Резервный контроллер домена на Debian 8

автор: ub4acj | 10.11.2016 | 2 Комментарии

Samba, Компьютеры

ActiveDirectory, Debian, Linux, Samba, Контроллер домена

В прошлой статье под названием "Контроллер домена на Debian 8 (...в котором уже есть собранная Samba4)" я рассказывал как поднять первичный контроллер домена Active Directory. В этой статье я расскажу как дополнить домен резервным (BDC) контроллером домена Active Directory и настроить репликацию между двумя контроллерами. Резервный контроллер мы будем строить на **Debian GNU/Linux 8.6.0 "Jessie" i386.**

Искренне надеюсь, что у нас уже есть работающий Samba AD DC со следующими сетевыми параметрами:

```
адрес сервера: 192.168.1.2;
маска подсети: 255.255.255.0;
шлюз: 192.168.1.1;
DNS-сервер: 192.168.1.2;
имя сервера: pdc;
имя домена: unlis.local.
```

Также крайне желательно иметь компьютер с Windows 7 с установленными **средствами удаленного администрирования сервера** и учетной записью администратора домена.

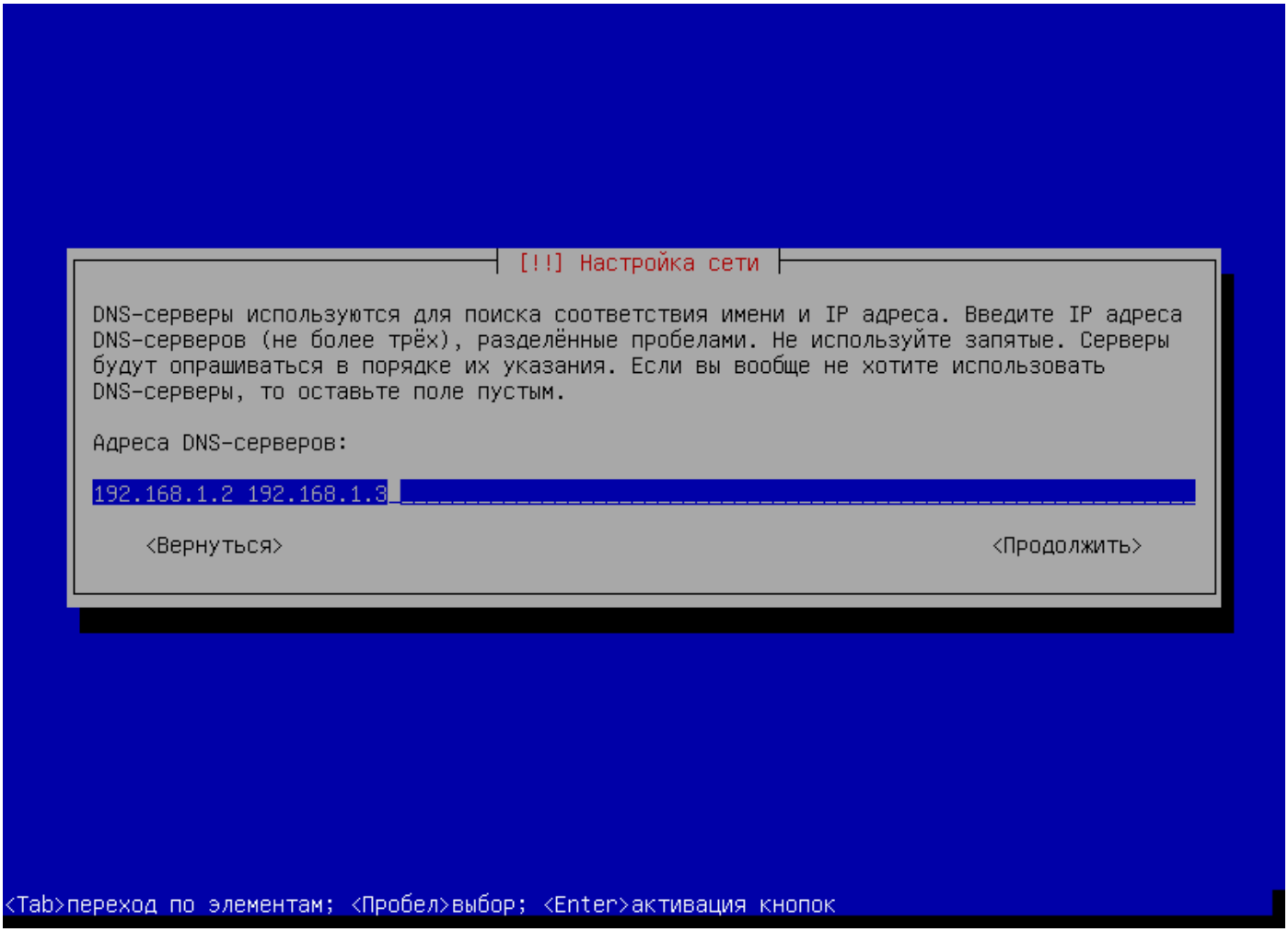
Весь процесс условно разбит на четыре пункта:

