Mar 15 · 9 min read

Миграция доменного контроллера Windows 2008R2 в Samba4

Стояла задача переноса контроллера домена Windows Server 2008R2 на Samba4 вместе пользователями, группами и политиками (GPO). Единственным верным решением было присоединение Samba4 в режиме domain controller к Windows Server 2008R2 с передачей ролей. Создание домена 2008R2 я расписывать не буду, процесс настройки Samba4 был рассмотрен **здесь**.

Процесс переноса будет происходить в четыре этапа:

1. Подключение Samba4 (BDC) к домену,
2. Передача и принятие ролей FSMO,
3. Удаление DC Windows Server 2008R2 (PDC),
4. Проверка результата.

Исходные сетевые настройки следующие:

- **PDC:** Netbios: DCTEMP | 192.168.0.201 и 192.168.1.201—Windows Server 2008R2
- **BDC:** Netbios: DC | 192.168.0.202 и 192.168.1.202—Samba4

Подключение Samba4 к домену.

Проверяем */etc/krb.conf*:

```
# nano /etc/krb.conf
```

```
[libdefaults]
 default_realm = DOMAIN.LOCAL
 dns_lookup_realm = true
 dns_lookup_kdc = true
```

Прописываем primary DNS:

```
# nano /etc/resolv.conf
```

```
nameserver 192.168.0.201
nameserver 8.8.8.8
```

Сверяем время:

```
date
```

Если разница будет более пяти минут возникнут проблемы с подключением. Проверяем аутентификацию Kerberos:

```
kinit Administrator@DOMAIN.LOCAL
klist
```

Если в ответ на команду *klist* вы получили что-то наподобие:

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@DOMAIN.LOCAL

Valid starting Expires Service principal
03/10/2016 02:44:57 03/10/2016 12:44:57
krbtgt/DOMAIN.LOCAL@DOMAIN.LOCAL
 renew until 03/11/2016 02:44:54
```

то можно вводить Samba в домен:

```
# /usr/local/samba/bin/samba-tool domain join
domain.local DC -Uadministrator --realm=domain.local
```

Если в качестве DNS используется Bind, то:

```
# /usr/local/samba/bin/samba-tool domain join
domain.local DC -Uadministrator --realm=domain.local
```

При успешном выполнении увидим что-то наподобие:

```
Joined domain DOMAIN (SID S-1-5-21-1242296740-777803924-
1461537156) as a DC
```

Проверяем, создались ли записи DNS:

```
# host -t A dc.domain.local
```

```
dc.domain.local has address 192.168.0.202
dc.domain.local has address 192.168.1.202
[root@dc samba-master]# host -t A dctemp.domain.local
dctemp.domain.local has address 192.168.0.201
dctemp.domain.local has address 192.168.1.201
```

В случае сбоя придется добавить A-запись вручную:

```
# samba-tool dns add IP-of-your-DNS-server domain.lan dc
A 192.168.0.202 -Uadministrator
# samba-tool dns add IP-of-your-DNS-server domain.lan dc
A 192.168.1.202 -Uadministrator
```

Проверим разрешается ли objectGUID в новое имя хоста:

```
# /usr/local/samba/bin/ldbsearch -H
/usr/local/samba/private/sam.ldb '(invocationid=*)' --
cross-ncs objectguid
```

Результат должен быть примерно таким:

```
# record 1
dn: CN=NTDS
Settings,CN=LostAndFoundConfig,CN=Configuration,DC=domai
n,DC=local
objectGUID: dd1a9239-02a0-4299-964d-75f3b9c54aa1
```

```
# record 2
dn: CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
objectGUID: bf035a91-72f6-4322-bdbf-bae54e342b36

# returned 2 records
# 2 entries
# 0 referrals
```

Для поиска objectGUID нового сервера:

```
# host -t CNAME dd1a9239-02a0-4299-964d-
75f3b9c54aa1._msdcs.domain.local
```

Если в результате запись не будет найдена:

