**Создание и администрирование объекта компьютер в Active Directory**

Компьютеры относятся к еще одному типу объектов Active Directory, но в отличие от пользователей и групп AD к ним нет должного внимания, и, соответственно, администраторы пренебрегают их администрированием. Но компьютеры, так же как и группы, пользователи AD имеют свой SID и соответственно их можно заключать в группы, назначать им доступ к ресурсам, управлять ими средствами групповых политик.

### Способы создания компьютера в AD.

Всем известно, после установки операционной системы, компьютер изначально включен в рабочую группу (по умолчанию в WORKGROUP). В рабочей группе каждый компьютер это независимая автономная система, в которой существует база данных диспетчера безопасности учетных записей SAM (Security Accounts Manager). При входе человека на компьютер выполняется проверка наличия учетной записи в SAM и в соответствии с этими записями даются определенные права. Компьютер, который введен в домен продолжает поддерживать свою базу данных SAM, но если пользователь заходит под доменной учетной записью, то он проходит проверку уже на контроллере домена, т.е. компьютер доверяет контроллеру домена идентификацию пользователя.

Ввести компьютер в домен можно различными способами, но перед тем как это делать, вы должны убедиться, что данный компьютер соответствует следующим требованиям:

- у вас есть право на присоединение компьютера к домену (по умолчанию это право имеют Администраторы предприятия (Enterperise Admins), Администраторы домена ( Domain Admins), Администраторы (Administrators), Операторы Учета (Account Admins));

- объект компьютера создан в домене;

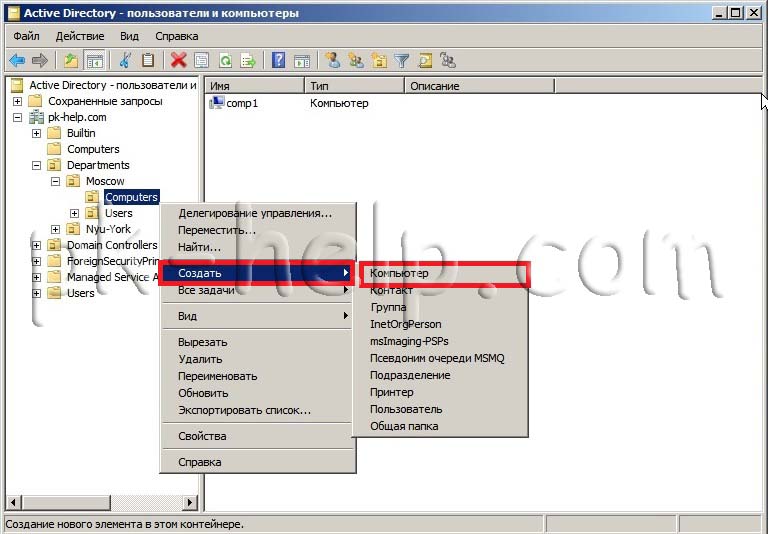
- вы должны войти в присоединяемый компьютер как локальный администратор.

У многих администраторов второй пункт может вызвать негодование, - зачем создавать компьютер в AD, если он появиться в контейнере Computers после ввода компьютера в домен. Все дело в том, что в контейнере Computers нельзя создать подразделения, но еще хуже, что к контейнеру нельзя привязать объекты групповой политики. Именно поэтому рекомендуется создать объект компьютер в необходимом подразделении, а не довольствоваться автоматически созданной учетной записью компьютера. Конечно, можно переместить автоматически созданный компьютер в необходимое подразделение, но зачастую подобные вещи администраторы забывают делать.

Теперь разберем способы создания компьютера (компьютеров) в AD:

#### Создание компьютеров при помощи оснастки «Active Directory – пользователи и компьютеры».

Для этого способа нам понадобится запустить оснастку «Active Directory – пользователи и компьютеры», у себя на компьютере с помощью [**Admin Pack**](http://pk-help.com/workstation/admin-pack/) или на контроллере домена. Для этого необходимо нажать "**Пуск- Панель управления- Система и безопасность- Администрирование- Active Directory – пользователи и компьютеры**" выберите необходимое подразделение, нажмите на нем правой кнопкой мыши, в контекстном меню выберите "**Создать- Компьютер**".



Впишите имя компьютера.

#### Создание учетной записи компьютера с помощью команды DSADD.

Общий вид команды:

**dsadd computer <DN\_компьютера> [-desc <описание>] [-loc <расположение>] [-memberof <группа ...>]  [{-s <сервер> | -d <домен>}] [-u <пользователь>]  [-p {<пароль> | \*}] [-q] [{-uc | -uco | -uci}]**  
  
Параметры:  
  
Значение                Описание  
**<DN\_компьютера>**        Обязательный параметр. Задает различающееся имя (DN) добавляемого компьютера.   
**-desc <описание>**      Задает описание компьютера.  
**-loc <размещение>**       Задает размещение компьютера.  
**-memberof <группа ...>**  Добавляет компьютер в одну или несколько групп, определяемых разделяемым пробелами списком имен DN <группа ...>.  
**{-s <сервер> | -d <домен>}**  
                        **-s** <сервер> задает подключение к контроллеру домена(DC) с именем <сервер>.  
                        **-d** <домен> задает подключение к DC в домене <домен>.  
                        По умолчанию: DC в домене входа.  
**-u <пользователь>**      Подключение под именем <пользователь>. По умолчанию: имя пользователя, вошедшего в систему. Возможные варианты: имя пользователя, домен\имя пользователя, основное имя пользователя (UPN).  
**-p {<пароль> | \*}**      Пароль пользователя <пользователь>. Если введена \*,  будет запрошен пароль.  
**-q**                     "Тихий" режим: весь вывод заменяется  стандартным выводом.  
**{-uc | -uco | -uci}**

**-uc** Задает форматирование ввода из канала или вывода в канал в Юникоде.  
                         **-uco** Задает форматирование вывода в канал или файл в Юникоде.  
                         **-uci** Задает форматирование ввода из канала или файла в Юникоде.

Пример использования команды Dsadd:

**Dsadd computer “CN=COMP001,OU=Moscow,OU=Departments,DC=pk-help,DC=com”  –desc “Компьютер отдела IT”**

**Создание  учетной записи рабочей станции или сервера с помощью команды Netdom.**

Общий вид команды Netdom:

**NETDOM ADD <компьютер> [/Domain:домен] [/UserD:пользователь] [/PasswordD:[пароль | \*]] [/Server:сервер] [/OU:путь к подразделению] [/DC] [/SecurePasswordPrompt]**  
**<компьютер>**   это имя добавляемого компьютера  
**/Domain**           указывает домен, в котором требуется создать учетную запись компьютера  
**/UserD**             учетная запись пользователя, используемая при подключении к домену, заданному аргументом /Domain  
**/PasswordD**      пароль учетной записи пользователя, заданной аргументом /UserD. Знак \* означает приглашение на ввод пароля  
**/Server**            имя контроллера домена, используемого для добавления.  Этот параметр нельзя использовать одновременно с параметром /OU.  
**/OU**                 подразделение, в котором необходимо создать учетную запись компьютера. Требуется полное различающееся доменное имя RFC 1779 для подразделения. При использовании этого аргумента необходимо работать непосредственно на контроллере указанного домена. Если этот аргумент не задан, учетная запись будет создана в подразделении по умолчанию для объектов компьютеров этого домена.  
**/DC**                 указывает, что требуется создать учетную запись компьютера контроллера домена. Этот параметр нельзя использовать одновременно с параметром /OU.  
**/SecurePasswordPrompt**    Использовать для указания учетных данных безопасное всплывающее окно. Этот параметр следует использовать при необходимости указания учетных данных смарт-карты. Этот параметр действует только в случае задания пароля в виде \*.

### Администрирование учетной записи компьютеров в Active Directory.

**Переименование компьютера в AD.**

Запускаем командную строку и с помощью команды Netdom переименовываем компьютер в AD:

**Netdom renamecomputer <Имя компьютера> /Newname: <Новое имя>**

Пример: **Netdom renamecomputer COMP01 /Newname: COMP02**

**Удаление учетных записей компьютера.**

1 Удалить учетную запись компьютера с помощью оснастки "**Active Directory – пользователи и компьютеры**". Запускаете оснастку "**Active Directory – пользователи и компьютеры**" находите необходимый компьютер нажимаете на нем правой кнопкой мыши, в контекстном меню выбираете "**Удалить**", подтверждаете удаление

2 Удалить компьютер можно с помощью команды DSRM:

**DSRM <DN объекта>**

Пример:

**DSRM CN=COMP001,OU=Moscow,OU=Departments,DC=pk-help,DC=com**.

**Устранение ошибки "Не удалось установить доверительных отношений между этой рабочей станцией и основным доменом".**

Иногда при попытке войти в компьютер пользователь получает сообщение "**Не удалось установить доверительных отношений между этой рабочей станцией и основным доменом**". Это ошибка возникает при отказе в работе безопасного канала между машиной и контроллером домена. Чтобы это устранить, необходимо сбросить безопасный канал. Можно воспользоваться одним из методов:

1 Зайти оснастку «Active Directory – пользователи и компьютеры», найти проблемный компьтер, нажать на нем правой кнопкой мыши и выбрать "Переустановить учетную запись" (Reset Account). После этого компьютер следует заново присоединить к домену и перезагрузить.

2 С помощью команды **Netdom**:

**Netdom reset <имя машины> /domain <Имя домена> /User0 <Имя пользователя> /Password0 <Пароль>** без кавычек <>

Пример: **Netdom reset COMP01 /domain pk-help.com /User0 Ivanov /Password \*\*\*\*\***  
Перезагрузка компьютера не нужна.

3 С помощью команды **Nltest**:

**Nltest  /server:<Имя компьютера> /sc\_reset:<Домен>\<Контроллер домена>**

Пример:**Nltest  /server:Comp01 /sc\_reset:pk-help.com\ad1**   
Перезагрузка компьютера не нужна.