- Установка Debian, Samba и необходимых компонентов, первичная настройка;
- Добавление Samba в домен, настройка DNS-сервера, синхронизации времени;
- Добавление записей в DNS и запуск репликации каталога Active Directory;
- Настройка репликации SYSVOL.

Итак. На **первом пункте** останавливаться подробно не вижу смысла - все то же самое, что и в первой статье, за исключением нескольких моментов. Это сетевые параметры. Для резервного контроллера домена они будут такими:

```
адрес сервера: 192.168.1.3;
маска подсети: 255.255.255.0;
шлюз: 192.168.1.1;
DNS-сервер: 192.168.1.2, 192.168.1.3;
имя сервера: bdc;
имя домена: unlis.local.
```

При установке отказываемся от настройки сети по DHCP и настраиваем сеть вручную. Настройку DNS выполняем следующим образом:



После установки в файле ***/etc/network/interfaces*** должно быть:

```
<...>
dns-nameservers 192.168.1.2 192.168.1.3
```

Также не забываем про файл ***/etc/resolv.conf***:

```
domain unlis.local
nameserver 192.168.1.2
nameserver 192.168.1.3
```

Далее устанавливаем **samba4**, **krb5-user, ntp, smbclient, winbind** и **bind9** командой ***apt-get install samba ntp smbclient krb5-user bind9 winbind***. Также как и в предыдущей статье krb5-user спросит realm, kdc и admin server. Можно оставить пустым и настроить позже, можно прописать в первом окне ***UNLIS.LOCAL*** (обязательно в верхнем регистре), во втором и третьем - сокращенное имя нашего основного контроллера, то есть ***pdc***. В любом случае необходимо после установки пакетов проверить содержимое файла ***/etc/krb5.conf***. Минимальная конфигурация:

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

Но я не ищу легких путей, поэтому привожу полную:

```
[libdefaults]
default_realm = UNLIS.LOCAL
dns_lookup_realm = false
dns_lookup_kdc = true
krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true

v4_instance_resolve = false
v4_name_convert = {
host = {
rcmd = host
ftp = ftp
}
plain = {
something = something-else
}
}
fcc-mit-ticketflags = true
[realms]
UNLIS.LOCAL = {
kdc = pdc
admin_server = pdc
default_domain = UNLIS.LOCAL
}

[domain_realm]
.unlis.local = UNLIS.LOCAL
unlis.local = UNLIS.LOCAL
```

Сразу тестируем:

```
root@bdc:~# kinit Administrator
Password for Administrator@UNLIS.LOCAL:
Warning: Your password will expire in 41 days on Чт 22 дек 2016 01:55:48

root@bdc:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
```

```
Default principal: Administrator@UNLIS.LOCAL

Valid starting Expires Service principal
10.11.2016 15:19:42 11.11.2016 01:19:42 krbtgt/UNLIS.LOCAL@UNLIS.LOCAL
renew until 11.11.2016 15:19:37
```

Далее переходим ко **второй части** нашего рассказа - ввода резервного контроллера в домен. Сделаем это командой ***samba-tool domain join unlis.local DC --realm=unlis.local --dns-backend=BIND9_DLZ -UAdministrator*** . Если при этом появилась ошибка

```
ERROR(<class 'samba.provision.ProvisioningError'>): Provision failed -
ProvisioningError: guess_names: 'server role=standalone server' in /etc/samba/smb.conf
must match chosen server role 'active directory domain controller'! Please remove the
smb.conf file and let provision generate it
```

