Настройка freeradius через ldap · Wiki · ecotelecom / ecotree

Последовательность действий для настройки freeradius через ldap:

a)User подключается к bras с использованием username/password ->
b)bras отправляет request на radius ->
c)radius отправляет запрос на поиск пользователя с таким username и password в ldap и если пользователь найден, то радиус забирает из ldap указанный атрибут пользователя (например, service_name) ->
d)radius отправляет на bras accept(если нашел пользователя) или reject(если не нашел) и добавляет указанный атрибут ->
e)bras на основе ответа от радиуса либо устанавливает сессию, либо нет

1. (Необязательный пункт): подключиться с локальной машине к базе ldap

Рекомендую, чтобы проверить правильность всех данных и облегчить debug в дальнейшем, в первую очередь подключится с локальной машины к базе ldap, для этого можно использовать утилиту JXplorer

```
sudo apt-get install jxplorer
```

После установки программы выбрать "Connect to a DSA" и заполнить необходимые поля. Пример для ldap компании rdp.ru:

```
        server = "10.210.9.99"
        port = 389
        identity = 'cn=vmail,dc=rdp,dc=ru'
        password = СпросиУДениса
        base_dn = 'domainName=rdp.ru,o=domains,dc=rdp,dc=ru'
```

После успешного подключения должна появится древовидная структура с группами и пользователями. У каждого пользователя есть три атрибута необходимых нам(в вашей схеме могут потребоваться совсем другие атрибуты): uid, userPassword, accountStatus Первые два нужны для аутентификации, а последний атрибут показывает заблокирован пользователь или нет, но мы данный атрибут в дальнейшем будем использовать в качестве имени сервиса

2. Настройка модуля ldap для freeradius

Теперь заходим на машину с радиусом в директорию:

```
cd /etc/raddb/mods-available
```

и изменяем файл ldap:
Как и в пункте 1:

```
        server = "10.210.9.99"
        port = 389
        identity = 'cn=vmail,dc=rdp,dc=ru'
        password = СпросиУДениса
        base_dn = 'domainName=rdp.ru,o=domains,dc=rdp,dc=ru'
```

кроме этого:

```
        update {
                control:Password-With-Header    += 'userPassword'
#               control:NT-Password             := 'ntPassword'
                reply:SERVICE_NAME              := 'accountStatus'
#               reply:Tunnel-Type               := 'radiusTunnelType'
#               reply:Tunnel-Medium-Type        := 'radiusTunnelMediumType'
#               reply:Tunnel-Private-Group-ID   := 'radiusTunnelPrivategroupId'
```

В первой строке как раз указывается с каким атрибутом в базе ldap сравнивается пароль пользователя, в данном примере userPassword

Во второй незакомменченой строке говорится, что в случае успешной аутентификации в ответ(reply) от радиуса добавить артибут с именем SERVICE_NAME, значением которого будет значение из атрибута accountStatus в ldap

UPDATE 5.09.18 Настройка выше предполагает использование протокола PAP, для использования CHAP необходимо добавить в поле update добавить строку

```
                control:Cleartext-Password    += 'userPassword'
```

Но в таком случае в атрибуте userPassword в ldap должен хранится пароль в открытом виде, а не md5 хэш. Дело в том, что пользователь отправляет на радиус challenge + хэш, посчитанный от пароля и challenge, и для того, чтобы радиус смог посчитать такой же хэш ему не хватает пароля в открытом виде

3. Подключение модуля ldap

у радиуса есть три папки:
mods-availiable - доступные модули
mods-config - содержит конфигурационные файлы для модулей
mods-enabled - подключенные модули
На предыдущем этапе мы настроили модуль ldap, но он еще не работает, чтобы его подключить нужно перейти в папку mods-enabled и сделать символьную ссылку:

```
ln -s ../mods-available/ldap ldap
```

А также в /etc/raddb/sites-available/default закомментить строки со словом

```
files
```

и расскоментить со словом (оно может быть уже расскоменчено)

```
ldap
```

Тоже самое сделать в In /etc/raddb/sites-available/inner-tunnel + расскоментить секцию:

```
Auth-Type LDAP {
        ldap
}
```

4. Добавить недефолтные атрибуты в словарь радиуса

В нашем примере радиус должен в ответах отправлять атрибут SERVICE_NAME, который является Vendor Specific компании rdp (даже Wireshark уже это знает, а ты до сих пор нет!), поэтому его нужно добавить в dictionary, для этого:

```
cd /etc/raddb
echo VENDOR        RDP        45555 > /etc/raddb/dictionary
echo BEGIN-VENDOR RDP >> /etc/raddb/dictionary
echo ATTRIBUTE    SERVICE_NAME        250    string >> /etc/raddb/dictionary
echo END-VENDOR    RDP >> /etc/raddb/dictionary
```

5. Установить библиотеку freeradius-ldap

Без нее радиус не запустится:

```
apt-get install freeradius-ldap
```

P.S на alpine соответственно apk add

6. Проверить, что все работает

На этом настройка радиуса завершена, если все ок, то после команды:

```
radiusd -X
```

он должен успешно включиться

P.S. По ссылке ниже доступно хорошее видео по настройке freeradius через ldap

```
https://www.youtube.com/watch?v=weTfRslHhZY
```

P.P.S Добавил radius_volume с готовым конфигом freeradius для ldap, его можно просто scp'шнуть в папку /mnt/extended/docker/volumes/radius_volume/ и если после копирования собьются права, то вернуть ихradius_volume.zip