```
Host dd1a9239-02a0-4299-964d-
75f3b9c54aa1._msdcs.kanon.local not found: 3(NXDOMAIN)
```

то придется создать (в нашем случае для каждой подсети):

```
# /usr/local/samba/bin/samba-tool dns add 192.168.0.202
_msdcs.kanon.local dd1a9239-02a0-4299-964d-75f3b9c54aa1
CNAME dc.kanon.local -Uadministrator

# /usr/local/samba/bin/samba-tool dns add 192.168.1.202
_msdcs.kanon.local bf035a91-72f6-4322-bdbf-bae54e342b36
CNAME dc.kanon.local -Uadministrator
```

Если в качестве DNS-бэкенда используется BIND, то читайте: “**Вновь добавляемые DNS записи не разрешаются**”.

Теперь проверим репликацию между контроллерами доменов:

```
# /usr/local/samba/bin/samba-tool drs showrepl
```

Вот тут у меня выдало ошибку:

```
ERROR(<class 'samba.drs_utils.drsException'>): DRS
connection to dc.domain.local failed — drsException: DRS
connection to dc.domain.local failed: (-1073741772, 'The
object name is not found.')
 File "/usr/local/samba/lib64/python2.7/site-
packages/samba/netcmd/drs.py", line 41, in
drsuapi_connect
 (ctx.drsuapi, ctx.drsuapi_handle,
ctx.bind_supported_extensions) =
drs_utils.drsuapi_connect(ctx.server, ctx.lp, ctx.creds)
 File "/usr/local/samba/lib64/python2.7/site-
packages/samba/drs_utils.py", line 54, in
drsuapi_connect
 raise drsException("DRS connection to %s failed: %s" %
(server, e))
```

Хотя на PDC в RSAT в оснастке "Пользователи и компьютеры Active Directory" отображались оба домен-контроллера. Оказалось, нужно было исправить:

```
# nano /etc/resolv.conf
```

```
nameserver 127.0.0.1
nameserver 192.168.0.201
nameserver 8.8.8.8
```

и:

```
# nano /etc/krb5.conf
```

```
[libdefaults]
 default_realm = DOMAIN.LOCAL
 dns_lookup_realm = true
 dns_lookup_kdc = true
```

Перезапускаем Samba, проверяем настройки DNS

```
# service samba4 restart && host -t A
dctemp.domain.local
```

```
dctemp.domain.local has address 192.168.1.201
dctemp.domain.local has address 192.168.0.201
```

```
# host -t A dc.domain.local
```

```
dc.domain.local has address 192.168.0.202
dc.domain.local has address 192.168.1.202
```

и заново смотрим информацию о репликации:

```
# /usr/local/samba/bin/samba-tool drs showrepl
```

```
Default-First-Site-Name\DC
DSA Options: 0x00000001
DSA object GUID: bf035a91-72f6-4322-bdbf-bae54e342b36
DSA invocationId: aa4b58df-2f3b-497d-8bda-ee1fc1faf5b8
```

```
==== INBOUND NEIGHBORS ====
```

```
DC=ForestDnsZones,DC=domain,DC=local
 Default-First-Site-Name\DCTEMP via RPC
 DSA object GUID: dd1a9239-02a0-4299-964d-75f3b9c54aa1
 Last attempt @ Thu Mar 10 08:07:15 2016 MSK was
successful
 0 consecutive failure(s).
 Last success @ Thu Mar 10 08:07:15 2016 MSK
```

```
CN=Schema,CN=Configuration,DC=domain,DC=local
 Default-First-Site-Name\DCTEMP via RPC
 DSA object GUID: dd1a9239-02a0-4299-964d-75f3b9c54aa1
 Last attempt @ Thu Mar 10 08:07:15 2016 MSK was
successful
 0 consecutive failure(s).
 Last success @ Thu Mar 10 08:07:15 2016 MSK


