

Samba: миграция на LDAP

Здесь описаны процедуры миграции с [MS Windows NT4 PDC](#) и [Samba \(passdb.tdb\)](#) на Samba 3 с использованием в качестве хранилища [OpenLDAP](#).

В процессе миграции демоны Samba на принимающем сервере могут быть остановлены.

Для успешного завершения процесса нужно подготовить сервер [OpenLDAP](#) для приёма данных.

[Примеры структур Samba LDAP](#)

MS Windows NT4 PDC

1. Нужно создать файл:

[smb.conf](#)

```
[global]
workgroup = ИМЯ_ДОМЕНА_NT4
domain master = no
ldap admin dn = dc=example,dc=domain,dc=com
ldap suffix = dc=example,dc=domain,dc=com
ldap group suffix = ou=groups
ldap user suffix = ou=users
ldap machine suffix = ou=computers
```

2. Добавить в домен:

```
net rpc join -S КОНТРОЛЛЕР_ДОМЕНА -w ИМЯ_ДОМЕНА -U АДМИНИСТРАТОР_ДОМЕНА
```

Импорт данных из NT4 PDC

[vampire2ldif.sh](#)

```
#!/bin/bash

net rpc vampire ldif -S КОНТРОЛЛЕР_ДОМЕНА -s ПУТЬ_К_ФАЙЛУ_smb.conf -U АДМИНИСТРАТОР_ДОМЕНА
>NT4.ldif
```

Ограничения net rpc vampire ldif

Не выдаётся список: Разрешённые рабочие станции (Logon Workstations)

Решение: На ПК с [MS Windows](#) использовать для каждого нужного пользователя команду:

```
net user ПОЛЬЗОВАТЕЛЬ /domain
```

Экспорт данных в LDAP сервер

Скрипт NT4_Split_LDIF.pl разделяет файл NT4.ldif на следующие файлы:

- NT4_1.ldif (группы и пользователи)
- NT4_2.ldif (члены групп)

NT4_Split_LDIF.pl

```
#!/usr/bin/perl

$lines="";
open(FILE,"NT4.ldif") or die $!;
open(FILE_1,">NT4_1.ldif") or die $!;
select FILE_1;

while(<FILE>){
    if(/SAM_DATABASE_DOMAIN: MODIFY ENTITIES/i){
        last;
    }else{
        $lines.=$_;
        print "$_";
    }
}
close(FILE_1);

$lines="";
open(FILE_2,">NT4_2.ldif") or die $!;
select FILE_2;
while(<FILE>){
    if(/SAM_DATABASE_BUILTIN: ADD ENTITIES/i){
        last;
    }else{
        $lines.=$_;

        s{ou=groups,dc=examlpe,dc=domain,dc=com}{ou=groups,dc=examlpe,dc=domain,dc=com\nreplace:
memberUid};
        print "$_";
    }
}
close(FILE_2);
close(FILE);
```



Нужно заменить ou=groups,dc=examlpe,dc=domain,dc=com на реальный путь к группам.

Исправления

Нужно найти наибольший RID для пользователя и записать его в поле sambaNextRid записи домена.

Samba (passdb.tdb)

Здесь описаны действия по миграции данных из старых версий Samba, в которых использовался файл passdb.tdb.

1. Надо задать пароль доступа к LDAP серверу

```
smbpasswd -w passwd
```

2. Создать файл:

smb.conf

```
[global]
ldap ssl = off
passdb backend = ldapsam:ldap://АДРЕС_СЕРВЕРА_LDAP/
```

```
ldap admin dn = cn=admin,dc=example,dc=domain,dc=com
ldap suffix = dc=example,dc=domain,dc=com
ldap group suffix = ou=groups
ldap user suffix = ou=users
ldap machine suffix = ou=computers
```

3. Выполнить команду:

```
pdbedit -s ПУТЬ_К_ФАЙЛУ_smb.conf -i tdbsam://ПУТЬ_К_ФАЙЛУ_passdb.tdb -e
ldapsam:ldap://АДРЕС_СЕРВЕРА_LDAP
```

4. Группы нужно брать из файла /etc/groups/

⚠ Для контроля над изменениями данных (в период тестирования) на старом сервере можно использовать команду:

```
pdbedit -L -w >old_`date '+%Y-%m-%d'`.txt
```

Дополнительные команды

⚠ Должны выполняться на контроллере домена (источнике)

- Дамп passdb.tdb

```
pdbedit -Lw
```

- Дамп SID

```
pdbedit -L -v
```

- Получение SID контроллера домена|

```
net getlocalsid
```

Ссылки

[Chapter 9. Migrating NT4 Domain to Samba-3](#)

https://sysadminmosaic.ru/samba/migrate_ldap

2019-05-11 00:39

