Настройка доверительных отношений между доменами Active Directory

Для возможности аутентификации с использованием учетных записей из нескольких доменов, необходимо, чтобы были доверительные отношения между последними. При создании домена в структуре леса, доверие выстраивается автоматически. Но если мы хотим объединить два домена разных организаций или которые раньше работали независимо друг от друга, то необходимо настроить доверительные отношения.

Мы будем рассматривать процесс настройки на примере двустороннего транзитивного доверия между доменами **kazan.wsr** (172.16.19.64) и **spb.wse** (172.16.20.96). Саму настройку разделим **на 2 этапа** — конфигурирование DNS и создания доверий. В качестве операционной системы по данной инструкции можно настроить Windows Server 2008 / 2012 / 2016 / 2019.

Определяемся с типом доверительных отношений

Доверительные отношению могут быть разных типов. Перед тем, как их настроить, нужно понять, какие нам требуются.

Одностороннее или двустороннее

Определяют направление доверия одного домена к другому.

В односторонних отношениях, только один домен доверяет другому. В результате, на компьютерах одного из доменов можно будет авторизоваться с использованием пользователей другого. При создании такого доверия нужно указать также направление (входящее или исходящее) — оно определяет чьи пользователи смогут проходить аутентификацию на чьем домене.

В двусторонних отношениях домены доверяют друг другу. Таким образом, аутентификация выполняется на всех компьютерах под пользователями любого из доменов.

Внешнее или доверие леса

Внешнее или нетранзитивное отношение устанавливается между двумя доменами напрямую вне леса.

Доверие леса или транзитивное отношение связывает леса и все их домены.

Настройка DNS

Для построения доверия необходимо, чтобы контроллеры домена видели друг друга. Все запросы на поиск узлов в AD выполняются через службы доменных имен. Таким образом, в нашем примере, мы должны сконфигурировать условную пересылку на DNS обоих доменов. Также важно, чтобы между контроллерами была сетевая доступность — по сети они должны видеть друг друга.

- **kazan.wsr** и **wsb.wse**

1. Открываем **Диспетчер серверов** - кликаем по **Средства** - **DNS**:

2. В открывшемся окне выбираем нужный сервер, если их несколько - раскрываем его - кликаем правой кнопкой мыши по **Серверы условной пересылки** - **Создать сервер условной пересылки**:
3. В «DNS-домен» пишем второй домен (в нашем случае, **secondary.local**), затем задаем его IP-адрес, ставим галочку **Сохранять условный сервер пересылки в Active Directory и реплицировать ее следующим образом** - выбираем **Все DNS-серверы в этом домене**:
4. Для проверки следует использовать команду **nslookup** в адрес только что добавленного домена. Если будет возвращен ответ с именем и адресом удаленного сервера, то все сделано правильно.

Настройка доверительных отношений

1. В домене kazan.wsr открываем **Диспетчер серверов** - кликаем по **Средства** - **Active Directory - домены и доверие**:
2. В открывшемся окне кликаем правой кнопкой по нашему домену - **Свойства**:
3. Переходим на вкладку **Отношения доверия** - кликаем по **Создать отношение доверия...**:
4. Нажимаем **Далее** - вводим имя для второго домена (**spb.wse**) и кликаем **Далее**:
5. Выбираем **Доверие леса** (если нам не нужно внешнее доверие) - **Далее**:
6. В окне «Направление отношения доверия» выбираем **Двустороннее**:
7. В следующем окне выбираем, на каком из доменов мы применяем настройку — если у нас есть права администратора для обоих доменов, то выбираем **Для данного и указанного доменов**:
8. Далее нужно выбрать «Уровень проверки подлинности исходящего доверия» — если оба домена принадлежат нашей организации, предпочтительнее выбрать **Проверка подлинности в лесу**, чтобы предоставить доступ ко всем ресурсам:
9. Доверие установлено

Источники:

- https://www.dmosk.ru/miniinstruktions.php?mini=trust-ad