Развёртывание и настройка Active directory

Лекция предполагает наличие у студента лишь самых начальных знаний об устройстве сетей (на уровне "Что такое IP-адрес и DNS-адрес").

*Начальное состояние стенда:*

1. *На машине* ***windows\_server*** *уже установлена ОС Windows Server 2019 Standard Evaluation (с GUI). Машина находится в состоянии "сразу после установки ОС". В процессе лекции на ней будут развернуты службы Active Directory (с доменом mydomain.com), DNS и DHCP.*
2. *Машина* ***workstation*** *выполняет роль рабочей станции. На ней установлена ОС Windows 7. Машина находится в состоянии "сразу после установки ОС". В процессе лекции она будет подключена к домену mydomain.com.*

Оглавление

[Что такое Active Directory 2](#_Toc98795908)

[Предварительная настройка windows\_server 2](#_Toc98795909)

[Базовые настройки Windows Server 3](#_Toc98795910)

[Смена сетевого имени 3](#_Toc98795911)

[Включение необходимых компонентов 4](#_Toc98795912)

[Доменные службы Active Directory 4](#_Toc98795913)

[DNS-сервер 5](#_Toc98795914)

[DHCP-сервер 5](#_Toc98795915)

[Мастер добавления ролей и компонентов 6](#_Toc98795916)

[Выбор типа установки 6](#_Toc98795917)

[Выбор целевого сервера 7](#_Toc98795918)

[Выбор добавляемых ролей 8](#_Toc98795919)

[Выбор компонентов 8](#_Toc98795920)

[Подтверждение устанавливаемых ролей и компонентов 9](#_Toc98795921)

[Настройка контроллера домена Active Directory 10](#_Toc98795922)

[Конфигурация развёртывания 11](#_Toc98795923)

[Параметры контроллера домена 12](#_Toc98795924)

[Делегирование DNS 14](#_Toc98795925)

[NetBIOS-имя 14](#_Toc98795926)

[Расположение базы данных 15](#_Toc98795927)

[Проверка предварительных требований 16](#_Toc98795928)

[Настройка DHCP-сервера 16](#_Toc98795929)

[Авторизация DHCP-сервера в домене 18](#_Toc98795930)

[Настройка диапазона адресов 20](#_Toc98795931)

[Понимание имени родительского домена 21](#_Toc98795932)

[Настройки DNS 21](#_Toc98795933)

[Создаём нового пользователя в домене AD 22](#_Toc98795934)

[Ввод рабочей станции в домен 24](#_Toc98795935)

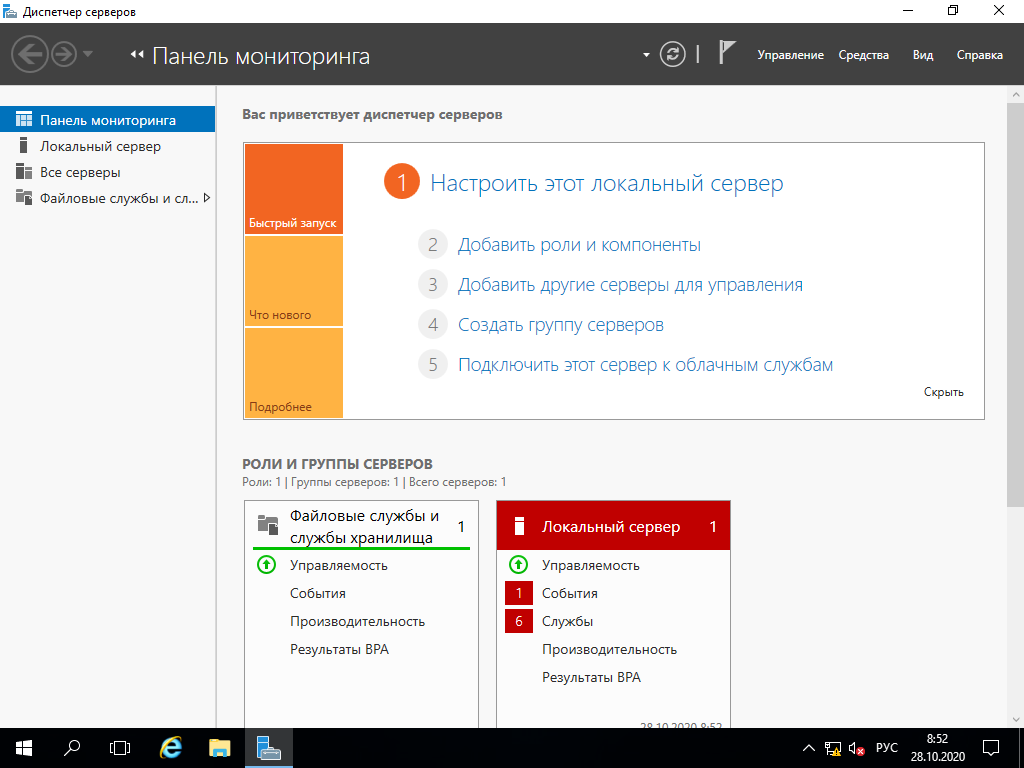
# Что такое Active Directory

**Active Directory** — это службы каталогов от компании Microsoft, как подсказывает нам Википедия. За этим сухим и невзрачным определением скрывается одна из важнейших технологий в администрировании сетей. Благодаря Active Directory администратор сети получает очень удобное централизованное средство управления учетными записями пользователей, групповыми политиками (в т.ч. политиками безопасности) и объектами в сети (причём Active Directory без особых проблем справляется даже с гигантскими сетями). А благодаря встроенному механизму репликации, "положить" правильно настроенные сервисы AD не так-то просто. Ну и напоследок, благодаря Windows настроить Active Directory можно буквально мышкой, так что даже совсем начинающие IT-шники смогут с этим справиться.

Несмотря на то, что технологией заведует Microsoft, она вовсе не ограничивается управлением Windows-машин — все известные Linux-дистрибутивы уже давно научились работать с этой технологией. Повстречаться с Active Directory не просто, а очень просто — практически каждый офис предполагает наличие этой технологии, поэтому даже самым заядлым любителям Linux было бы неплохо разбираться в азах работы Active Directory.

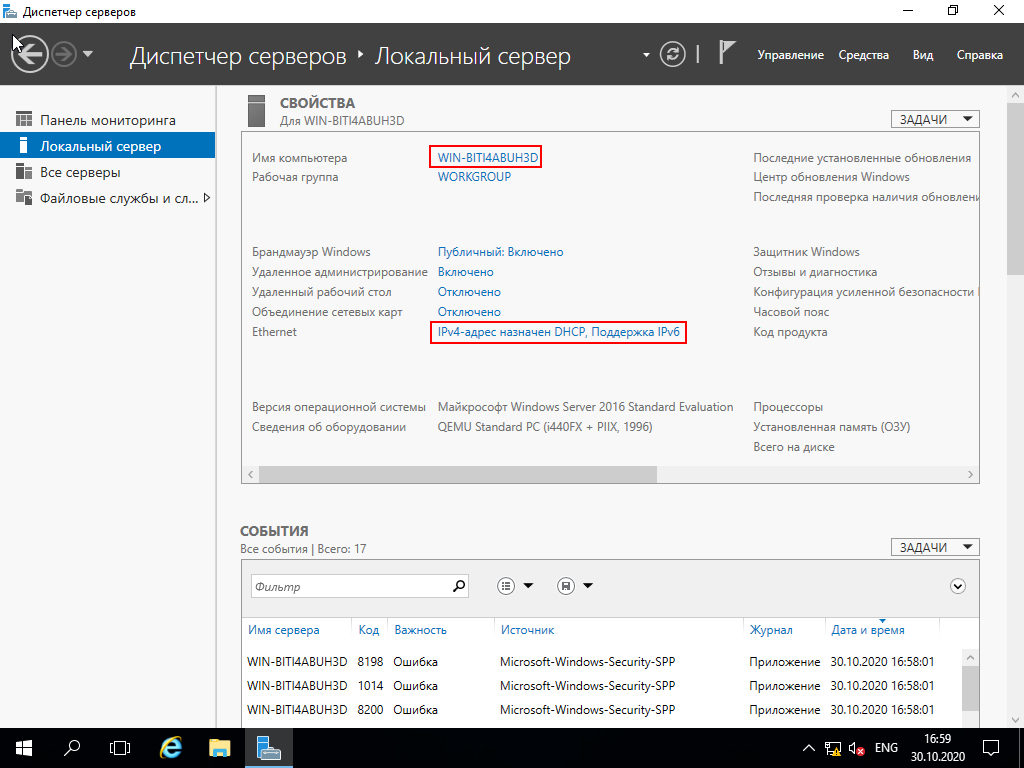
# Предварительная настройка windows\_server

Вы установили Windows Server 2019 и скорее всего видите следующий экран:



Эта панель — основное (графическое) средство администрирования Windows Server 2019. Здесь вы можете управлять компонентами и сервисами на вашем сервере (проще говоря, настраивать то, что умеет делать сервер). Эту же панель можно использовать и для базовых сетевых настроек Windows Server, для чего есть вкладка "Локальный сервер".

## Базовые настройки Windows Server



Первое, что нужно сделать — это поменять сетевое имя сервера.

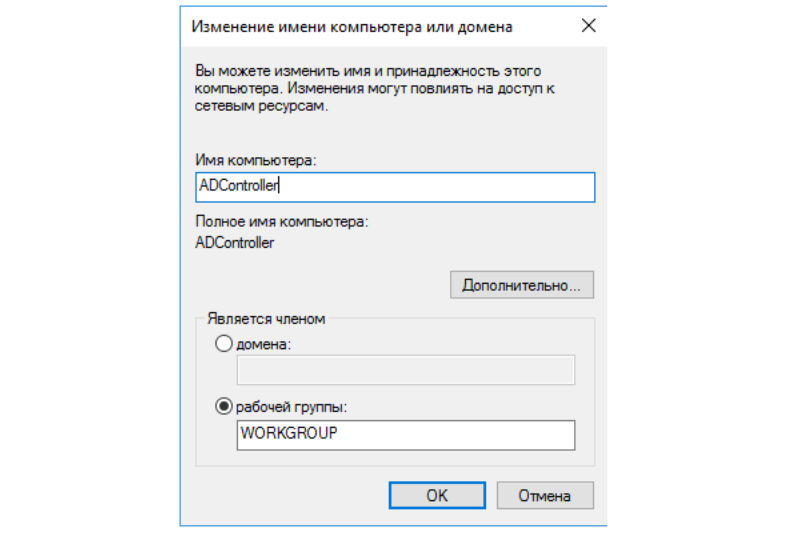
Сетевое имя (hostname) — это удобный способ идентификации узла в сети. Сетевое имя используется как альтернатива IP-адресу и позволяет не запоминать IP-адрес компьютера (при том, что этот адрес может меняться время от времени), а связываться с этим компьютером по его логическому названию.

Проблема в том, что по умолчанию для Windows Server генерируется совершенно нечитаемое и неинформативное сетевое имя (выделено красным цветом на скриншоте).

Рабочие станции ещё могут позволить себе иметь нечитаемый Hostname, но никак не сервер. Поэтому предлагается поменять это имя на что-то более осмысленное (например, на ADController), делается это быстро.

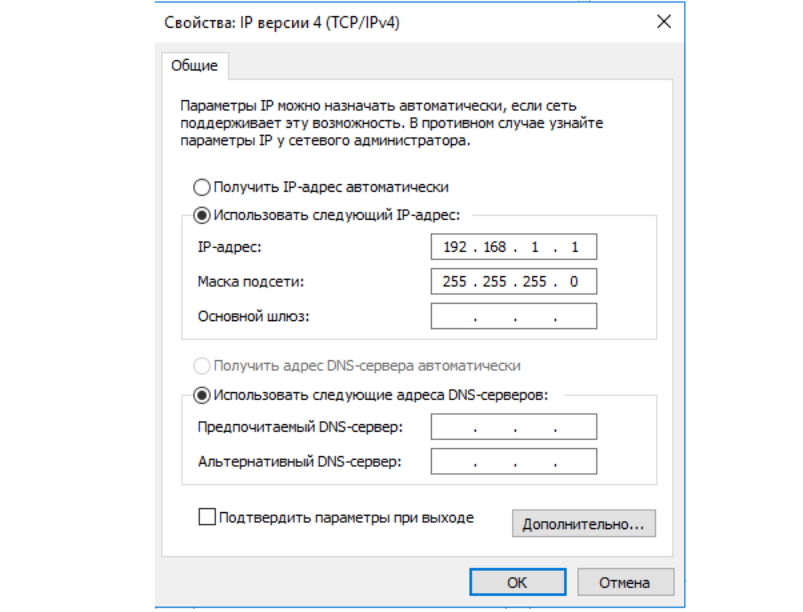
## Смена сетевого имени

Нужно кликнуть на текущее имя сервера (отмечено красным цветом), затем во вкладке "Имя компьютера" нажать на кнопку "Изменить...", после чего ввести что-то более удобное:



После смены имени машину нужно будет перезагрузить.

Теперь зададим статический IP-адрес для сервера. Чаще всего это делать не обязательно, учитывая мы всё равно собрались поднимать DHCP службу, но на самом деле это хорошая практика, когда все ключевые элементы корпоративной сети имеют фиксированные адреса. Открыть меню по настройке сетевого адаптера можно из вкладки "Локальный сервер", кликнув на текущие настройки Ethernet-адаптера (тоже выделены красным цветом).



# Включение необходимых компонентов

Для нашего стенда нам понадобится включить следующие сервисы (или, как они тут называются, роли) на Windows Server:

* Доменные службы Active Directory;
* DNS-сервер;
* DHCP-сервер.

Пройдемся вкратце по каждому из них.

## Доменные службы Active Directory

Эта роль фактически "включает" технологию Active Directory на сервере и делает его контроллером домена (под доменом в технологии AD понимается группа логически связанных объектов в сети). Благодаря этой роли администратор получает возможность управлять объектами в сети, а также хранить информацию о них в специальной распределенной базе данных.

Эта база данных содержит всю информацию об объектах в сети (например, именно в неё заносится информация об учётных записях пользователей). Когда человек подходит к рабочей станции и пытается выполнить вход в свою доменную учётную запись, эта рабочая станция связывается с контроллером домена с запросом на аутентификацию, и в случае успеха загружает пользовательский рабочий стол.

Однако, что же делать, если контроллер домена выйдет из строя (или просто будет недоступен для рабочих станций)? Если вы настроили только один контроллер домена, то дела ваши довольно плохи — без связи с рабочим контроллером домена пользователи не смогут выполнить вход на свои рабочие места. Поэтому в реальных сетях всегда рекомендуется устанавливать, как минимум два контроллера на каждый домен. Каждый контроллер домена участвует в так называемом механизме репликации, благодаря чему все контроллеры домена имеют полную копию базы данных со всеми объектами в домене. Если по какой-то причине один из контроллеров выйдет из строя, его место всегда может занять резервный контроллер — и пользователи даже ничего не заметят.

## DNS-сервер

Обычно протокол DNS (Domain Name System) используется для обращения к узлам в сети не по их IP-адресу, а по доменному имени (строковый идентификатор), что, конечно, гораздо удобнее. Другими словами, DNS чаще всего используется для разрешения доменных имен.

Но область применения протокола DNS не ограничивается только сопоставлением хостового имени и IP-адреса, что как раз подтверждает технология Active Directory. Дело в том, что Microsoft решила построить технологию Active Directory не с нуля, а на основе протокола DNS. В частности, протокол DNS используется при определении местонахождения всех ключевых сервисов Active Directory в сети. Другими словами, рабочая станция при подключении к контроллеру домена понимает, "куда" ей надо обращаться, именно с помощью протокола DNS.

Все DNS-записи (в том числе с информацией о сервисах Active Directory) хранятся на DNS-сервере, а это значит, что нам нужно заиметь свой собственный DNS-сервер! Вот только вопрос, откуда его взять? Есть два варианта:

* Использовать отдельную машину в роли DNS-сервера;
* Использовать саму машину windows\_server в роли DNS-сервера.

Первый вариант, безусловно, самый правильный — именно так и надо поступать при реальном администрировании сетей (чем больше вы разносите логику по разным узлам в сети — тем лучше). Но в учебных целях я решил выбрать второй вариант (хотя бы потому, что не придётся создавать ещё одну виртуальную машину).

Именно поэтому эту роль (DNS-сервера) тоже нужно добавить к ролям машины windows\_server.

Кстати, если не добавить роль "DNS-сервер" сейчас, то в будущем у вас ещё будет такая возможность при конфигурировании контроллера домена AD.

## DHCP-сервер

Протокол DHCP (Dynamic Host Configuration Protocol) нужен для автоматической выдачи сетевых настроек узлам в сети. Под сетевыми настройками понимается IP-адрес, адрес шлюза по умолчанию, адрес DNS-сервера, и ещё ряд других настроек. Этот протокол чрезвычайно удобен при администрировании сетей, особенно больших.

Протокол DHCP не имеет никакого отношения к технологии Active Directory, и можно было бы обойтись вовсе без него (достаточно прописать все сетевые настройки на рабочей станции самостоятельно), но я решил включить этот протокол в данную лекцию просто для общего ознакомления. К тому же, такая связка "Контроллер AD — DNS-сервер — DHCP-сервер" довольно часто встречается в реальной жизни, потому что это очень удобный набор сервисов.

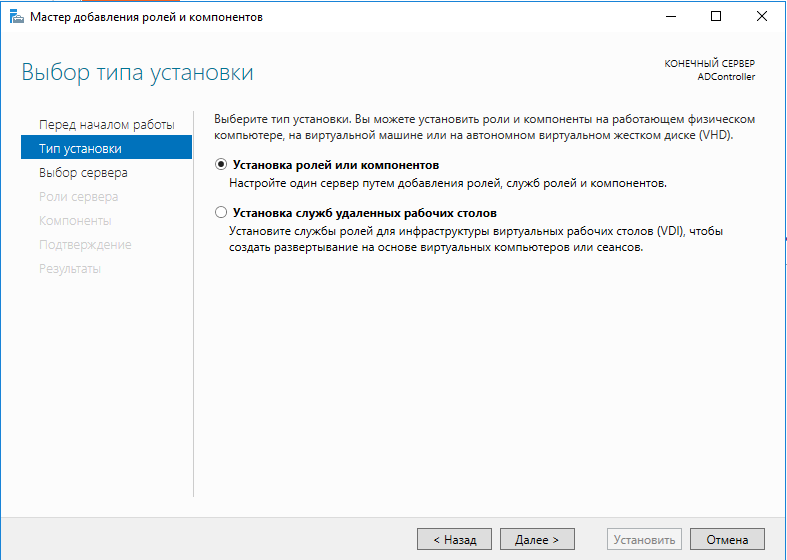
При этом вопрос о том, стоит ли выделять отдельную машину под DHCP-сервер, остаётся открытым. Для небольших сетей однозначно не стоит разносить DNS и DHCP-серверы по разным машинам, но для больших сетей, возможно, имеет все-таки смысл задуматься об этом. В нашей же крошечной сети мы абсолютно ничего не потеряем, если включим DHCP-сервер на той же машине, что и DNS-сервер.

Теперь перейдём к включению этих самых ролей.

# Мастер добавления ролей и компонентов

Возвращаемся на панель мониторинга (самый первый скриншот) и щелкаем на пункт "Добавить роли и компоненты". Вас поприветствует мастер добавления ролей и компонентов. Первый экран ("Перед началом работы") пропускаем, он совсем неинтересный, а вот дальше идёт экран "Выбор типа установки".

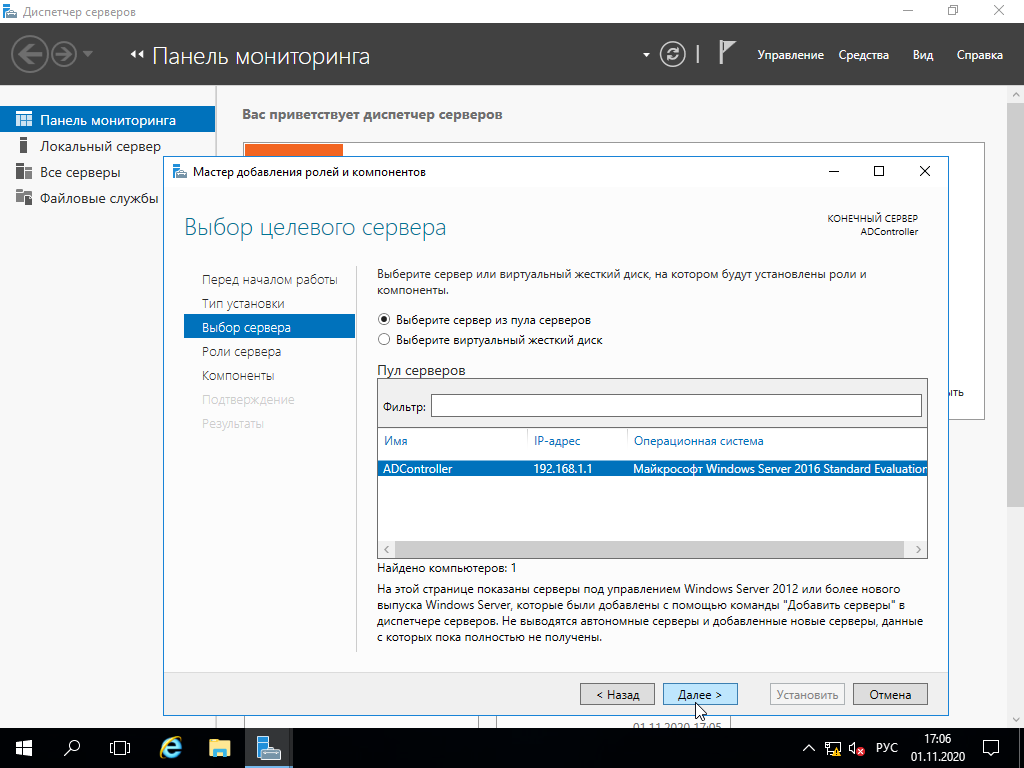
## Выбор типа установки



Нас устраивает значение по умолчанию (Установка ролей или компонентов"), но интересен и второй пункт — он позволяет задействовать ещё одну возможность Windows Server — инфраструктуру виртуальных рабочих мест (Virtual Desktop Environment — VDI). Эта интереснейшая технология позволяет, буквально, виртуализировать рабочее место. То есть для пользователя создаётся виртуальное рабочее место, к которому он может подключаться через тонкий клиент. Пользователь лишь видит картинку, тогда как само рабочее место может совершенно прозрачно работать где угодно.

Впрочем, технология VDI это отдельная большая тема, а в этой лекции надо сосредоточиться на контроллере AD, так что кликаем "Далее" и видим экран выбора целевого сервера.

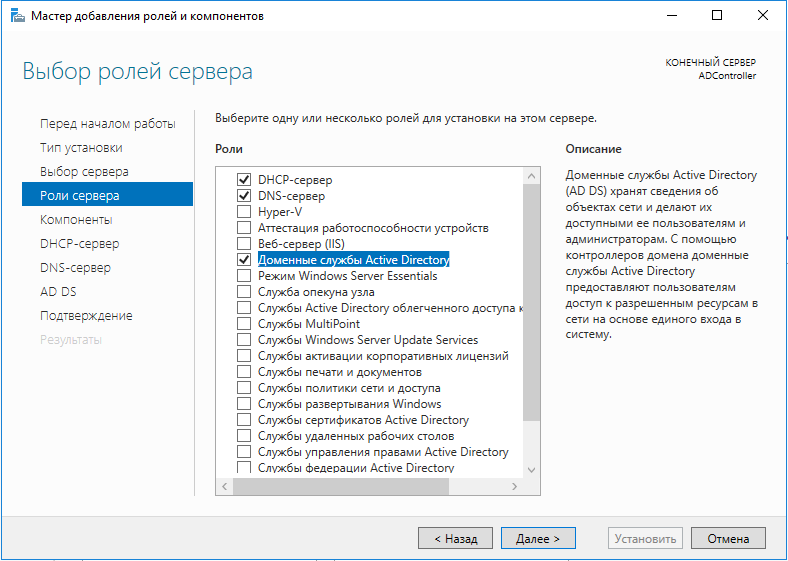
## Выбор целевого сервера



Мастер добавления ролей позволяет устанавливать роль не только на текущую машину, но вообще на любой добавленный сервер, и даже на виртуальный жёсткий диск. Да, если ваша Windows Server развернута на виртуальной машине (а это довольно частое явление), то вы можете администрировать эту виртуальную машину даже не запуская её!

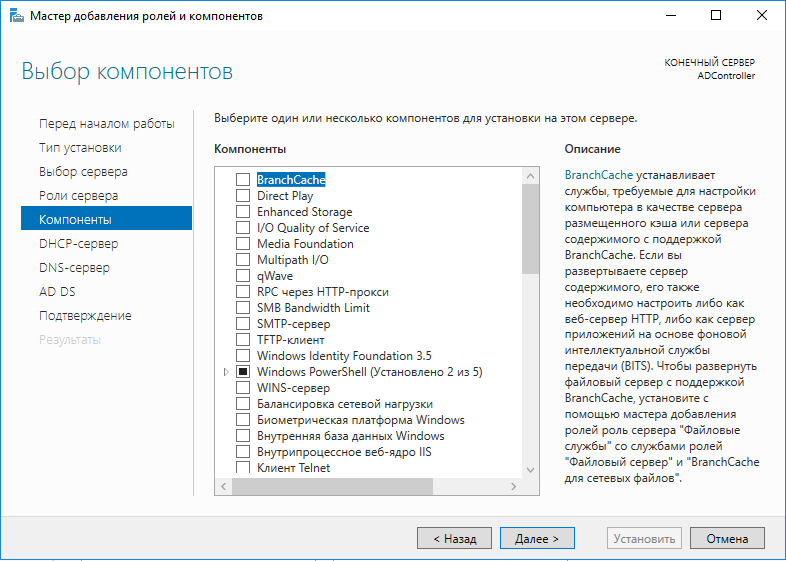
Выбираем единственный возможный сервер (обратите внимание, что он теперь называется ADController), жмём "Далее" и, наконец, попадаем на экран выбора ролей, которые нужно добавить.

## Выбор добавляемых ролей



Выбираем три роли, о которых уже говорили ранее, и продолжаем.

## Выбор компонентов



Теперь необходимо выбрать дополнительные компоненты.

*В чём разница между ролью и компонентом, можете спросить вы?*

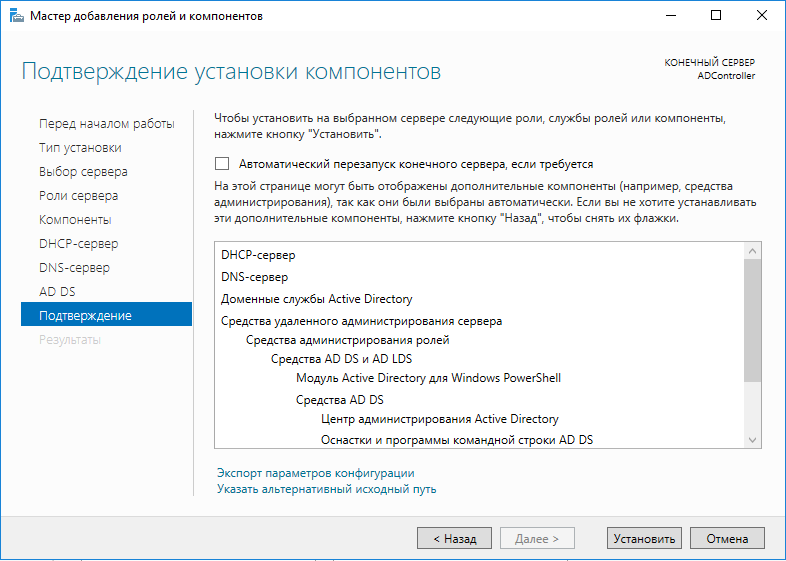
*Согласно идеологии Microsoft, роль — это набор программ, которые позволяют компьютеру предоставлять некоторые функции для пользователей в сети. Например, DNS, DHCP, контроллер домена AD — это всё роли. А вот компоненты — это набор программ, которые улучшают либо возможности ролей сервера, либо самого сервера.*

*При этом глядя на список "Компонентов" так сходу и не скажешь, что какие-то вещи в списке лишь "вспомогательные". Вот, например, DHCP-сервер расценивается как роль, а WINS-сервер — уже как компонент. А чем SMTP-сервер хуже DNS?*

*В общем-то, чёткой границы между ролью и компонентом не существует. Я лично предпочитаю относиться к ролям, как к большим функциональным возможностям сервера, а к компонентам — как к небольшим дополнениям.*

В любом случае, дополнительные компоненты нам не нужны, так что кликаем "Далее". После этого идёт несколько пояснительных экранов с информацией по каждой добавленной роли.

## Подтверждение устанавливаемых ролей и компонентов

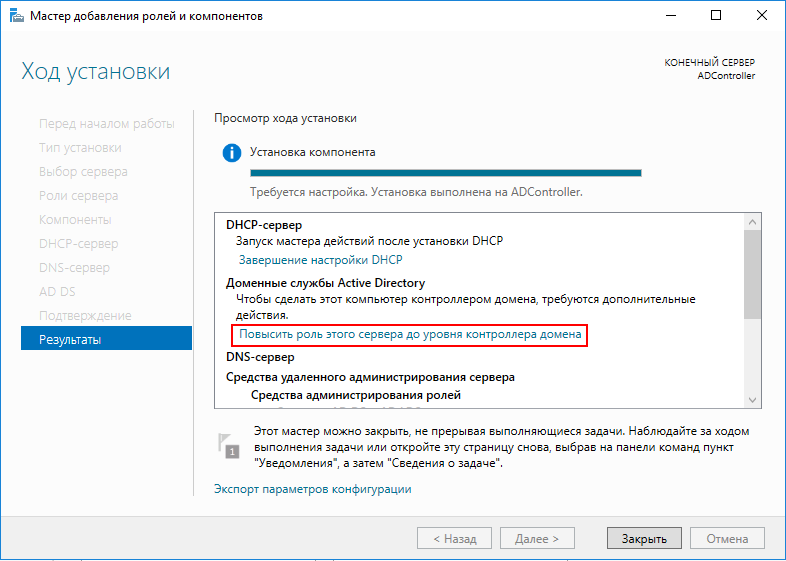


На экране подтверждения ещё раз видим все устанавливаемые роли и компоненты, после чего жмём "Установить".

Остаётся лишь дождаться, когда заполнится полоса прогресса, и перейти к следующему пункту лекции — настройке контроллера домена AD.

# Настройка контроллера домена Active Directory

Все роли и компоненты успешно добавлены, о чём свидетельствует следующий экран:

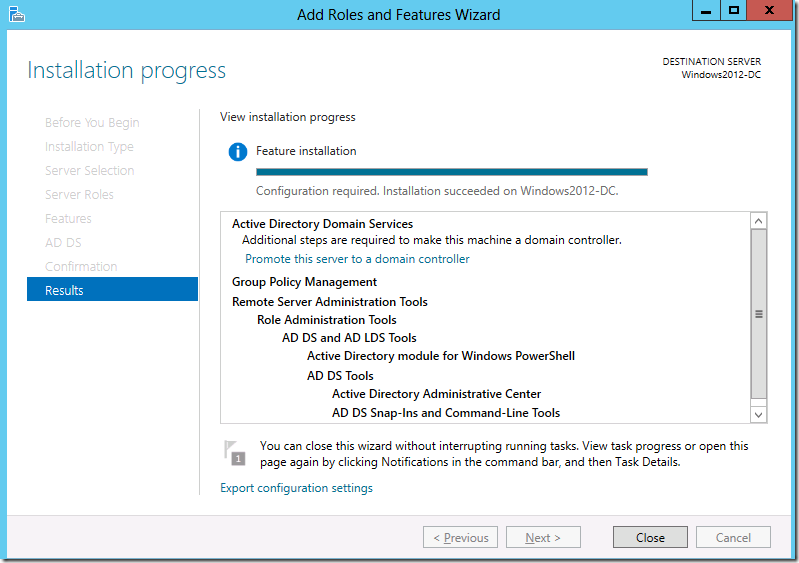


Сейчас AD на сервере всё еще не работает — для этого его необходимо донастроить. Для этого нам настойчиво предлагают "Повысить роль этого сервера до уровня контроллера домена".

У внимательно изучающего лекцию студента мог возникнуть вопрос:

*Чем же я занимался последние 15 минут? Я же добавлял роли, и судя по сообщению, они успешно добавились! И тут меня снова хотят заставить добавлять какие-то новые роли? В чем-то тут подвох.*

Подвох тут действительно имеется, но вообще в не самом очевидном месте. Вот так выглядит предыдущий скриншот в английской версии Windows Server (картинка из интернета):

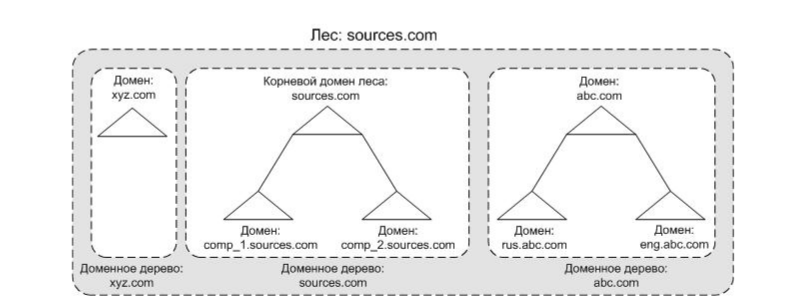


Здесь видно разницу. В английской версии не упоминаются ни какие роли. Про повышение есть, про роли — нет. Один из тех случаев, когда перевод вносит сумятицу на пустом месте. Согласно английской версии, никакими ролями мы дальше не занимаемся, что и логично, ведь мы их как раз только что добавили.

Разобравшись с профессиональным переводом Windows, мы нажимаем на предложение "Повысить роль этого сервера до уровня контроллера домена", и теперь нас приветствует мастер настройки доменных служб Active Directory с предложением выбрать конфигурацию развёртывания.

## Конфигурация развёртывания

Всего тут есть 3 варианта развития событий. Для того, чтобы выбрать правильный пункт, давайте сначала разберёмся, что эти пункты означают. В этом нам поможет вот такая картинка:



Технология Active Directory (как и DNS) подразумевает иерархическое построение имён на основе доменов. Домены могут выстраиваться в доменные деревья по принципу "родительско-дочерних" отношений. В основе дерева лежит так называемый корневой домен (на картинке выше это sources.com, xyz.com и abc.com). При этом домен может иметь сколько угодно потомков. Домен-потомок располагается в пространстве имён родителя и является его "поддоменом" (subdomain). У доменного имени домена-потомка есть дополнительный префикс относительно доменного имени родителя (rus.abc.com, eng.abc.com). Один корневой домен основывает только одно доменное дерево со своим независимым пространством имён.

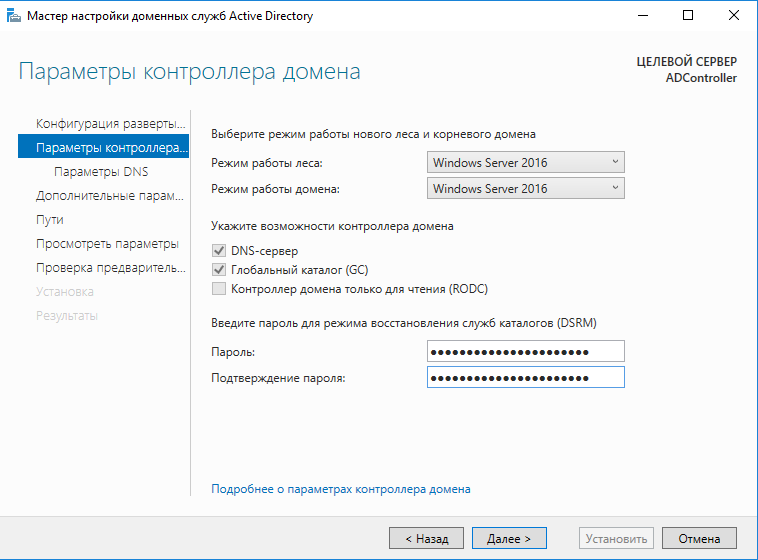
Теперь представьте, что таких независимых деревьев может быть много — в этом случае эти деревья образуют структуру, которая называется "лес". При этом в Active Directory доменные деревья не могут быть "сами по себе" — они обязательно должны находиться в лесу (даже если лес будет состоять всего из одного-единственного домена). Первый домен, который добавляется в лес, называется корневым доменом леса (на рисунке выше это sources.com). Корневой домен леса используется для идентификации всего леса (то есть если корневой домен называется sources.com, то и весь лес называется sources.com).

Теперь возвращаемся к мастеру настройки доменных имен. На этом этапе мастер предлагает следующие варианты:

1. Добавить контроллер домена в существующий домен (помните про резервирование контроллеров в домене, так ведь?). Этот вариант не для нас, ведь домена ещё никакого нет;
2. Добавить новый домен в лес. Этого мы тоже сделать не можем, т.к. и леса у нас тоже никакого нет;
3. Добавить новый лес. Это вариант как раз для нас. При этом нам тут же предлагают выбрать корневой домен для этого леса (первый домен, который будет создан в лесу).

Назовём корневой домен mydomain.com и кликнем "Далее".

## Параметры контроллера домена



Рассмотрим возможные параметры:

1. Режим работы леса и домена. Домены в одном лесу могут работать в разных режимах в зависимости от версии Windows Server на борту. Лес должен иметь режим не выше, чем самый "старый" домен в его составе. Т.к. мы планируем использовать только Windows Server 2019, то оставим этот режим и для леса, и для домена;
2. DNS-сервер. Если ранее Вы не активировали роль DNS-сервера в мастере добавления ролей, то можете сделать это сейчас (вам даже предложат такой вариант по умолчанию);
3. Должен ли контроллер домена выступать в роли Global Catalog-сервера.

Пункт 3 рассмотрим поподробнее, он довольно интересный.

Как уже упоминалось выше, каждый контроллер домена имеет полную и исчерпывающую информацию обо всех объектах в своём домене. Если же в домене несколько контроллеров, то они ещё и участвуют в механизме репликации, поддерживая несколько актуальных копий базы данных с объектами домена. Получается, что рабочая станция в домене может узнать информацию о любом объекте из этого домена от своего ближайшего контроллера домена.

Но что же делать, если рабочей станции нужно получить информацию об объекте из другого домена? И вот тут в дело вступает ещё один важнейший механизм технологии Active Directory, который называется глобальный каталог.

Что такое вообще "Глобальный каталог"? Согласно Microsoft — это распределенное хранилище данных, которое хранит частичное представление обо всех AD-объектах в лесу. Это хранилище располагается на котроллерах домена, которые имеют дополнительную роль "Global Catalog Server" (Сервер глобального каталога). От обычного контроллера домена GC-сервер отличается в первую очередь тем, что помимо полной копии всех объектов в своем домене, хранит также частичную информацию обо всех объектах в других доменах леса.

Чего это позволяет достичь? Давайте представим, что рабочая станция запросила информацию об объекте из другого домена. Она обращается на ближайший GC-сервер с просьбой предоставить ей информацию об этом объекте. GC-сервер, в свою очередь, может:

* Либо отдать рабочей станции нужную информацию сразу (если эта информация у GC-сервера имеется);
* Либо перенаправить запрос к нужному контроллеру домена, где эта информация точно будет находиться. Чтобы понять, какому контроллеру домена нужно перенаправить запрос, как раз и происходит поиск по GC.

Информация о том, какие атрибуты попадают в глобальный каталог, определена в Partial Attribute Set (PAS), который может настраивать администратор AD. Например, если администратор понимает, что рабочие станции часто будут обращаться к атрибуту, который не содержится в глобальном каталоге, он может добавить туда этот атрибут. Тогда запросы рабочих станций при чтении этого атрибута будут выполняться значительно быстрее, т.к. уже ближайший GC-сервер сможет предоставить им всю нужную информацию.

Однако, если в лесе всего один домен (как у нас), то Глобальный каталог содержит полную копию объектов в домене и всё.

Что ж, возвращаемся к галочке GC, которую за нас уже проставил мастер настройки доменных служб. Если вы попробуете её отключить, то убедитесь, что отключить её нельзя. Это связано с тем, что каждый домен в AD должен иметь хотя бы один GC-сервер, и при добавлении первого контроллера в домен этот контроллер сразу помечается как GC-сервер.

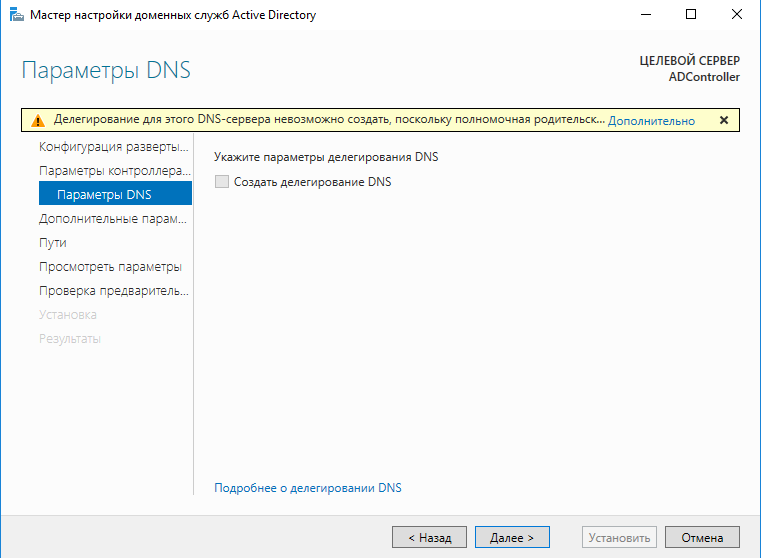
Мы согласимся с этим "выбором" мастера и перейдём к последнему параметру на этом скриншоте — к паролю для режима восстановления служб каталогов. Это особый режим безопасной загрузки Windows Server, который позволяет администратору работать с базой данных AD. Этот режим применяется, например, в следующих случаях:

* база Active Directory повреждена и нуждается в исправлении;
* требуется выполнить обслуживание базы данных AD (сжатие, анализ на наличие ошибок);
* требуется восстановить резервную копию базы данных AD;
* требуется сменить пароль администратора.

Да, чтобы просто восстановить резервную копию базы данных, нужно перезагрузить машину и загрузиться в особом "безопасном" режиме. ~~Это вам не Linux какой-нибудь (~~[~~История chroot~~](https://habr.com/ru/company/selectel/blog/655485/)~~).~~

Теперь перейдем дальше на шаг, где нам предложат настроить делегирование DNS.

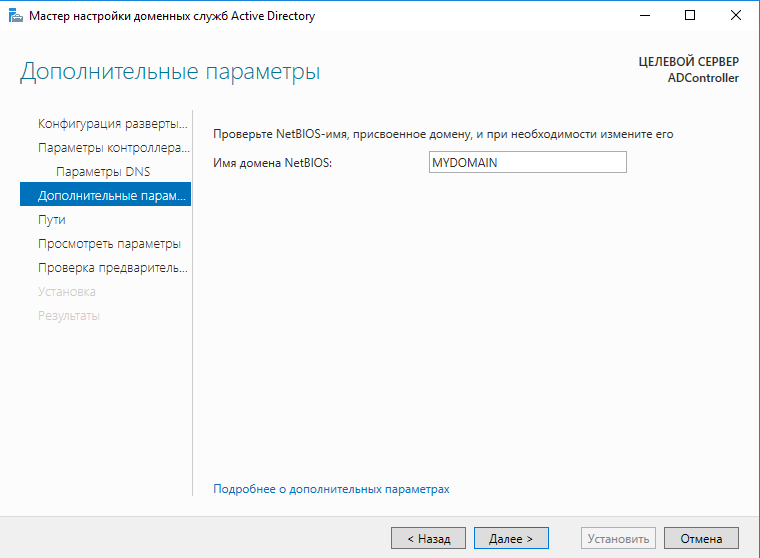
## Делегирование DNS



Что такое делегирование DNS? По большей части, это передача ответственности за некоторую DNS-зону отдельному DNS-серверу. Это распространенная практика в больших сетях, в которых требуется разграничить зоны ответственности за доменные зоны между различными серверами. При делегировании DNS в "главный" DNS-сервер вносится запись о том, что "вот за эту DNS-зону несёт ответственность вон тот DNS-сервер, обращайся туда".

Т.к. у нас всего одна зона DNS и DNS-сервер тоже один, то этот шаг нам необходимо пропустить и перейти к выбору NetBIOS-имени.

### NetBIOS-имя



Мы видим, что мастер предложил нам на выбор сразу же имя для нашего домена — MYDOMAIN. Но вы можете (и должны) задать себе вопрос: а что такое вообще NetBIOS-имя и зачем оно нужно? И разве мы уже не настраивали сетевое имя узла (Hostname) в самом начале? Чего же от вас хотят?

NetBIOS (Network Basic Input/Output) — это ещё один способ разрешения имён узлов в сети (более древний и более примитивный, чем DNS). NetBIOS-имена не предполагают никакой иерархии, их длина ограничивается всего лишь 16 символами, и они применяются только для разрешения имён компьютеров в локальной сети. Когда мы в самом начале лекции выбрали сетевое имя ADController — мы, на самом деле, задали именно NetBIOS-имя для сервера. Но теперь от нас снова требуют выбрать NetBIOS-имя (да ещё и другое, отличное от ADContoller). Не много ли NetBIOS-имён для одного компьютера?

Дело в том, что Microsoft пошла ещё дальше — и ограничила длину NetBIOS-имен не 16 символами, а 15 символами. 16-ый символ при этом считается зарезервированным суффиксом, который может принимать фиксированные значения. В зависимости от значения 16-го байта получаются разные классы NetBIOS-имён. Например, если суффикс равен 00, то NetBIOS-имя относится к рабочей станции. Если суффикс равен 1С, то это имя относится к имени домена.

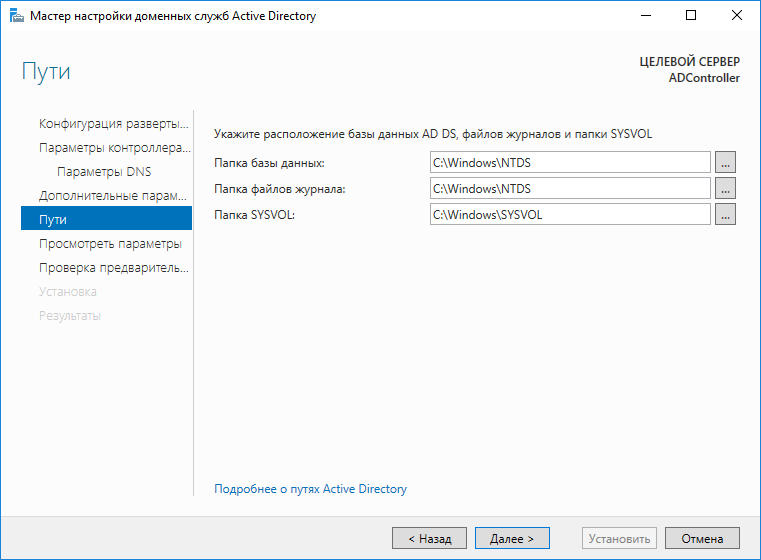
То есть, как вы понимаете, на первом шаге мы задавали NetBIOS-имя для компьютера Windows Server (с суффиком 00). А теперь задаём NetBIOS-имя домена mydomain.com (с суффиксом 1С).

Кстати, можете, ради интереса, отмотать лекцию в самое начало и посчитать количество символов в "нечитаемом" автоматически сгенерированном сетевом имени windows\_server (｡•̀ᴗ-) ✧.

И напоследок скажу, что вы не можете пропустить этот шаг. NetBIOS хоть и устаревшая технология, но до сих пор используется ради совместимости с некоторыми старыми службами. Настроить контроллер домена Active Directory без NetBIOS-имени нельзя.

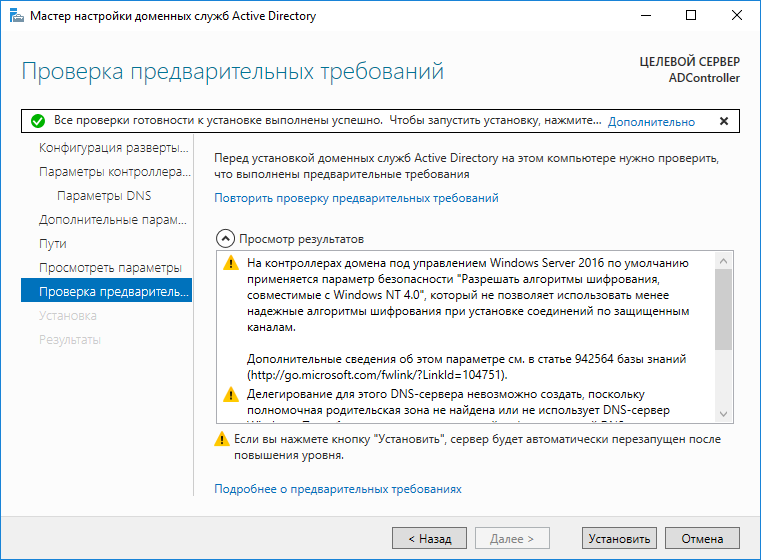
## Расположение базы данных

Оставляем NetBIOS-имя по умолчанию и двигаемся дальше, к выбору места расположения базы данных AD. Можно оставить значение по умолчанию.



## Проверка предварительных требований

Все ваши настройки должны пройти предварительную проверку:



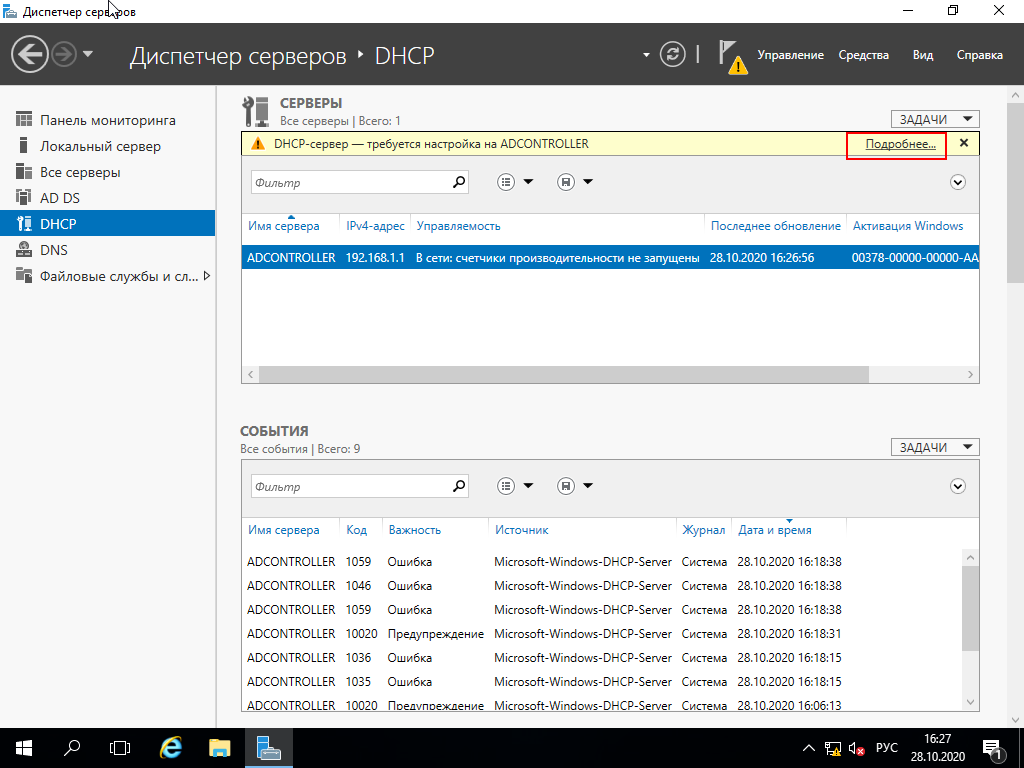
Как только всё готово, жмите "Установить" и можете спокойно идти пить чай, потому что после установки автоматически начнётся очень-очень долгая перезагрузка. Зато настройка контроллера домена AD на этом закончена, поздравляю!

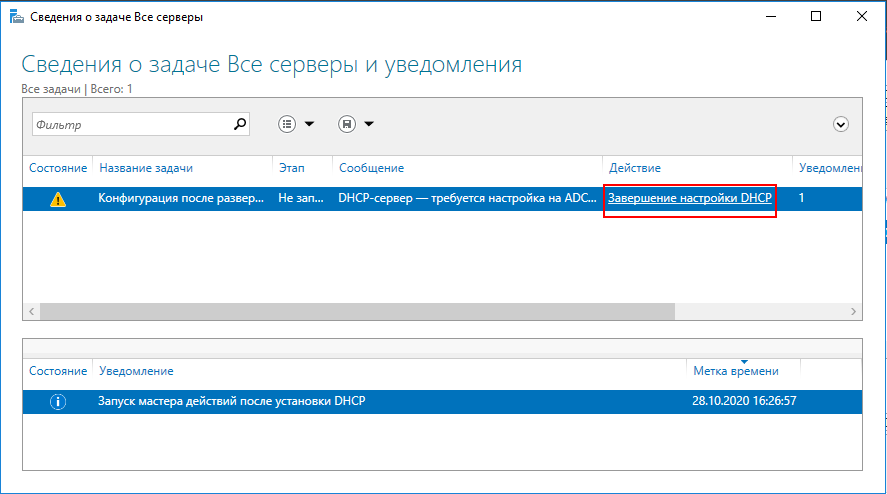
# Настройка DHCP-сервера

Пришло время заняться настройкой DHCP-сервера. Настройка глобально состоит из двух частей:

1. Авторизация DHCP-сервера в домене AD. Не каждый DHCP-сервер может раздавать сетевые настройки в домене AD — только авторизованные. Это сделано с целях безопасности, чтобы другие DHCP-серверы не могли "подсунуть" неправильные настройки компьютерам в домене;
2. Настройка новой DHCP-области. Это уже непосредственно настройка самого DHCP-сервера, в ходе которой определяются какие сетевые настройки будут выдаваться компьютерам в сегменте сети.

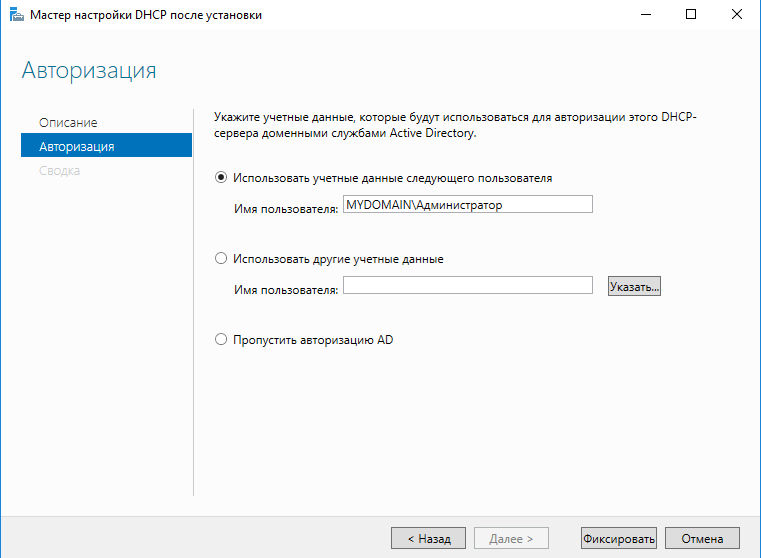
Для того, чтобы авторизовать DHCP-сервер, нужно вернуться на панель мониторинга (она и так должна быть перед вами после перезагрузки), перейти на вкладку DHCP (слева) и кликнуть на предложение донастроить DHCP-сервер:





В открывшемся мастере настройки DHCP после установки пропускаем первый приветственный экран и переходим к экрану авторизации.

## Авторизация DHCP-сервера в домене



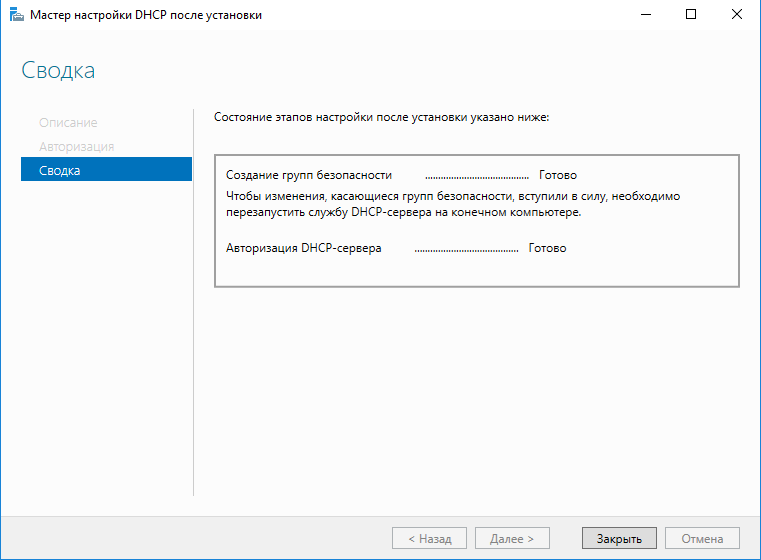
На выбор предлагаются три варианта:

1. Использовать учётные данные администратора (по умолчанию)
2. Использовать учётные данные другого пользователя;
3. Пропустить авторизацию AD.

По умолчанию авторизовать DHCP-сервер в домене могут только члены группы EnterpriseAdmins, куда как раз и входит пользователь MYDOMAIN\Администратор. При желании можно потратить немного времени и делегировать эту возможность админам "помельче" (региональным администраторам), почерпнуть больше информации по этой теме можно отсюда.

Итак, выбираем вариант по умолчанию и завершаем первый этап настройки DHCP-сервера. Теперь переходим непосредственно к настройкам DHCP. Для этого на панели мониторинга кликаем вкладку "Средства" и выбираем пункт "DHCP".

В открывшемся окне с настройками DHCP нужно кликнуть правой кнопкой мышки на IPv4 и затем на пункт меню "Создать область". После этого откроется мастер создания новой области.



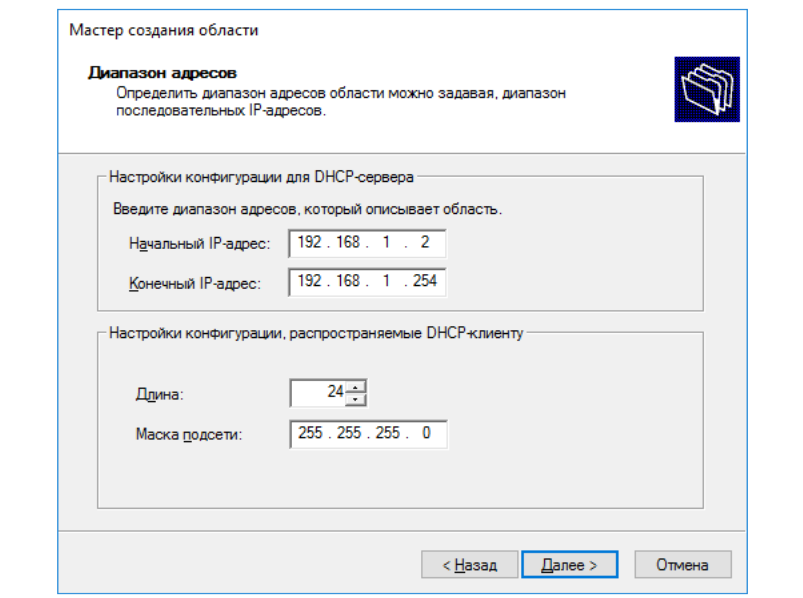
Что такое DHCP-область? Под этим понимается некий диапазон IP-адресов, которые может выдавать DHCP-сервер другим компьютерам в сети. Каждая область помимо диапазона IP-адресов также содержит другие сетевые настройки, с которыми мы сейчас и познакомимся.

