**Workgroup** - Workgroups are small peer-to-peer local area networks, where each computer has its own set of rules and settings, managed by the administrator of that device, and a unique computer name in that workgroup

1 ПК может получить доступ к файлам 2 ПК, если пользователь 1 ПК знает креды **локального пользователя** 2 ПК, или любого пользователя, созданного на 2 ПК. При условии что они находятся в 1 ворк группе и в 1 сети

* Если пользователь сменит пароль на своей машине, то он не обновится на всех остальных машинах, и адину придется вручную обходить каждый ПК и менять там пароль, *что не удобно.*
* Если есть файловый сервер, и нужно ограничить доступ к нему ряду пользователей, то нужно создать разные учетные записи, и при изменении пароля на любой машине, придется в ручную менять пароль для записей и на сервере, *что не удобно*

Аутентификация – это проверка того, что пользователь ввел корректные данные для входа

Авторизация – проверка того, что у пользователя есть доступы к ресурсу (Например скачивание файла)

Для решения этой проблемы существует Active Directory Domain Services

**Домен** – это область компьютерной сети, которая централизовано управляется, имеет общие настройки, групповые политики и тд

**Доменной имя** – имя, необходимое для идентификации областей, автономных единиц в сети

**Признаки домена**:

* Есть 1 или более контроллер домена
* Изменения на 1 машине затрагивают все машины, если у них единые политики
* При подключении в домен нужно вводить его имя

**Active Directory** – это иерархически организованное хранилище данных (учетки, политики,…) об объектах сети (сервера, хосты, перефирия), обеспечивающее удобные средства для поиска и использования этих данных. Компьютер, на котором работает Active Directory, называется контроллером домена. Представляет из себя Служба (сервис) каталогов Windows, группирующие все объекты которые могут быть добавлены в домен

В структуру сети вводится **Контроллер Домена**. Он хранит все **объекты** Active Directory. На нем мы можем сделать несколько учетных записей. Далее пользователи могут ввести свои машины в домен и пользоваться **доменными учетными записями.** Тем самым 2 разных ПК смогут получить доступ к чужой машине, введя креды не **локальной**, а **доменной учетной записи.** Контроллеров домена может быть несколько для увеличения отказоустойчивости или быстродействия

При логине на ПК с доменной учеткой, домен контроллер выдает этому ПК - ticket (пропуск). Далее этот пропуск используется в пределах домена для авторизации пользователя и доступу к ресурам. Запрашиваемый ресурс пошлет запрос в домен контролер, что бы узнать может ли юзер получить доступ.