DC=domain,DC=local
 Default-First-Site-Name\DCTEMP via RPC
 DSA object GUID: dd1a9239-02a0-4299-964d-75f3b9c54aa1
 Last attempt @ Thu Mar 10 08:07:15 2016 MSK was
successful
 0 consecutive failure(s).
 Last success @ Thu Mar 10 08:07:15 2016 MSK
```

```
CN=Configuration,DC=domain,DC=local
 Default-First-Site-Name\DCTEMP via RPC
 DSA object GUID: dd1a9239-02a0-4299-964d-75f3b9c54aa1
 Last attempt @ Thu Mar 10 08:07:15 2016 MSK was
successful
 0 consecutive failure(s).
 Last success @ Thu Mar 10 08:07:15 2016 MSK
```

```
DC=DomainDnsZones,DC=domain,DC=local
 Default-First-Site-Name\DCTEMP via RPC
 DSA object GUID: dd1a9239-02a0-4299-964d-75f3b9c54aa1
 Last attempt @ Thu Mar 10 08:07:15 2016 MSK was
successful
 0 consecutive failure(s).
 Last success @ Thu Mar 10 08:07:15 2016 MSK
```

```
==== OUTBOUND NEIGHBORS ====
```

```
CN=Schema,CN=Configuration,DC=domain,DC=local
 Default-First-Site-Name\DCTEMP via RPC
 DSA object GUID: dd1a9239-02a0-4299-964d-75f3b9c54aa1
 Last attempt @ Thu Mar 10 07:52:23 2016 MSK was
successful
 0 consecutive failure(s).
 Last success @ Thu Mar 10 07:52:23 2016 MSK
```

```
DC=domain,DC=local
 Default-First-Site-Name\DCTEMP via RPC
 DSA object GUID: dd1a9239-02a0-4299-964d-75f3b9c54aa1
 Last attempt @ Thu Mar 10 07:52:23 2016 MSK was
successful
 0 consecutive failure(s).
 Last success @ Thu Mar 10 07:52:23 2016 MSK
```

```
CN=Configuration,DC=domain,DC=local
 Default-First-Site-Name\DCTEMP via RPC
 DSA object GUID: dd1a9239-02a0-4299-964d-75f3b9c54aa1
 Last attempt @ Thu Mar 10 07:52:23 2016 MSK was
successful
 0 consecutive failure(s).
 Last success @ Thu Mar 10 07:52:23 2016 MSK
```

```
==== KCC CONNECTION OBJECTS ====
```

```
Connection —
 Connection name: 69973043-da7f-4497-a47a-f8bc9e8347a9
 Enabled : TRUE
 Server DNS name : DCTEMP.domain.local
 Server DN name : CN=NTDS
Settings,CN=DCTEMP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
 TransportType: RPC
 options: 0x00000001
Warning: No NC replicated for Connection!
```

Для окончательной проверки успешной репликации необходимо создать по одному объекту на каждом контроллере домена. Например, создадим по одному пользователю на каждом контроллере домена и проверим, реплицируются ли они.

1. Создадим пользователя testuser1 в Windows Server (PDC). Создадим пользователя в оснастке AD “Пользователи и компьютеры”, или через Powershell от имени администратора:

```
Import-Module ActiveDirectory
```

после того, как включили возможность управлять пользователями через Powershell создаем пользователя:

```
New-ADUser -SamAccountName testuser1 -AccountPassword
(read-host "Set user password" -assecurestring) -name
"testuser1" -enabled $true -PasswordNeverExpires $true -
ChangePasswordAtLogon $false
```

2. Создадим пользователя user2 в samba 4 server (BDC):

```
# /usr/local/samba/bin/samba-tool user add testuser2
```

Смотрим список пользователей в Samba:

```
# /usr/local/samba/bin/wbinfo -u
```

и в оснастке “Active Directory: Пользователи и компьютеры” в Windows Server (PDC).

Передача ролей FSMO.

FSMO, или Flexible Single-Master Operations—это операции выполняемые контроллерами домена *Active Directory (AD)*, которые требуют обязательной уникальности сервера для каждой операции. В зависимости от типа операции уникальность FSMO подразумевается в пределах или леса доменов, или домена. Различные типы FSMO выполняются одним или несколькими контроллерами домена. Если в сети несколько контроллеров доменов необходимо, то требуется определить владельцев ролей FSMO (Flexible single-master operations).

Определение владельцев для Windows Server:

> *dsquery server -hasfsmo schema—Schema Master*
> *dsquery server -hasfsmo name—Domain Naming Master*
> *dsquery server -hasfsmo rid—Relative ID Master*

> *dsquery server -hasfsmo pdc—Primary Domain Controller Emulator*
> *dsquery server -hasfsmo infr—Infrastructure Master*
> *dsquery server -forest -isgc—Global Catalog (GC)*

Определение владельцев для Samba4:

```
# /usr/local/samba/bin/samba-tool fsmo show
```

В данном случае все роли принадлежат Windows Server (PDC):

```
SchemaMasterRole owner: CN=NTDS
Settings,CN=DCTEMP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
InfrastructureMasterRole owner: CN=NTDS
Settings,CN=DCTEMP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
RidAllocationMasterRole owner: CN=NTDS
Settings,CN=DCTEMP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
PdcEmulationMasterRole owner: CN=NTDS
Settings,CN=DCTEMP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
DomainNamingMasterRole owner: CN=NTDS
Settings,CN=DCTEMP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
DomainDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DCTEMP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
ForestDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DCTEMP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
```

Передачу ролей можно осуществить с правами “администратора домена”, “администратора схемы”, “администратора предприятия”. Существуют добровольный способ передачи и принятие ролей. Я рекомендую воспользоваться добровольной передачей ролей с PDC на BDC.

На всякий случай на нашем Windows Server (PDC) в дополнительном DNS прописываем адрес второго домен контроллера, которому передаем роли. Должно быть так:

> *DNS1: 127.0.0.1*
> *DNS2: 192.168.0.202*

И из командной строки Windows Server (PDC) поочередно вводим:

```
ntdsutil
roles
connections
connect to server dc
q
```

После уведомления об успешном подключении вводим (FSMO maintance):

```
transfer naming master
transfer infrastructure master
transfer rid master
transfer schema master
transfer pdc
```

Проверяем результат:

```
# /usr/local/samba/bin/samba-tool fsmo show

SchemaMasterRole owner: CN=NTDS
Settings,CN=DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
InfrastructureMasterRole owner: CN=NTDS
Settings,CN=DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
RidAllocationMasterRole owner: CN=NTDS
Settings,CN=DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
PdcEmulationMasterRole owner: CN=NTDS
Settings,CN=DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
DomainNamingMasterRole owner: CN=NTDS
Settings,CN=DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
DomainDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DCTEMP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
ForestDnsZonesMasterRole owner: CN=NTDS
Settings,CN=DCTEMP,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=domain,DC=local
```

Первые пять ролей переданы, о чем свидетельствует надпись “CN=**DC**”. DomainDnsZonesMasterRole и ForestDnsZonesMasterRole

передаются следующим образом:

```
# /usr/local/samba/bin/samba-tool fsmo seize --
role=forestdns
# /usr/local/samba/bin/samba-tool fsmo seize --
role=domaindns
```

Здесь вы можете получить ошибку:

```
Attempting transfer...
ERROR: Failed to delete role 'forestdns': LDAP error 50
LDAP_INSUFFICIENT_ACCESS_RIGHTS -  <00002098: SecErr:
DSID-0315211E, problem 4003 (INSUFF_ACCESS_RIGHTS), data
0
```

Потому как вышеизложенный способ при использовании SAMBA_INTERNAL в качестве DNS-бэкенда **не работает.** Можно использовать более **принудительный** способ принятия ролей (что не рекомендуется):