удаляем или перемещаем файл ***/etc/samba/smb.conf*** и выполняем команду заново.

```
root@bdc:~# samba-tool domain join unlis.local DC --realm=unlis.local --dns-
backend=BIND9_DLZ -UAdministrator
Finding a writeable DC for domain 'unlis.local'
Found DC pdc.unlis.local
Password for [WORKGROUP\Administrator]: <Пароль_администратора_домена>
workgroup is UNLIS
realm is unlis.local
checking sAMAccountName
Adding CN=BDC,OU=Domain Controllers,DC=unlis,DC=local
Adding CN=BDC,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=unlis,DC=local
Adding CN=NTDS Settings,CN=BDC,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=unlis,DC=local
Adding SPNs to CN=BDC,OU=Domain Controllers,DC=unlis,DC=local
Setting account password for BDC$
Enabling account
Adding DNS account CN=dns-BDC,CN=Users,DC=unlis,DC=local with dns/ SPN
Setting account password for dns-BDC
Calling bare provision
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
```

```
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
A Kerberos configuration suitable for Samba 4 has been generated at /var/lib/samba
/private/krb5.conf
Provision OK for domain DN DC=unlis,DC=local
Starting replication
Schema-DN[CN=Schema,CN=Configuration,DC=unlis,DC=local] objects[402/1550]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=unlis,DC=local] objects[804/1550]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=unlis,DC=local] objects[1206/1550]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=unlis,DC=local] objects[1550/1550]
linked_values[0/0]
Analyze and apply schema objects
Partition[CN=Configuration,DC=unlis,DC=local] objects[402/1616] linked_values[0/0]
Partition[CN=Configuration,DC=unlis,DC=local] objects[804/1616] linked_values[0/0]
Partition[CN=Configuration,DC=unlis,DC=local] objects[1206/1616] linked_values[0/0]
Partition[CN=Configuration,DC=unlis,DC=local] objects[1608/1616] linked_values[0/0]
Partition[CN=Configuration,DC=unlis,DC=local] objects[1616/1616] linked_values[28/0]
Replicating critical objects from the base DN of the domain
Partition[DC=unlis,DC=local] objects[98/98] linked_values[23/0]
Partition[DC=unlis,DC=local] objects[369/271] linked_values[23/0]
Done with always replicated NC (base, config, schema)
Replicating DC=DomainDnsZones,DC=unlis,DC=local
Partition[DC=DomainDnsZones,DC=unlis,DC=local] objects[42/42] linked_values[0/0]
Replicating DC=ForestDnsZones,DC=unlis,DC=local
Partition[DC=ForestDnsZones,DC=unlis,DC=local] objects[18/18] linked_values[0/0]
Committing SAM database
Sending DsReplicaUpdateRefs for all the replicated partitions
Setting isSynchronized and dsServiceName
Setting up secrets database
See /var/lib/samba/private/named.conf for an example configuration include file for
BIND
and /var/lib/samba/private/named.txt for further documentation required for secure DNS
updates
Joined domain UNLIS (SID S-1-5-21-684804980-2631616034-4274127141) as a DC
```

Сразу же дописываем в файл ***/etc/samba/smb.conf*** в секцию *[global]* строку:

```
idmap_ldb:use rfc2307 = yes
```

Обязательно шаманим **bind9**, как в прошлой статье:

Узнаем версию **bind9** командой ***named -v***. Дописываем в конец файла ***/etc/bind/named.conf***

```
include "/var/lib/samba/private/named.conf";
```

Дописываем в конец файла ***/etc/bind/named.conf.options*** *после символа };*

```
tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
```

И в файле ***/var/lib/samba/private/named.conf*** комментируем/раскомментируем строку под нашу версию bind (в данном случае 9.9)

```
dlz "AD DNS Zone" {
# For BIND 9.8.x
# database "dlopen /usr/lib/i386-linux-gnu/samba/bind9/dlz_bind9.so";

# For BIND 9.9.x
database "dlopen /usr/lib/i386-linux-gnu/samba/bind9/dlz_bind9_9.so";

# For BIND 9.10.x
# database "dlopen /usr/lib/i386-linux-gnu/samba/bind9/dlz_bind9_10.so";
};
```

На основном контроллере домена файлы ***/etc/resolv.conf*** и ***/etc/network/interfaces*** изменяем так же, как мы делали это на резервном (см. выше).

Настройка NTP ничем не отличается от настройки на основном контроллере. Конфигурация /**etc**/**ntp.conf** та же

```
# Local clock (Note: This is not the localhost address!)
server 127.127.1.0
fudge 127.127.1.0 stratum 10

# The source, where we are receiving the time from
server 0.pool.ntp.org iburst prefer

driftfile /var/lib/ntp/ntp.drift
logfile /var/log/ntp
ntpsigndsocket /var/lib/samba//ntp_signd/

# Access control
# Default restriction: Only allow querying time (incl. ms-sntp) from this machine
restrict default kod nomodify notrap nopeer mssntp
```

```
# Allow everything from localhost
restrict 127.0.0.1

# Allow that our time source can only provide time and do nothing else
restrict 0.pool.ntp.org mask 255.255.255.255 nomodify notrap nopeer noquery
```

В любом случае время (и часовой пояс соответственно) на обоих контроллерах должно быть одинаковым, иначе не работает Kerberos.