**Плюсы**:

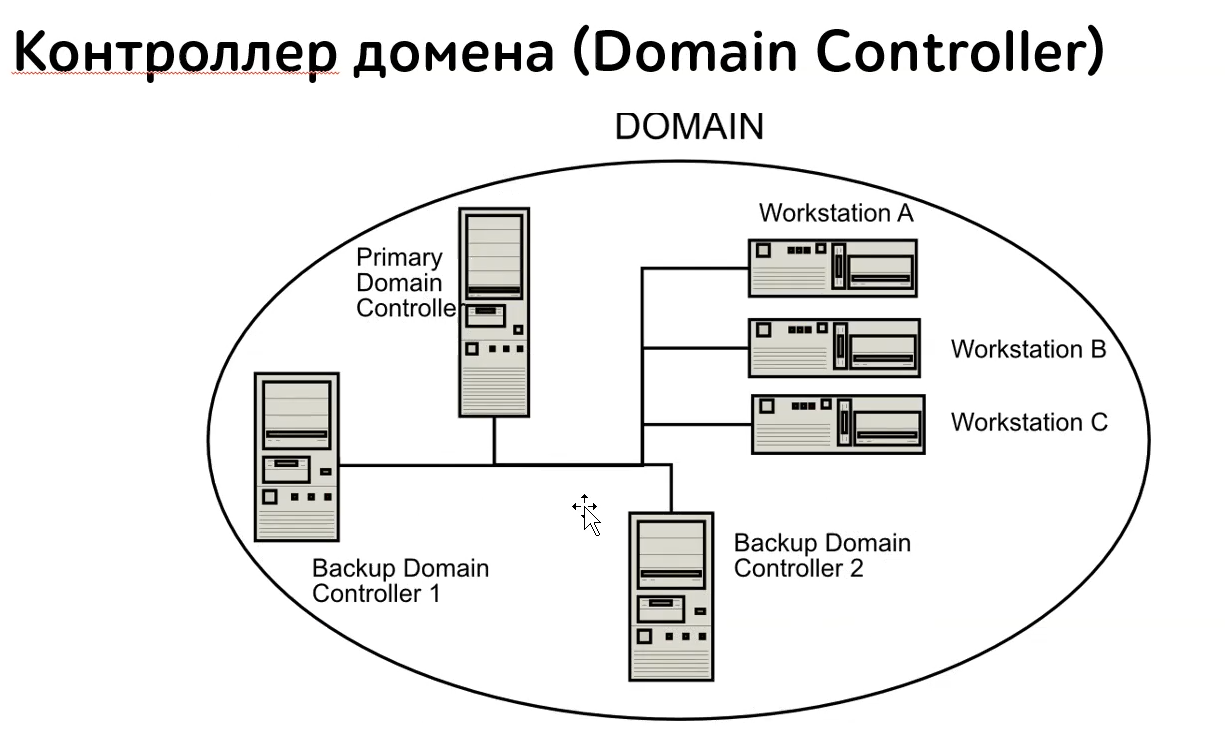
* Нам не нужно создавать учетки на каждом ПК, достаточно создать 1 на контроллере домена
* При смене пароля на доменной учетной записи, обновленный пароль отсылается на контроллер домена, и обновляется так же там
* Если нужно заблокировать доступ для юзера, то мы можем заблокировать пользователя на контроллере домена
* AD - так же позволяет залогиниться под своими кредами к другому компу, и AD создаст временную локальную учетку

**Минусы**:

* Если падает домен контроллер, то никто не сможет получить доступ ни к какой сущности домена. Обойти это можно добавлением еще 1 домен контроллера, на который будет копироваться содержимого первого

**На контроллере домена хранятся**:

* Пользователи
* Групповые политики



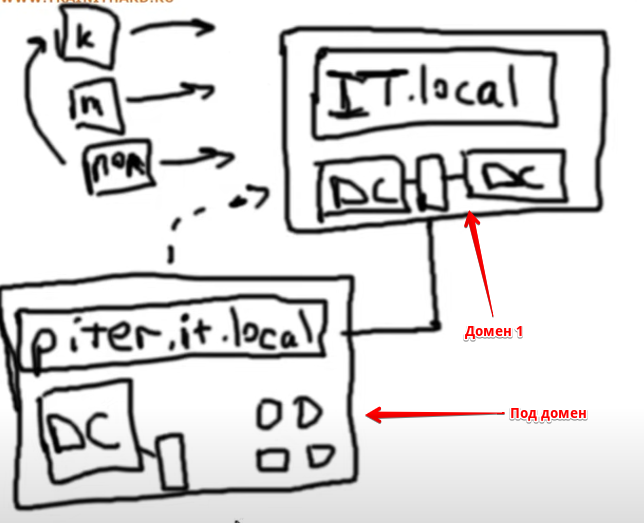


**Структура Active Directory**

1. Деление AD по административным полномочиям

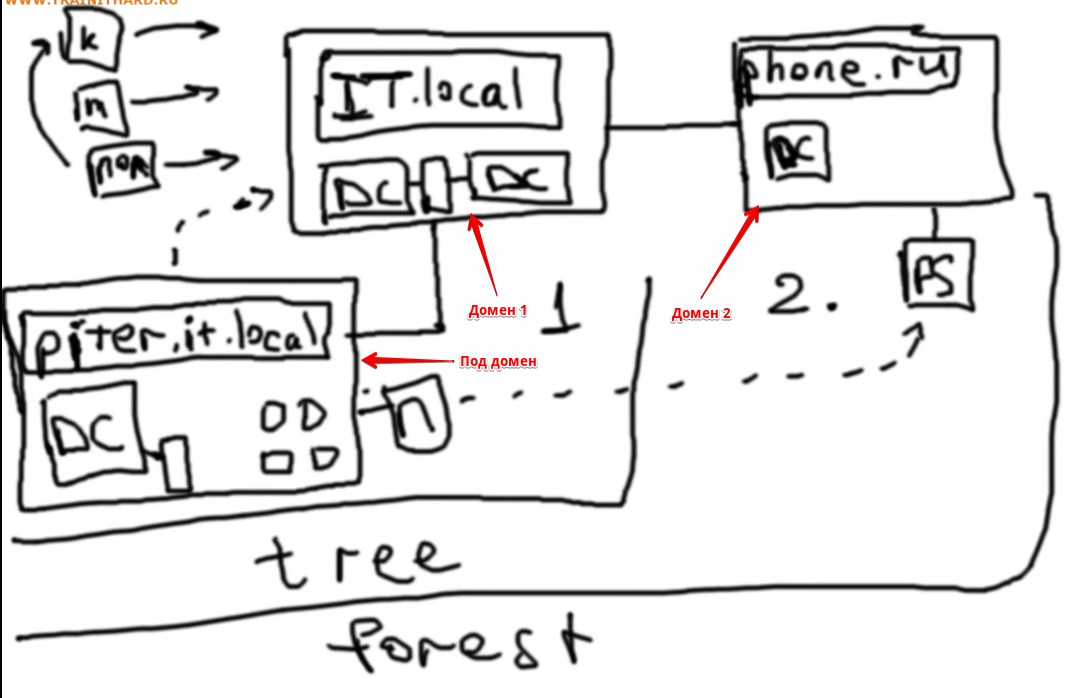
**Дерево AD (tree) – это когда у домена есть под домен, тем самым они образует дерево**

В AD может быть не только 1 домен. У главного домена могут быть дочерние домены. Они могут иметь доступ друг к другу или не иметь. Например если компания открывает второе подразделение в другом городе, то оно будет иметь второй домен

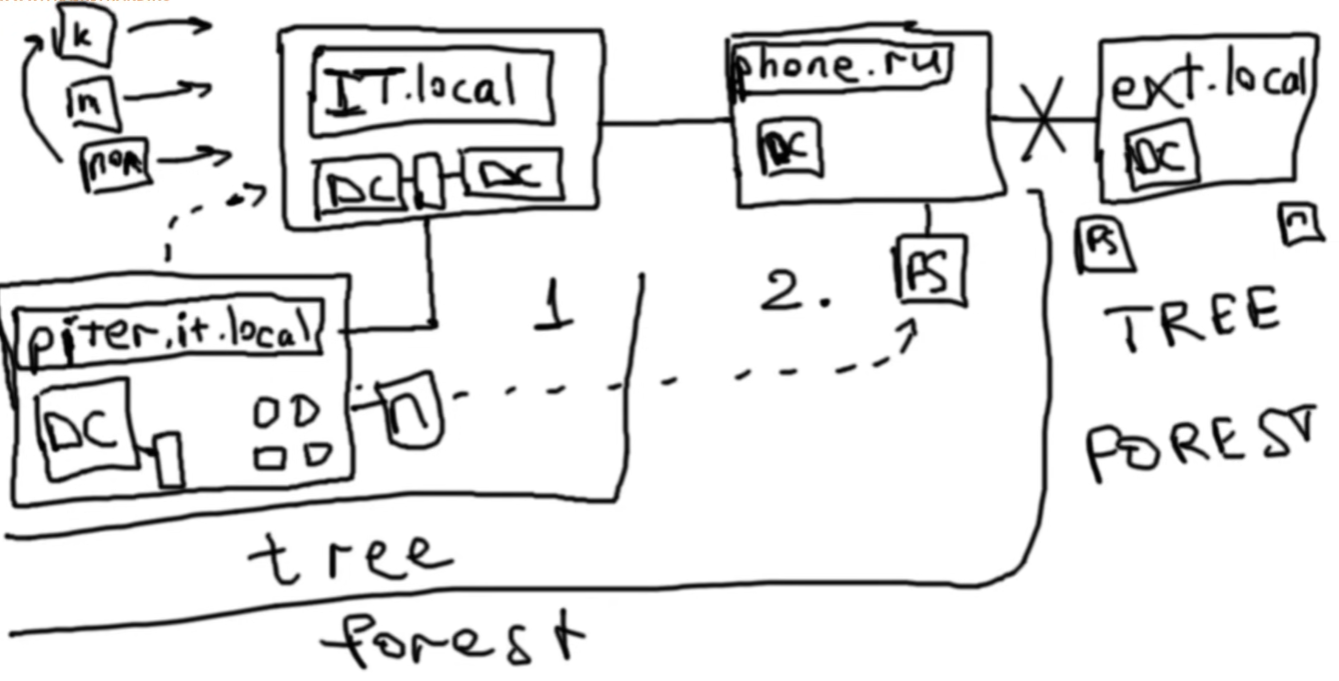


**Лес (forest) – это когда происходит связь нескольких разных доменов. В таком случае, даже если домен не имеет под доменов, то это все равно будет дерево**

Если компания купила другую компанию, но хочет что бы структура домена сохранилась, то создается еще 1 домен, но он не будет являться под доменом, а будет существовать как отдельный домен. Мы делаем связь доменов, что бы они могли связываться между собой



Например если купили организацию, и хотят сделать организацию не связанную с другими доменами. То она сама по себе будет образовывать и дерево и лес



1. Сайты AD. Территориальное деление

Например если 2 офиса находятся далеко друг от друга, то пользователи домена из Новосибирска будут всегда стучаться к контроллеру домена в Москве, используя VPN. Это сильно замедляет работу, по этому мы разворачиваем локальный контроллер домена. Но не факт что машины будут идти именно к нему, из за этого и существует **деление на сайты**

Указываем что 1 сайт – MSC, 2 сайт – NV. Тогда сущность видит что она находится в пределах сайта, и будет обращаться к контроллеру домена в пределах своего сайта

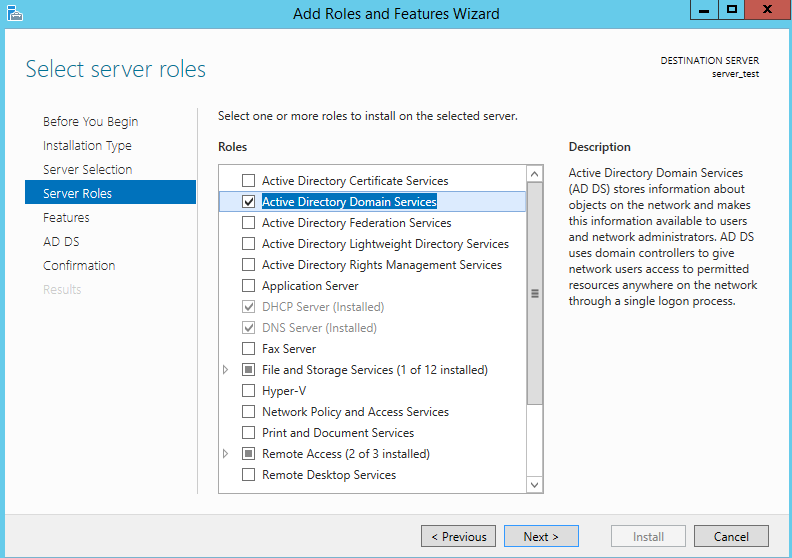


**AD завязан на DNS**

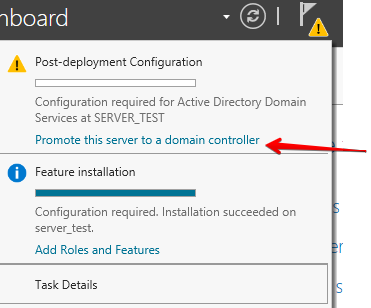
Когда мы указываем имя домена при подключении, то домен делает запрос в DNS, откуда клиент и получает местоположение контроллера домена. DNS по этому обязательно должен знать местоположение контроллера домена. Если мы не можем войти в домен, то первым делом проверяем конфигурацию DNS. При установке Active Directory, сразу предложит установить DNS сервер, если он еще не был установлен

**Создание Active Directory домена**

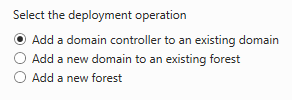
Manage > Add Roles and Features



Повышаем сервер до домен контроллера

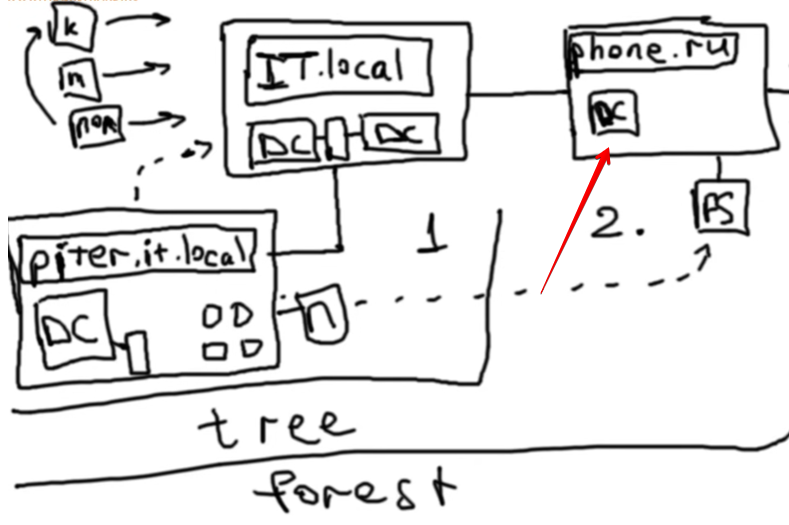


**Настройка домен контроллера**



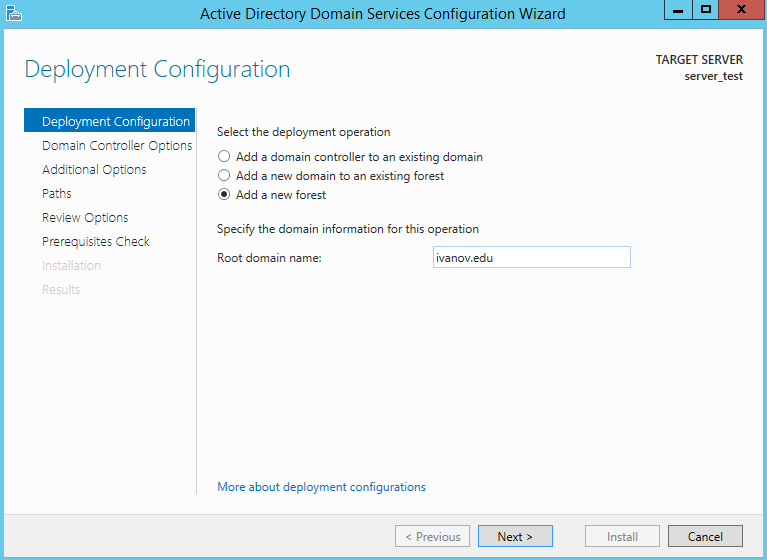
Add a new forest – когда мы развертываем домен контроллер первый раз. Мы создаем сразу лес, дерево, и в нем домен контроллер

Add a new domain to an existing forest

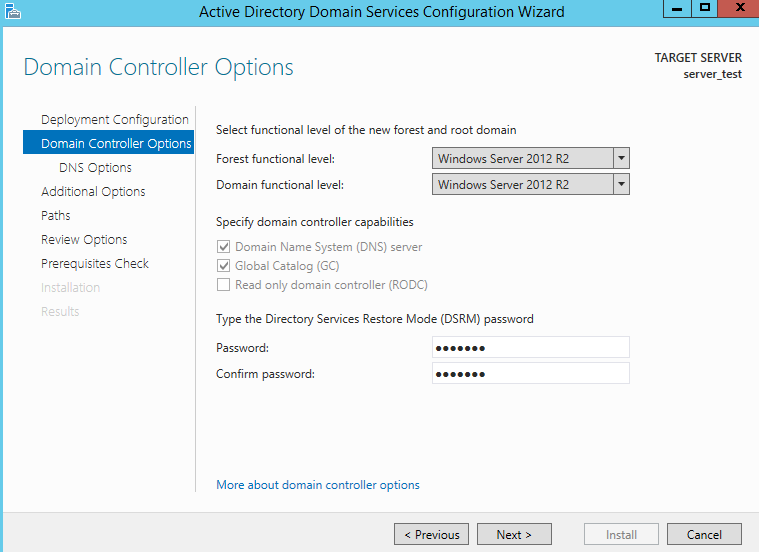


Add a domain controller to an existing domain – добавление нового контроллера, что бы в случае отказа первого контроллера, сущности могли получать права

**имя\_домена.доменная\_часть**

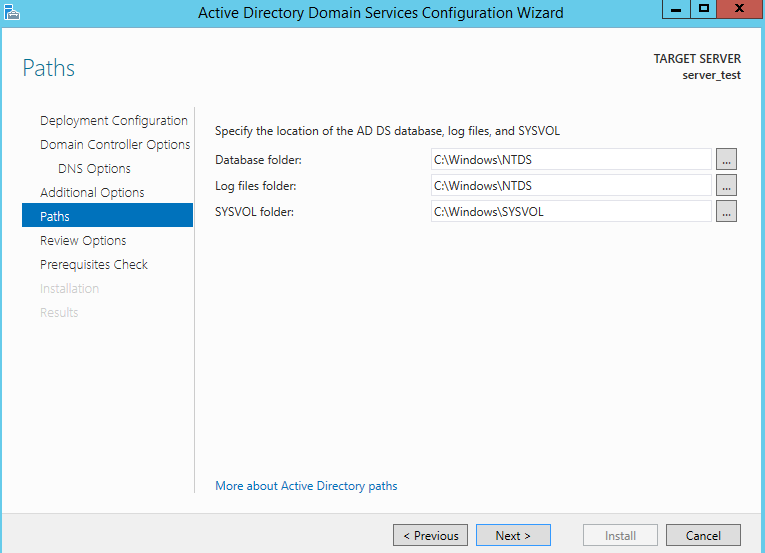


Directory Services Restore Mode – если нужно восстановить контроллер домена, то нужно указать пароль, для доступа к нему

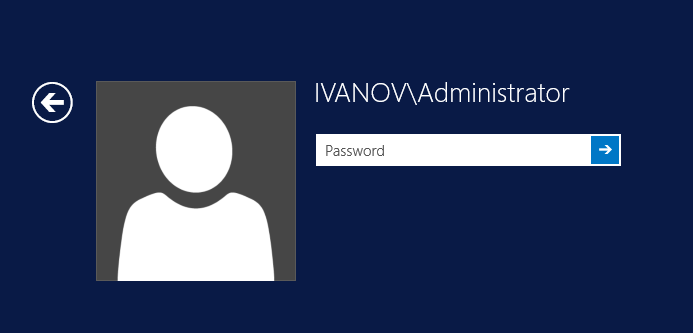


Выбор базы данных, куда будут сохраняться данные

SYSVOL – здесь хранятся групповые политики

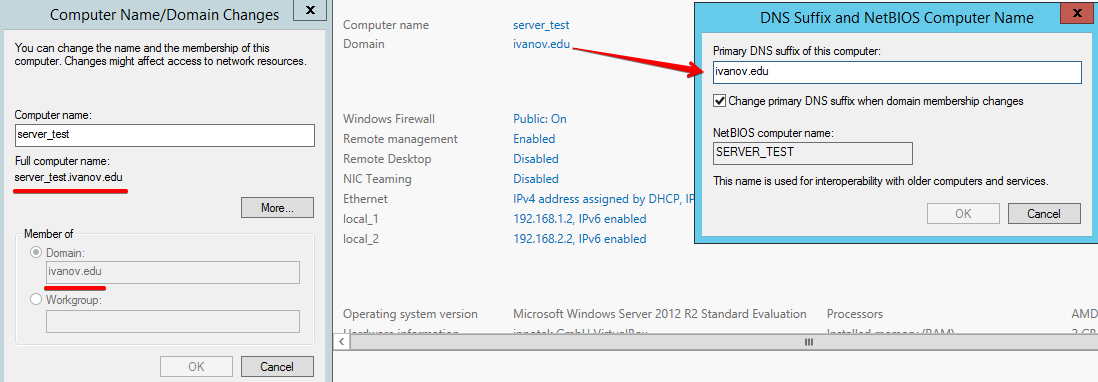


**На домен контроллере есть только доменные пользователи**



Что бы зайти за локального пользователя, то нужно перед вводом имени пользователя ввести **.\**

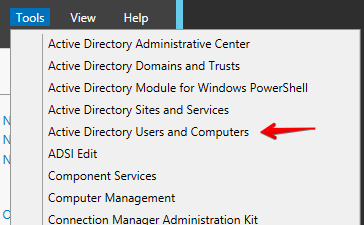
Одновременно с добавлением домена **имя\_домена.доменная\_часть**  добавляется DNS suffix



**Active Directory Users and Computers**

Здесь мы видим структуру домена

Tools > Active Directory Users and Computers

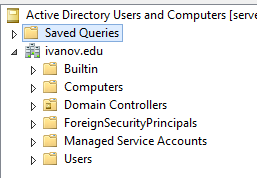


**Builtin** – все **локальные** пользователи, группы, которые существовали ранее, находятся здесь. Они превратились в **доменные**

**Computers** – тут создаются компьютеры, которые вводятся в домен

**Domain Controllers** – компьютер контроллера домена

**Users** – здесь создаются пользователи для домена, а так же находятся доменные встроенные группы по умолчанию



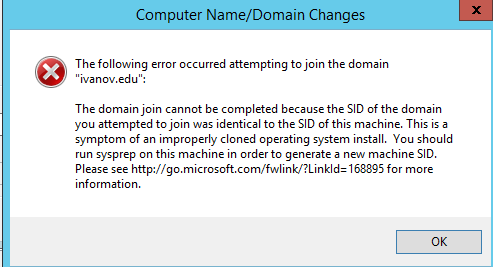
Структура AD представлена в виде дерева. В дереве могут быть:

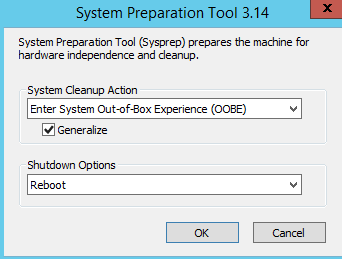
1. Контейнер (Builtin, Computers, ForeignSecurityProncipals, Managed Service Accounts, Users)
2. Organization Unit (Организационно подразделение) (Domain Controllers) –выглядит как папку с файлом внутри
3. Объект (то что хранится внутри контейнера/OU – пользователь, группа, компьютер и тд)

