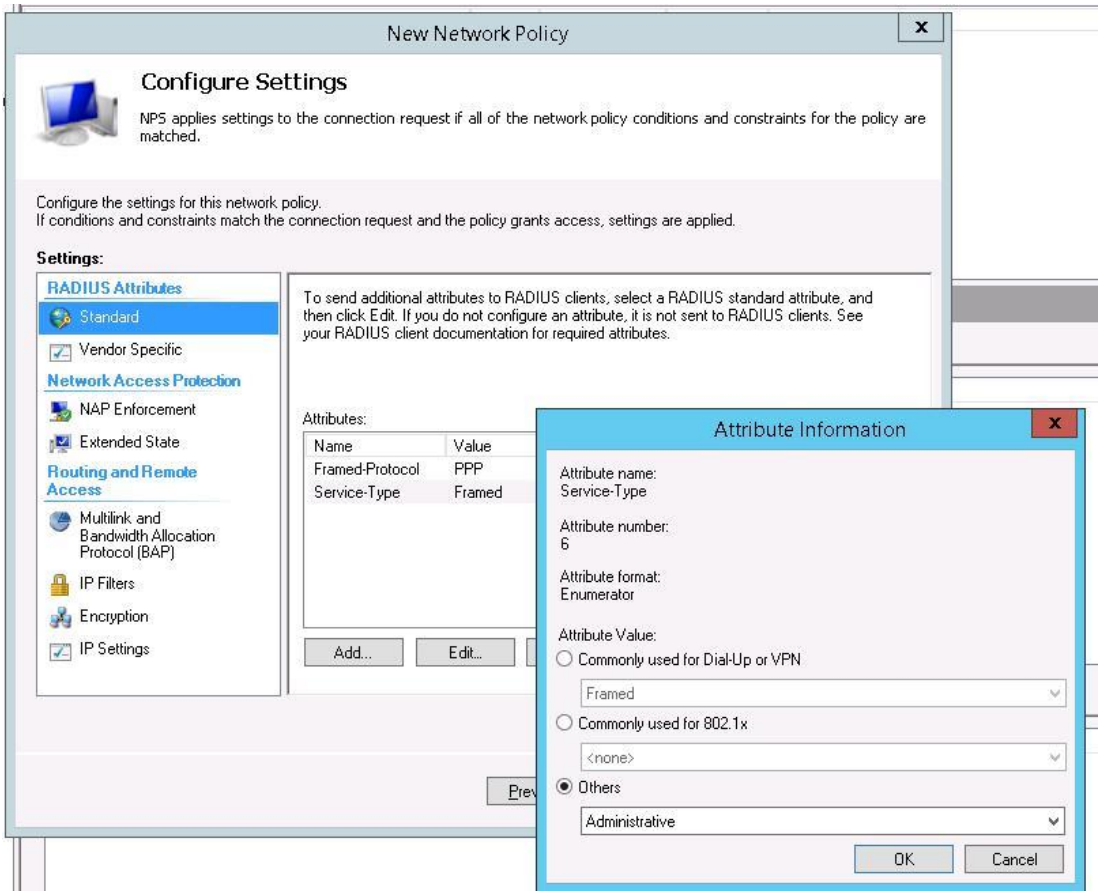




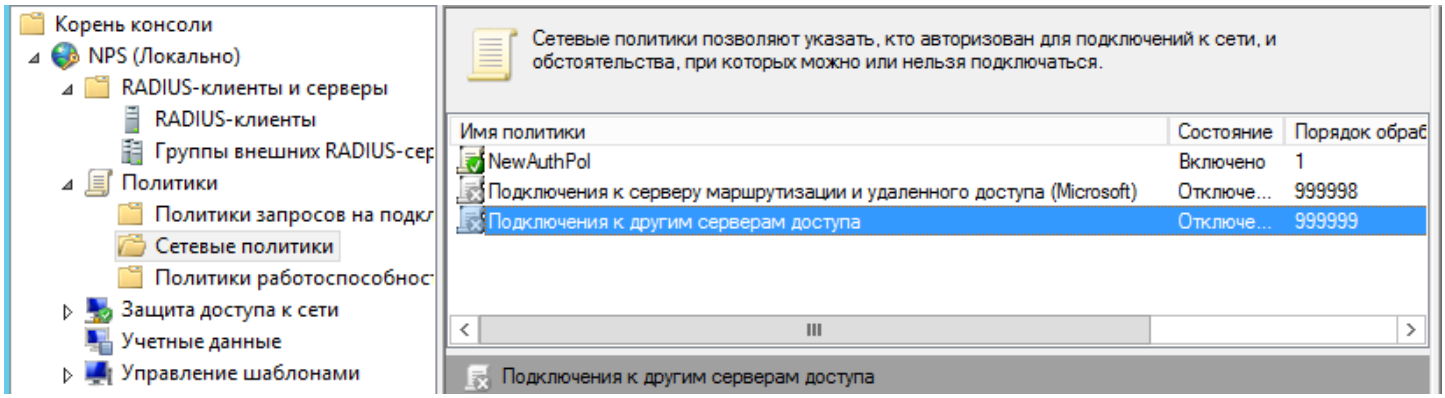
2. Далее в окне ***Configure Authentication Methods*** снимаем галки со всех типов аутентификации, кроме ***MSCHAP v2***.



3. В окне **Configure Settings** изменим значение атрибута ***Service-Type*** на ***Administrative*** и Нажмите Enter.



4. В остальных случаях соглашаемся со стандартными настройками и завершаем работу с мастером. И, напоследок, переместим новую политику на первое место в списке политик.



http://winitpro.ru/index.php/2010/12/02/udalennyj-dostup-ts-web-access-cherez-ts-gateway/

http://itstuff.info/network/configure-radius-on-windows-server-2008-r2-and-cisco-router/
https://corp2.info/windows-server-2012-ustanovka-i-nastrojka-udalyonnyx-rabochix-stolov/