> *Теперь у меня две коровы © Матроскин*

Все бы ничего, но как говорится "Это Linux, детка". Поэтому достаем напильники и бубны и читаем про **третий пункт**.

Дело в том, что если бы мы поднимали домен на МастДай Server 2k3/8/12, то при добавлении резервного контроллера домена автоматически создались бы DNS-записи в зонах прямого просмотра *unlis.local* и *_msdcs.unlis.local* о нашем резервном контроллере. При использовании Samba эти записи не создаются, и их придется добавить вручную...

Тут у нас есть два путя: настроить все через консоль, либо добавить записи с клиентской машины Windows 7 при помощи утилиты удаленного администрирования сервера. Я сделаю так: добавлю записи через консоль, а потом посмотрю утилитой из-под Windows, что получилось.

Подключаемся к первичному DC и добавляем запись A в зону прямого просмотра *unlis.local*:

```
root@pdc:~# samba-tool dns add 192.168.1.2 unlis.local bdc A 192.168.1.3
-UAdministrator
Password for [UNLIS\Administrator]:
Record added successfully
```

Проверяем:

```
root@pdc:~# nslookup
> bdc
Server: 192.168.1.2
Address: 192.168.1.2#53

Name: bdc.unlis.local
Address: 192.168.1.3
```

Далее необходимо узнать **objectGUID** нашего резервного DC и добавить соответствующую запись в зону *_msdcs.unlis.local*, чтобы другие члены сети могли с ним работать (эта зона используется для публикации сайтов и служб Active Directory, без записей в этой зоне не будет работать репликация). Выполним поиск по файлу **/var/lib/samba/private/sam.ldb** (если ругается на ***ldbsearch*** - ставим пакет **ldb-tools**):

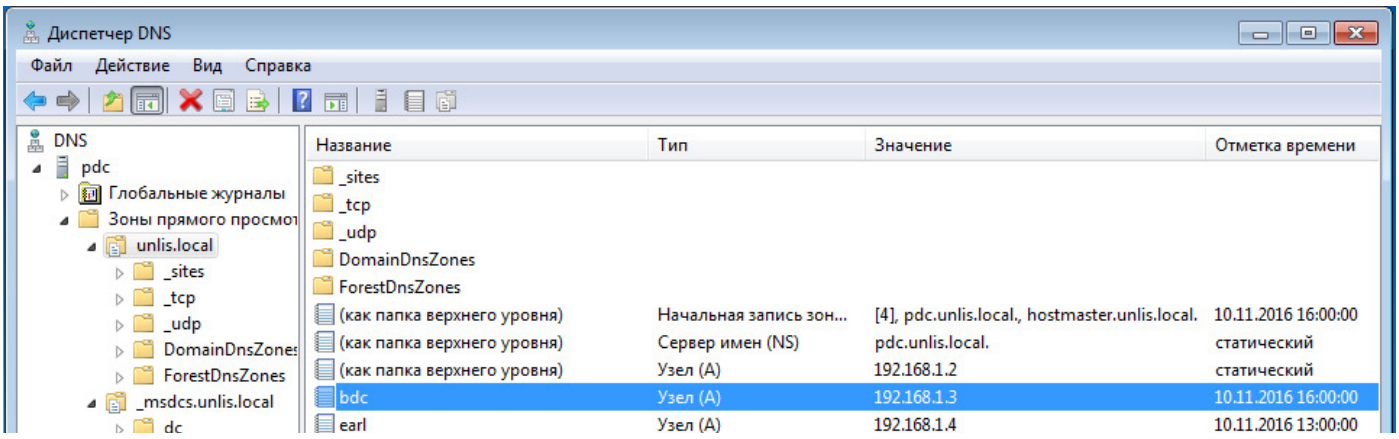
```
root@pdc:~# ldbsearch -H /var/lib/samba/private/sam.ldb '(invocationid=*)' --cross-ncs
```

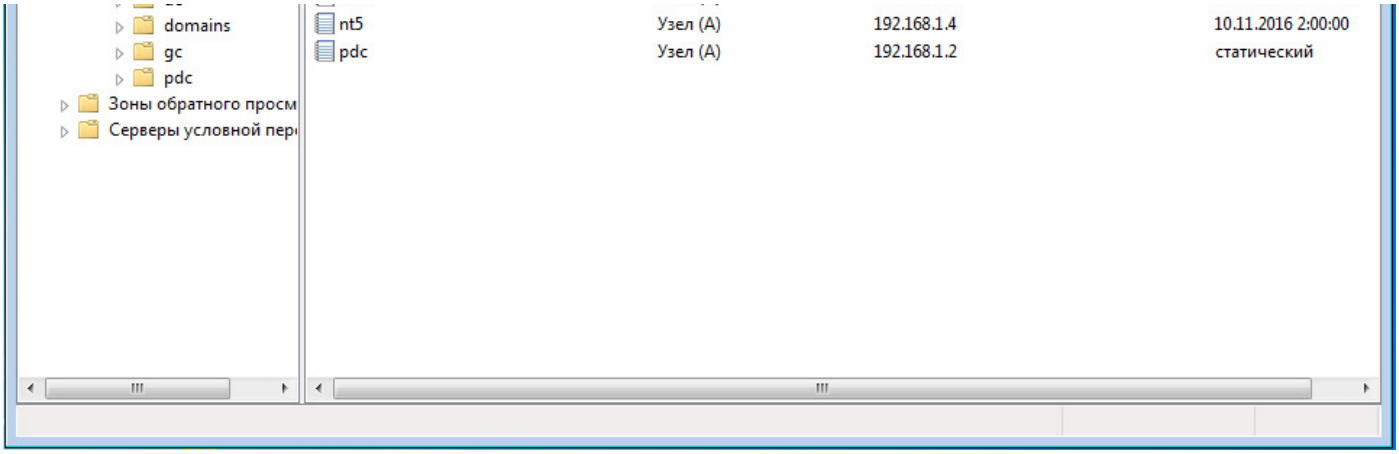
```
objectguid
# record 1
dn: CN=NTDS Settings,CN=BDC,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=unlis,DC=local
objectGUID: 37835335-23ef-491e-a19a-57b00ddf456d

# record 2
dn: CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=unlis,DC=local
objectGUID: 8f44a672-e080-4b1c-bfea-88d5219cc577

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

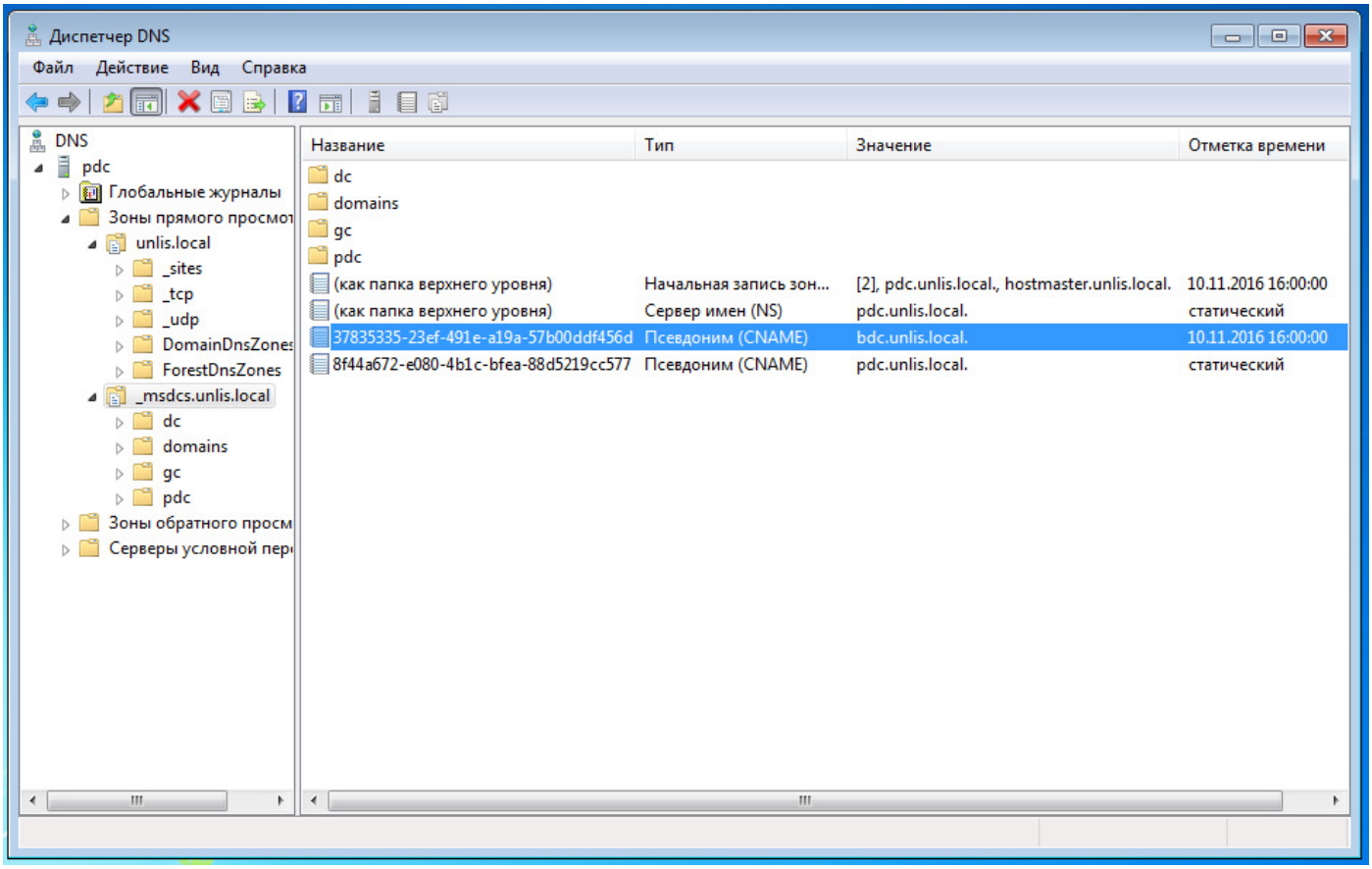
Как видим, нашему BDC при вводе в домен был присвоен **objectGUID** *37835335-23ef-491e-a19a-57b00ddf456d* . Добавляем CNAME запись в зону **_msdcs.unlis.loca**l и сразу же тестируем:

```
root@pdc:~# samba-tool dns add 192.168.1.2 _msdcs.unlis.local 37835335-23ef-491e-a19a-
57b00ddf456d CNAME bdc.unlis.local -UAdministrator
Password for [UNLIS\Administrator]:
Record added successfully

root@pdc:~# nslookup
> 37835335-23ef-491e-a19a-57b00ddf456d._msdcs.unlis.local
Server: 192.168.1.2
Address: 192.168.1.2#53

37835335-23ef-491e-a19a-57b00ddf456d._msdcs.unlis.local canonical name =
bdc.unlis.local.
Name: bdc.unlis.local
Address: 192.168.1.3
```

Запись есть, и это означает, что вторичный доменный контроллер добавлен в DNS правильно, и теперь с ним можно работать как с полноценным участником сети. Посмотрим под виндой:







Перезапускаем samba, а лучше весь резервный контроллер. Через несколько минут после перезапуска автоматически установится соединение между контроллерами домена и начнется репликация. Для проверки репликации выполним на резервном контроллере команду ***samba-tool drs showrepl***

```
root@bdc:~# samba-tool drs showrepl
Default-First-Site-Name\BDC
DSA Options: 0x00000001
DSA object GUID: 37835335-23ef-491e-a19a-57b00ddf456d
DSA invocationId: b575be91-9526-4c00-8c8c-a73e55abcdb6

==== INBOUND NEIGHBORS ====

DC=DomainDnsZones,DC=unlis,DC=local
Default-First-Site-Name\PDC via RPC
```

```
DSA object GUID: 8f44a672-e080-4b1c-bfea-88d5219cc577
Last attempt @ Thu Nov 10 17:30:34 2016 MSK was successful
0 consecutive failure(s).
Last success @ Thu Nov 10 17:30:34 2016 MSK

<...>
==== OUTBOUND NEIGHBORS ====

DC=ForestDnsZones,DC=unlis,DC=local
Default-First-Site-Name\PDC via RPC
DSA object GUID: 8f44a672-e080-4b1c-bfea-88d5219cc577
Last attempt @ NTTIME(0) was successful
0 consecutive failure(s).
Last success @ NTTIME(0)