На Organization Unit можно применять групповые политики, а на контейнер не можем

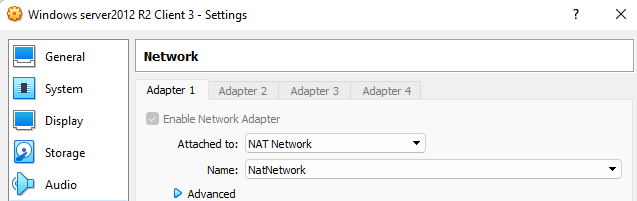
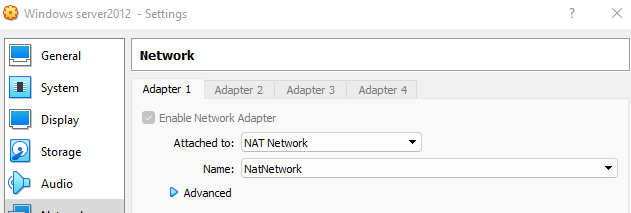
Вводим клиента в домен. Клиент должен находиться в той же локальной сети, что и сервер

Запускаем команду sysprep, что бы решить проблему с клонированной виртуалкой

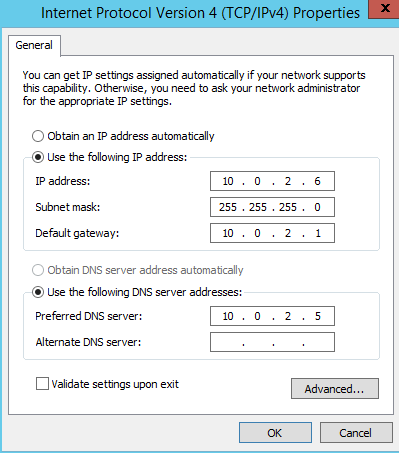




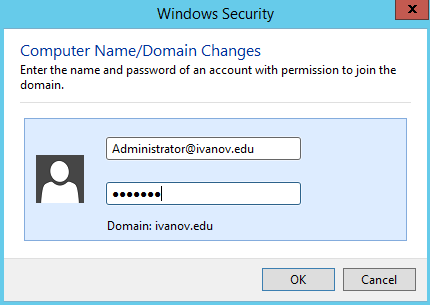
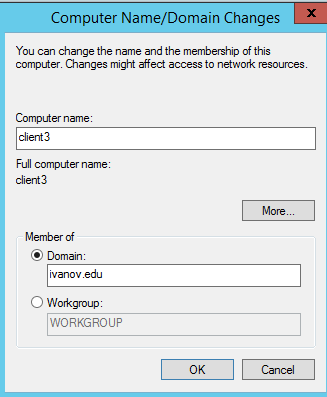
Клиент машину вводим в туже сеть, что и сервер, здесь имеется ввиду подключить их щнуром друг к другу



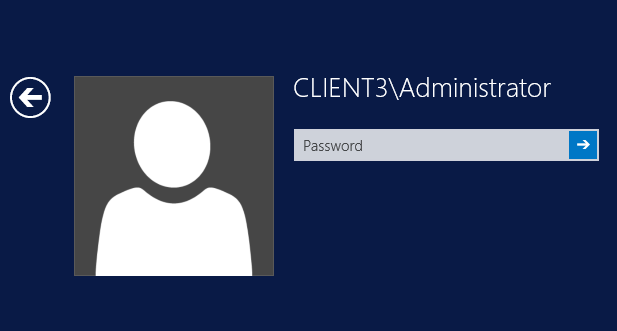
Если нет DHCP сервера, то для клиент машины вручную задаем статичный IP адрес, в той же сети, что и сервер. В качестве DNS сервера **обязательно** указываем IP адрес нашего DNS, AD сервера. Так же если мы раздаем адреса DNS по DHCP, то если мы раздадим их несколько, клиент может не подключиться к домену, так как не будет знать по какому DNS адресу ему стоит обращаться. Для этого мы можем вручную указать адрес DNS (наш сервер, где есть Active Directory с DNS)



После вводим его в домен



Пользователь введен в домен и является доменным пользователем



**Сетевые ресурсы -** (общие, скрытые, административные). Общие - мы можем подключиться к папке соседа/принтер/... по группе, домену. Скрытые папки - мы их не видим, но можем получить доступ. Если добавить в конце имени $