Назовём DHCP-область SCOPE1 и перейдём дальше.

На следующем экране вам предложат выбрать диапазон адресов, которые будут выдаваться компьютерам в сети. Ранее я настраивал сетевой интерфейс на Windows Server, выдав ему адрес 192.168.1.1/24. Это статический адрес, и он зарезервирован, его выдавать другим компьютерам нельзя.

Зато никто не мешает выдавать все остальные адреса в сети 192.168.1.0/24 — так что задаём диапазон от 192.168.1.2 до 192.168.1.254 (192.168.1.255 — это зарезервированный широковещательный адрес, его выдавать тоже нельзя).

## Настройка диапазона адресов

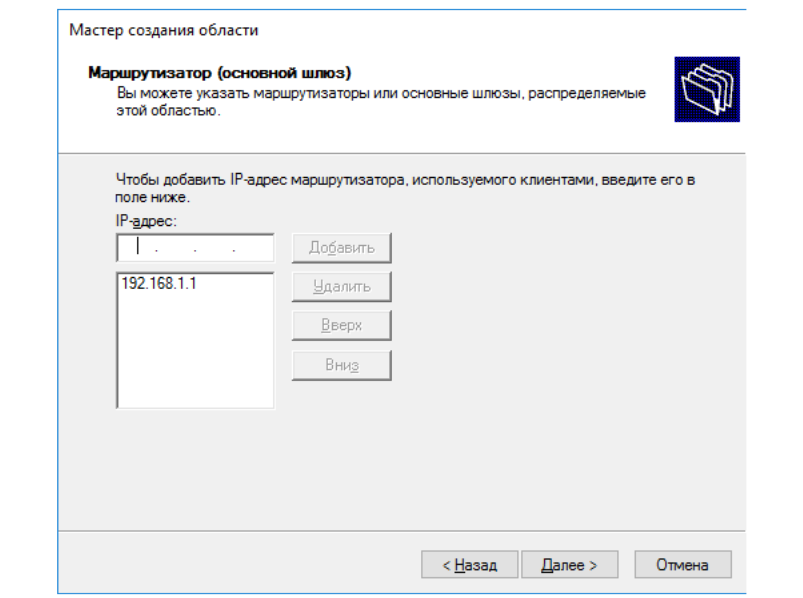


Переходим далее и видим предложение о выборе исключений из указанного диапазона адресов, а также о настройке задержки при передаче сообщения DHCPOFFER. С исключениями всё более-менее понятно: если вы не хотите выдавать некоторые адреса в указанном ранее диапазоне, то вы можете указать эти адреса здесь в виде исключений. А что за задержка в DHCPOFFER такая?

Эта настройка уже относится к довольно продвинутому администрированию сетей: если в вашей сети есть несколько DHCP-серверов, то с помощью этой задержки вы можете регулировать нагрузку между ними (подробнее можно прочитать, например, тут).

В любом случае, исключений в диапазоне у нас нет, да и задержка по умолчанию нас устраивает, так что кликаем дальше и видим настройку сроков аренды адресов.

Протокол DHCP предполагает выделение адресов только на определённое время, после чего компьютеры должны продлять аренду. Здесь можно настроить это время (по умолчанию — 8 дней). Кликаем "Далее" и видим предложение настроить другие настройки, которые будут получать клиенты в сети (помимо IP-адреса). Соглашаемся.



Первая сетевая настройка для клиентов — это шлюз по умолчанию. В стенде из двух виртуальных машин эта настройка в принципе не нужна. Но можно представить, что windows\_server будет играть роль шлюза во внешнюю сеть, и добавить адрес 192.168.1.1 как шлюз по умолчанию.

Далее идет настройка DNS. Здесь можно задать имя родительского домена и адреса DNS-серверов. С адресами DNS-серверов всё более-менее понятно — это IP-адреса серверов, куда следует обращаться клиентам за помощью в разрешении DNS-имён. Сейчас в этом списке фигурирует тот же адрес, что мы добавили, как шлюз по умолчанию.

### Понимание имени родительского домена

Для понимания имени родительского домена, рассмотрим следующую ситуацию.

Допустим, есть домен mydomain.com и есть два компьютера в этом домене с именами comp1.mydomain.com и comp2.mydomain.com. Если comp1 хочет связаться с comp2, то он должен, по-хорошему, использовать следующую команду (обращение по Fully Qualified Domain Name — FQDN):

ping comp2.mydomain.com

Но задумывались ли вы когда-нибудь, что именно произойдет, если попытаться пропинговать другой узел следующим образом?

ping comp2

На самом деле, в этом случае начинается целая магия — очень хитрый процесс разрешения имён.

Согласно алгоритму разрешения сетевых имен, сначала comp1 попробует найти информацию о comp2 в hosts.txt — файле. Если этой информации там не окажется, то начинается процесс поиска узла через DNS. Вот только вопрос — DNS-имена же находятся в каком-то домене, верно? Какое доменное имя нужно "пристыковать" к comp2 при выполнении пинга?

Вот тут в дело и вступает настройка DHCP, которая называется "имя родительского домена". Это как раз тот суффикс, который будет автоматически "пристыкован" к имени comp2 при выполнении DNS-разрешения имени. Так что если имя родительского домена равно "mydomain.com", то команда ping comp2 неявно преобразуется в ping comp2.mydomain.com.

Если же DNS-разрешение окажется неудачным, дальше начнутся попытки найти comp2 уже по NetBIOS-имени. Что такое WINS, и чем он отличается от Broadcast — информация будет чуть дальше по тексту.

Что ж, в нашем случае имя родительского домена должно быть mydomain.com (значение по умолчанию), а нужный DNS-сервер уже находится в списке, так что в итоге просто кликаем "Далее".

# Настройки DNS

Теперь нас попросят указать настройки WINS-сервера. WINS (Windows Internet Name Service) сервер участвует в разрешении NetBIOS-имён в сети (прямо как DNS-сервер для DNS-имён). Вот только, в отличие от DNS, WINS-сервер не обязательно должен присутствовать в сети, чтобы разрешение NetBIOS-имён работало. Так зачем же он нужен тогда?

Дело в том, что по умолчанию разрешение NetBIOS-имен происходит через широковещательные запросы. С одной стороны, это очень простой механизм (проще не придумаешь), но, с другой стороны, обладает парой недостатков:

* При наличии большого количества NetBIOS-имён в сети широковещательный трафик может начать "зашумлять" канал;
* Широковещательные запросы не могут "выйти" за пределы текущей сети, поэтому узнать NetBIOS-имя из другой сети таким способом не выйдет.

Так вот, WINS-сервер позволяет решить обе этих проблемы. Этот сервер централизованно хранит NetBIOS-имена компьютеров, и обычные узлы в сети могут обращаться к нему для поиска IP-адреса интересующего их имени (как и для DNS). Такой подход, во-первых, резко уменьшает количество широковещательного трафика в сети, а, во-вторых, позволяет посылать NetBIOS-запросы в другие сети, а не только в текущую.

В нашей небольшой сети WINS-сервер нам ни к чему, поэтому просто пропускаем эту настройку и едем дальше.

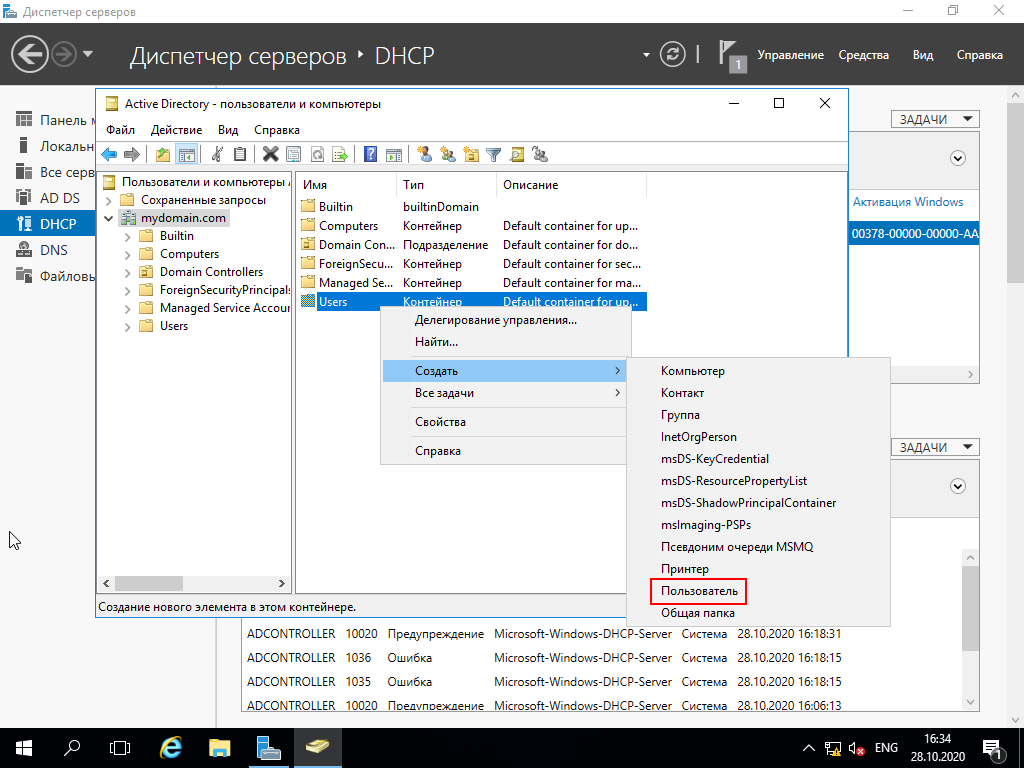
В последнем шаге настройки вам предлагают сразу активировать настроенную область. Соглашаемся, и на этом заканчиваем настройку DHCP.