```
# /usr/local/samba/bin/samba-tool fsmo seize --force --
role=forestdns
# /usr/local/samba/bin/samba-tool fsmo seize --force --
role=domaindns
```

Вполне возможно, проблему удастся решить простым исправлением на стороне Windows Server (PDC)—из командной строки:

```
adsiedit.msc
```

Выбираем *Action -> Connect to…* и создаем новое соединение:

1. Computer: DCTEMP.domain.local

2. В поле Connection point вводим: **DC=ForestDnsZones, DC=domain,DC=local**
(без пробелов и в одну строку, как на скриншоте слева)

3. В раскрывающихся списках находим **CN=Infrastructure**, дважды кликаемся и в раскрывшемся окне находим

fSMORoleOwner и дважды кликаем.

4. Находим **CN=DCTEMP** и меняем на CN=DC.

5. Повторяем все заново с первого пункта, но вместо DC=ForestDnsZones указываем: **DC=DomainDNSZones**.

Но исправление через adsiedit в моем случае оказалось так же неэффективным:

```
Operation failed. Error code 0x20ae
The role owner attribute could not be read.

000020AE: SvcErr: DSID-03152965, problem 5003
(WILL_NOT_PERFORM), data 0
```

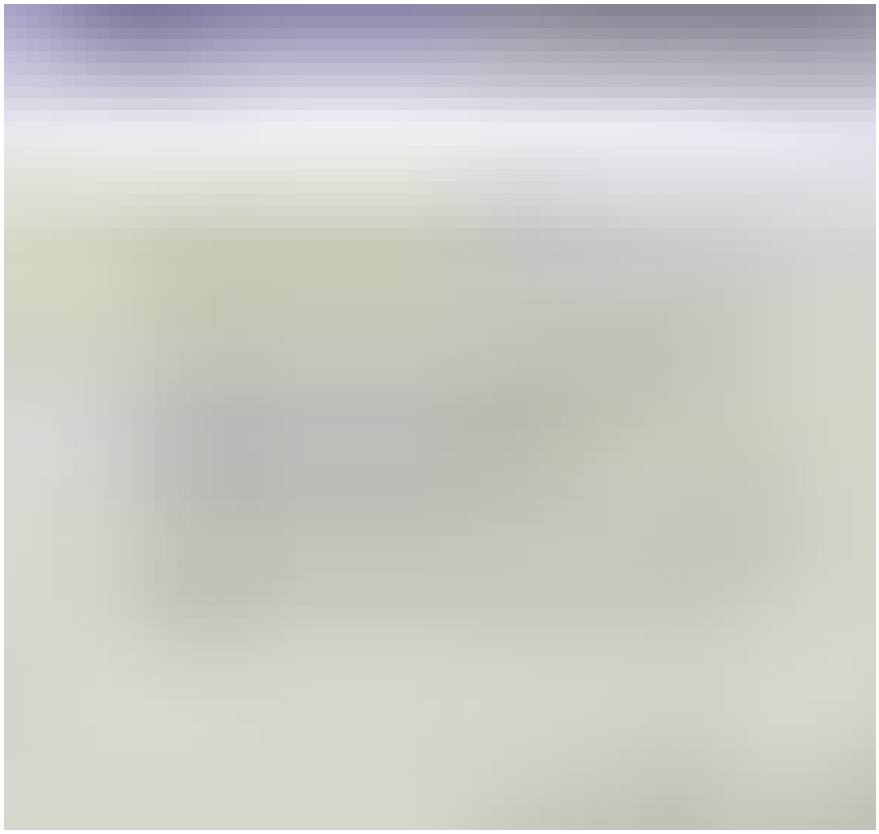
Если все прошло успешно, то проверяем результат через samba-tool и на этом этап передачи ролей завершен. Теперь можем произвести дополнительные настройки: сменить DNS, перенести, или добавить сетевые папки, создать правила iptables и тд. Лично я предпочел протестировать пару дней BDC с

выключенным Windows Server (PDC) и лишь только затем перешел к этапу полного удаления PDC.

Удаление DC Windows Server 2008R2.

Для демонтажа контроллера домена на стороне Winows Server (PDC) необходимы права “Администратором домена”. Удаление контроллера можно осуществить средствами графического интерфейса или через командную строку. Сам процесс удаления через графический интерфейс затруднений вызвать не должен:

```
dcpromo
```



Снимаем галочку—это не последний контроллер. Игнорируем сообщение, что это последний DNS-сервер:

> *The Active Directory domain controller appears to be the last DNS server for the following Active Directory-integrated zones:*

> *_msdcs.domain.local*
> *domain.local*

вводим пароль и продолжаем.

В моем случае PDC на смог связаться с DNS-бэкендом, на что отреагировал сообщением:

> *The operation failed because:*

> *Active Directory Domain Services could not find another Active Directory Domain Controller to transfer the remaining data in directory partition DC=DomainDNSZones,DC=domain,DC=local.*

> *“The specified domain either does not exist or could not be contacted”.*

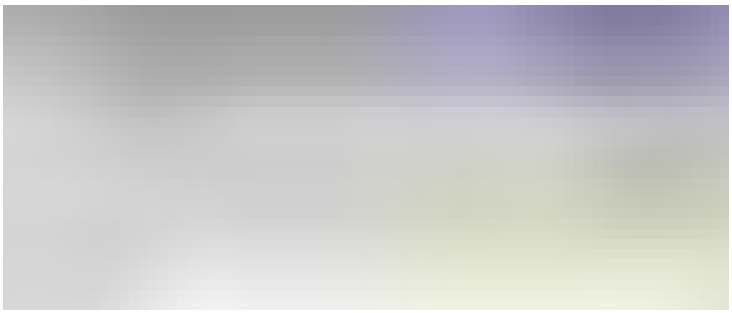
Если мастер понижения контроллера домена успешно завершен, то Windows Server можно просто выключить и перейти к этапу №4: проверка результата. В противном случае—в командной строке повторно запускаем мастер с дополнительными ключами:

```
dcpromo /forceremoval
```

Игнорируем все предупреждения и по завершению выключаем Windows Server (он нам больше не нужен) и на стороне Samba4 выполняем:

```
/usr/local/samba/bin/samba-tool domain demote — remove-
other-dead-server=DCTEMP
```

Далее на любом присоединенным к домену Windows-компьютере копируем и выполняем **этот скрипт**.



Вводим netbios-имя, жмем ОК, отвечаем на предупреждение “да” и получаем сообщение: Metadata Clean Completed for DCTEMP.

На всякий случай исправим возможные ошибки БД:

```
# /usr/local/samba/bin/samba-tool dbcheck --fix
```

Теперь на всякий случай добавим в конфигурации Samba следующие строки:

```
# nano /usr/local/samba/etc/smb.conf
```

```
[global]
        domain master = yes
        local master = yes
        domain master = yes
        preferred master = yes
```

Проверка результата.

На введенном в домен компьютере под управлением Windows 7 устанавливаем RSAT и открываем оснастку “Active Directory—пользователи и компьютеры”, открываем контейнер “Domain Controllers”, дабы убедиться, что отсоединенный контроллер домена отсутствует:

Аналогично сверяем результат в оснастке “Active Directory— сайты и службы”:

И в завершение необходимо убедиться, что в зонах DNS все записи для DCTEMP удалены:

Если, все же, записи dctemp по прежнему там остались то меняем их вручную. В моем случае пришлось заменить в папках верхнего уровня в зонах прямого просмотра ‘dctemp’ на ‘dc’: