**Группы в Active Directory**

Рассмотрим такое понятие, как группы в AD.

Группы содержат элементы (пользователей, компьютеры, другие группы), управление которыми осуществляется как одним объектом. В Windows Server существует семь типов групп - две группы доменов с тремя областями действий в каждой и локальная группа безопасности.

Существует два типа групп - **безопасности** и **распространения**.

**Группа распространения** - применяется для создания групп почтовых рассылок. Письмо, отправленное на группу распространения дойдет всем пользователям группы. Это группа не предназначена для работы с предоставлением доступа на ресурсы.

**Группа безопасности** - применяется для управления безопасности доступа к ресурсам. Т.е. если вы хотите для сетевой папки создать группу, для этого необходимо создать группу безопасности. Так же с помощью группы безопасности можно сделать почтовую рассылку, но это не рекомендуется делать, поскольку для этого есть группа распространения.

Помимо групп существует три области действия для каждой группы:

**Локальная в домене** - используется для управления разрешениями доступа к ресурсам в пределах всего домена.

**Глобальная группа** - используется для определения коллекции объектов доменов на основании бизнес-правил и управление объектами, которые требуют ежедневного использования.

**Универсальная группа** - Рекомендуется использовать в лесах из множества доменов. С помощью нее можно определять роли и управлять ресурсами, которые распределены на нескольких доменах.

Более наглядное отличие всех трех групп представлено в таблице.

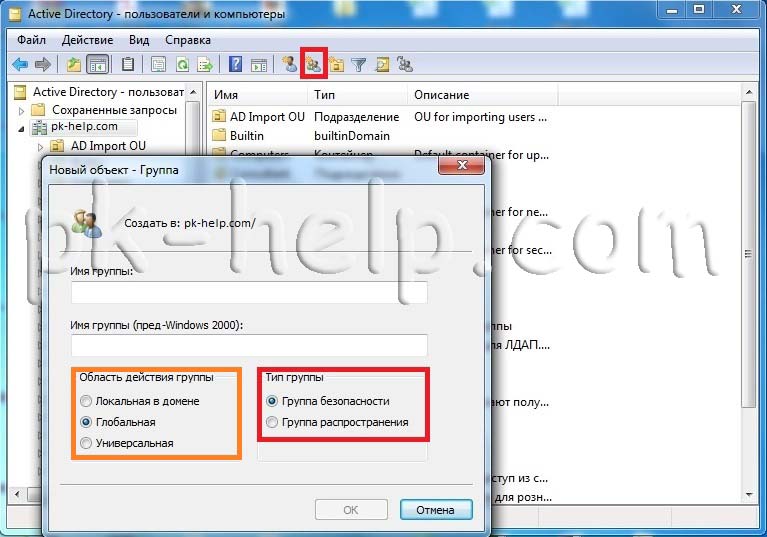
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Область действия группы** | **Члены группы из того же домена** | **Члены группы из другого домена в том же лесу** | **Члены группы из доверенного домена** | **Группе могут быть назначены разрешения в…** | **Область действия группы можно преобразовать в…** |
| Локальная в домене | - Пользователи  - Компьютеры  - Глобальные группы  - Локальные группы  - Локальные группы | - Пользователи  - Компьютеры  - Глобальные группы  - Локальные группы | - Пользователи  - Компьютеры  - Глобальные группы | Разрешения члена могут быть назначены только в домене, которому принадлежит родительская локальная группа домена | - в универсальную в том случае, если эта группа не содержит другую локальную группу в домене в качестве члена; |
| Универсальная группа | - Пользователи  - Компьютеры  - Глобальные группы  - Локальные группы | - Пользователи  - Компьютеры  - Глобальные группы  - Локальные группы | Нет доступа | Любой домен или лес | - в глобальную в том случае, если эта группа не содержит в качестве члена другую универсальную группу;  - в локальную группу в домене. |
| Глобальная группа | - Пользователи  - Компьютеры  - Глобальные группы | Нет доступа | Нет доступа | Разрешения члена могут быть назначены в любом домене | - в универсальную в том случае, если изменяемая группа не является членом другой глобальной группы; |

Последний столбец таблицы показывает, что существующую область действия группы можно изменить на любую из трех, единственный нюанс, что для изменения некоторых областей необходимо выполнить два шага, первый изменить на промежуточный, а уже затем на необходимый. Например, для того, чтобы изменить глобальную группу в локальную, потребуется изменить в начале на универсальную, а уже после этого в локальную группу.

Осталась одна группа, которую не рассмотрели - Локальная группа. Локальная группа считается самой примитивной, так как она доступна только на одном компьютере. Такая группа создается в базе данных диспетчера безопасности учетных записей рядового компьютера и поэтому в домене управление локальными группами не нужно.

### Создание группы с помощью консоли ****Active Directory- Пользователи и компьютеры.****

Для того что бы создать группу, необходимо запустить консоль **Active Directory- Пользователи и компьютеры**, зайти в необходимое подразделение нажать кнопку "**Создание новой группы в текущем контейнере**", в открывшемся окне **Новый объект- Группа** введите имя группы и выберите необходимый тип и область действия.



### Создание группы с помощью командной строки.

Для создания группы в командной строке служит команда Dsadd. Общий вид команды Dsadd group DN\_группы + дополнительные параметры.

**-secgrp**. Данный параметр указывает тип группы: безопасности (yes) или распространения (no). Если параметр не указан, то по умолчанию значением данного параметра считается yes;

**-scope**. Текущий параметр задает область действия группы. Доступные параметры: локальная в домене (l), глобальная (g) или универсальная (u). По умолчанию, также как и при помощи графического интерфейса, область действия назначается глобальной;

**-samid**. Этот параметр определяет использование для данной группы SAM имени, как уникального атрибута sAMAccountName группы. Желательно имя для sAMAccountName и группы указывать идентичные;

**-desc**. Данный параметр отвечает за краткое описание группы;

**-memberof**. Этот параметр назначает одну или несколько групп, к которым требуется добавить новую. Если групп несколько, то их следует добавлять через пробел;

**-members**. При помощи этого параметра вы можете добавить членов в группу. Члены должны указываться в виде DN-имен и разделяться пробелами.

Пример создания группы с помощью командной строки:

**Dsadd group «CN=Администраторы,OU=Группы,DC=pk-help,DC=com» -secgrp yes -scope g -samid «Администраторы сети» -desc «Администраторы сети»**