# Создаём нового пользователя в домене AD

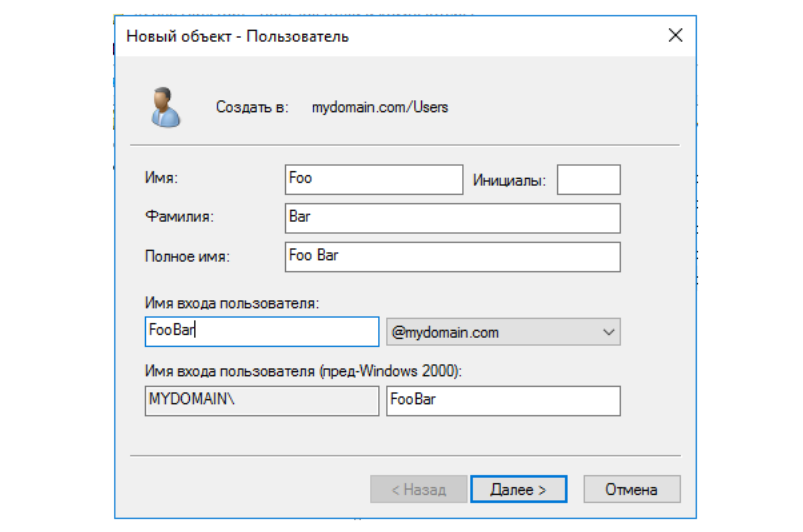
Собственно, настройка контроллера домена и различных сервисов уже фактически закончена, все параметры выставлены как надо. Теперь нужно просто зарегистрировать нового пользователя, от имени которого рабочая станция workstation будет выполнять вход в домен.

Для этого возвращаемся на панель мониторинга, кликаем на "Средства" и затем на "Пользователи и Компьютеры Active Directory".

В открывшемся меню можно заметить созданный домен mydomain.com и его состав. Видно, что помимо пользователей в домене созданы папочки для Computers, Domain Controllers и других сущностей. Но нас сейчас интересуют пользователи, поэтому кликаем правой кнопкой мышки на папке Users и выбираем "Создать" -> "Пользователь".

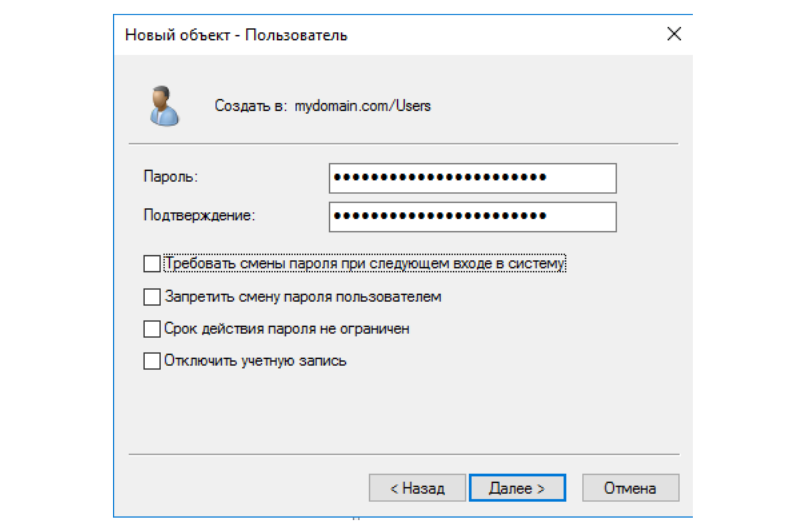


После этого появляется диалоговое окно с преложением ввести данные нового пользователя. По старой доброй традиции назовём пользователя Foo Bar. Обратите внимание, что пользователь отображается лишь как "Объект" в Active Directory наравне с другими объектами.



Теперь необходимо задать пароль и дополнительные параметры для пользователя. Пароль должен соответствовать политике паролей по умолчанию, которая, в том числе, предписывает паролям в домене быть довольно сложными (должен использовать числа, буквы верхнего и нижнего регистра, а также спец символы).

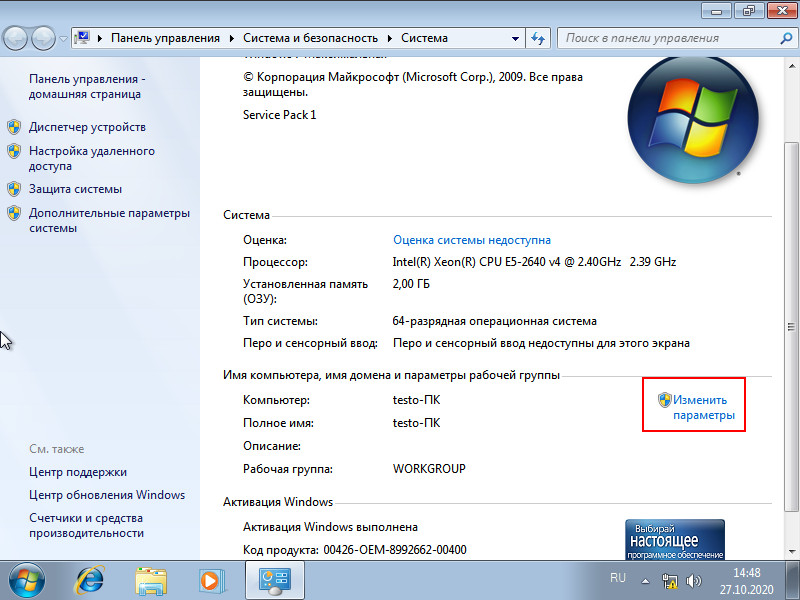
Обычно администратор создаёт простой пароль для пользователя, а затем требует от пользователя сменить его при первом входе в систему (первая галочка в списке доступных опций). Это очень хорошая практика с точки зрения безопасности, ведь таким образом даже администратор AD не сможет узнать пароль пользователя. Также хорошей практикой считается ограничивать срок действия пароля. В этой лекции для простоты мы уберём требование о смене пароля пользователем при входе в систему.



После этого останется лишь подтвердить создание нового пользователя. Ну что ж, вот, кажется, и всё. Осталось лишь проверить ввод рабочей станции в домен.

# Ввод рабочей станции в домен

Переключаемся на вторую машину workstation под управлением Windows 7 (мне было проще использовать свои старые скриншоты) и заходим в свойства системы. Сейчас видно, что рабочая станция находится в рабочей группе (не в домене). Кстати говоря, WORKGROUP — это тоже NetBIOS-имя. Только в отличии от имени домена оно имеет суффикс 1E.

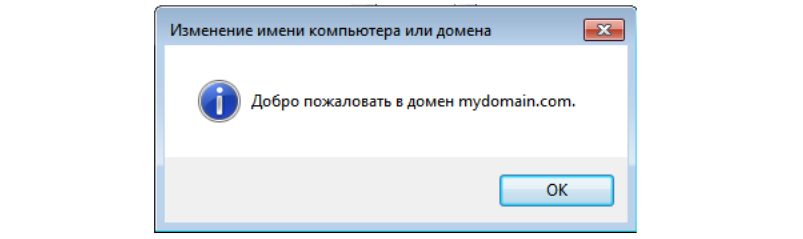


Щелкаем на кнопку "Изменить параметры", затем в появившемся окне ещё раз "Изменить...".

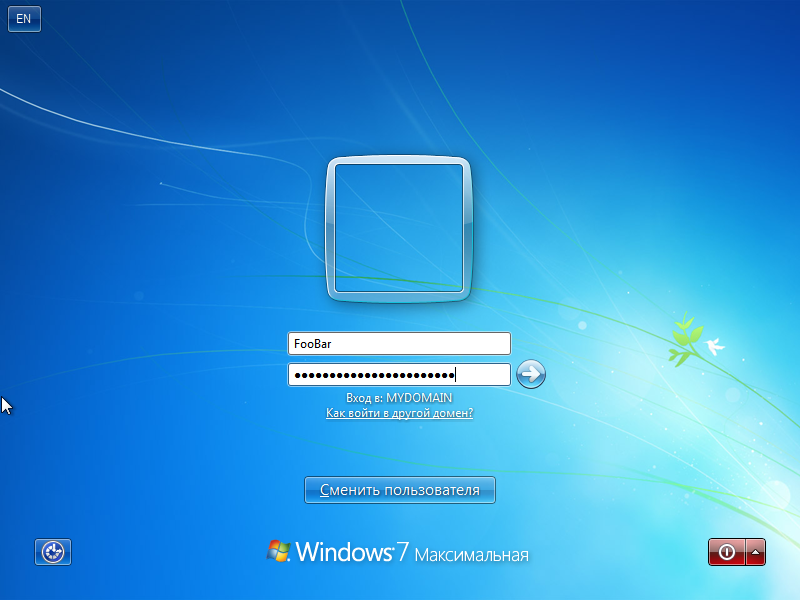
В окне изменения имени компьютера пишем, что он должен принадлежать домену mydomain.com.

Видим предупреждение о нестандартном имени компьютера (testo-ПК содержит кириллицу). Это связано с тем, что NetBIOS-имена не могут содержать кириллицу. Но мы с вами настроили DNS-сервер (DNS настройки прилетели на рабочую станцию по DHCP), а DNS-механизм разрешения имён, как мы знаем, имеет приоритет перед NetBIOS. Так что в данном случае на работоспособность AD кириллица не влияет. Но на практике так делать не надо!

Вводим логин-пароль от новой учетной записи FooBar и, наконец, видим заветное сообщение "Добро пожаловать в домен".



После ввода компьютера в домене необходимо перезагрузить компьютер, ну а дальше — вводим учётные данные пользователя в AD.



И после успешного входа на рабочий стол перепроверяем свойства системы. Полное имя компьютера поменялось на testo-ПК.mydomain.com, а это значит, что мы успешно ввели рабочую станцию в домен mydomain.com.

На этом настройка домена AD завершена.