==== KCC CONNECTION OBJECTS ====

Connection --
Connection name: 5a576470-40eb-4fcb-9835-9013d316c1f6
Enabled : TRUE
Server DNS name : pdc.unlis.local
Server DN name : CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Ciguration,DC=unlis,DC=local
TransportType: RPC
options: 0x00000001
Warning: No NC replicated for Connection
```

Последний warning не опасен и может быть проигнорирован. Для более детальной проверки репликации можно воспользоваться утилитой samba-tool ldapcmp.

Четвертым номером нашей программы будет настройка репликации системного каталога SYSVOL.

Папка SYSVOL содержит групповые политики и другие важные данные для работы домена. Важно, чтобы содержимое папки было одинаковым и одновременно изменялось на всех контроллерах домена. Отсутствие репликации приводит к неправильной работе групповых политик, сценариев входа и т. д. В ОС типа МастДай существует сервис **FRS** (**DFS-R** в w2k8 и выше), реплицирующий содержимое папки SYSVOL на всех контроллерах домена. Samba пока не поддерживает репликацию SYSVOL через DFS-R или FRS, поэтому приходится забивать костыли....

Существует два путя: однонаправленная репликация (например, с основного контроллера домена на все резервные) и двунаправленная. Если выбрать однонаправленную - считай пропало, а если двунаправленную - то тогда у нас два путя будет.

А теперь серьезно. Любая репликация осуществляется с помощью **Rsync** и периодически запускается с помощью **Cron**. Однонаправленную, естественно, проще настраивать, файлы могут быть переданы только в

одном направлении. Поэтому необходимо выбрать один DC, на котором делаются все модификации (правки GPO, изменения сценариев входа и т.д.), на все другие DC изменения будут перезаписаны при синхронизации. Двунаправленная также использует **Rsync**, но, в отличие от однонаправленной, дополнительно используется **osync** либо **Unsion** (вот они, два путя), все это тяжелее настраивать.

Как вы и догадались, легких путей мы не ищем, поэтому настроим двунаправленную синхронизацию с помощью **Rsync** и **Unison**. Итак, сначала установим Rsync и Unison на контроллер домена с FSMO ролью эмулятора PDC (надеюсь все знают, что это и кто это). Можно ставить из исходников, но мы поставим из пакетов:

```
root@pdc:~# apt-get install rsync unison
```

Далее приступим к генерации и распространению ключей SSH. Сгенерируем RSA-ключ с помощью команды ***ssh-keygen -t rsa:***

```
root@pdc:~# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): <Оставляем_путь_как_есть>
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase): <Пароль_должен_быть_пустой!>
Enter same passphrase again: <Пароль_должен_быть_пустой!>
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
8b:37:08:fd:aa:f2:89:d4:25:27:c0:c2:47:aa:2e:71 root@pdc
The key's randomart image is:
+---[RSA 2048]----+
| . |
|..o |
|.oo. |
|.... . |
|o E + + S |
|.o . * + . |
|... . o = |
|.... . o . |
| .o+.. |
+-----------------+
```

Скопируем полученный публичный ключ на bdc:

```
root@pdc:~# ssh-copy-id -i ~/.ssh/id_rsa.pub root@bdc
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any
that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now
```

```
it is to install the new keys
root@bdc's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@bdc'"
and check to make sure that only the key(s) you wanted were added.
```

Если при вводе пароля ругается на Permission denied, измените в файле ***/etc/ssh/sshd_config*** на сервере bdc *PermitRootLogin without-password* на *PermitRootLogin yes* и перезапустите демон ssh

Теперь можно подключиться к bdc посредством ssh. Выполним команду ***ssh bdc*** - авторизация должна пройти по только что скопированному публичному ключу.

Создаем файл ***/root/.ssh/ctl/config*** с содержанием:

```
Host *
ControlMaster auto
ControlPath ~/.ssh/ctl/%h_%p_%r
ControlPersist 1
```

Далее настроим сохранение логов:

```
root@pdc:~# touch /var/log/sysvol-sync.log
root@pdc:~# chmod 640 /var/log/sysvol-sync.log
```

Настраиваем **Unison**. Выполним команду ***install -o root -g root -m 0750 -d /root/.unison***. Создадим файл ***/root/.unison/default.prf*** и напишем туда:

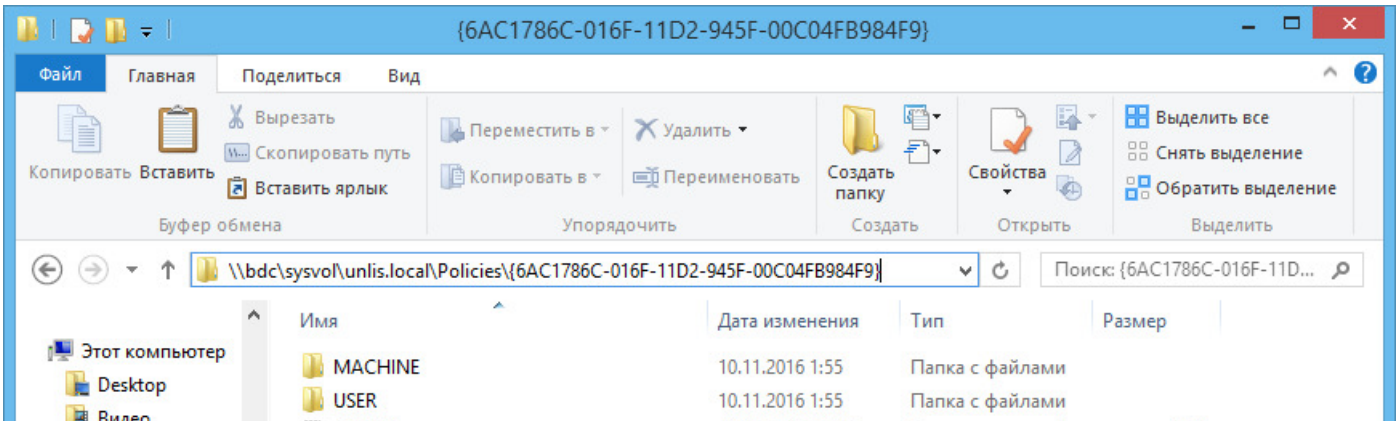
```
# Unison preferences file
# Roots of the synchronization
#
# copymax & maxthreads params were set to 1 for easier troubleshooting.
# Have to experiment to see if they can be increased again.
root = /var/lib/samba
# Note that 2 x / behind DC2, it is required
root = ssh://root@bdc//var/lib/samba
#
# Paths to synchronize
path = sysvol
#
#ignore = Path stats ## ignores /var/www/stats
auto=true
batch=true
perms=0
```

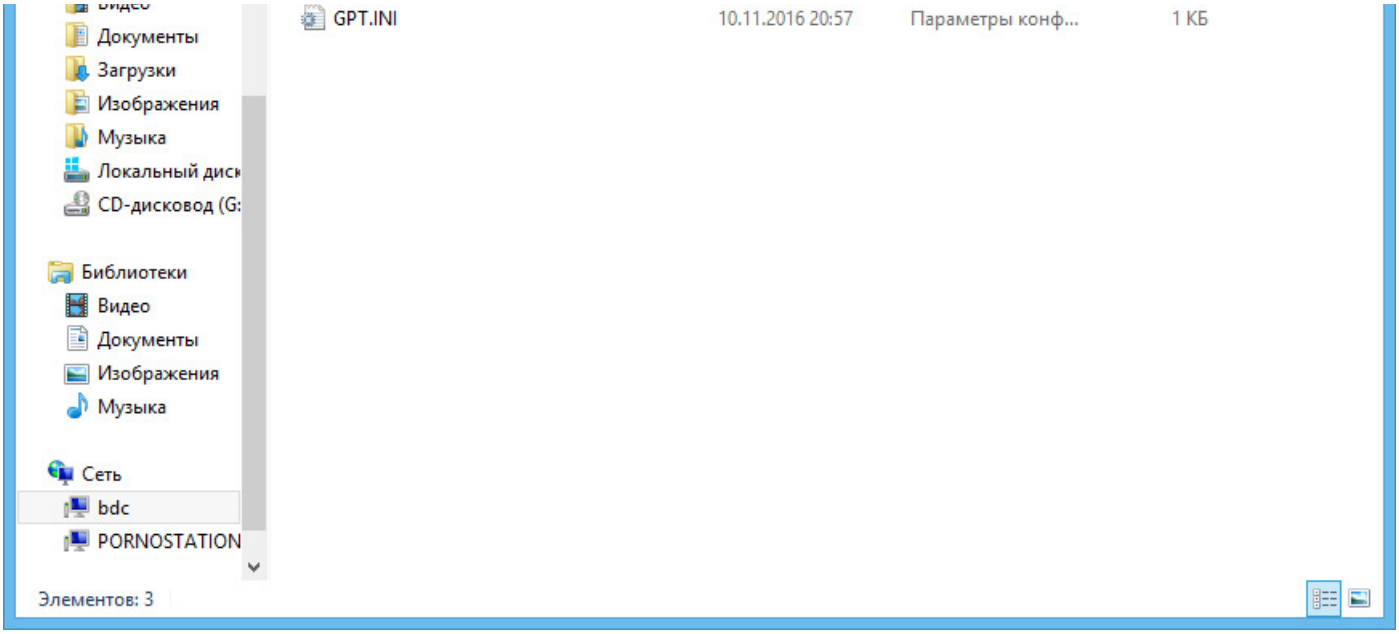
```
rsync=true
maxthreads=1
retry=3
confirmbigdeletes=false
servercmd=/usr/bin/unison
copythreshold=0
copyprog = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --inplace --compress
copyprogrest = /usr/bin/rsync -XAavz --rsh='ssh -p 22' --partial --inplace --compress
copyquoterem = true
copymax = 1
logfile = /var/log/sysvol-sync.log
```

На резервном контроллере также ставим **rsync** и **unison** (настраивать ничего не надо). После установки выполняем на первичном контроллере команду:

```
root@pdc:~# /usr/bin/rsync -XAavz --log-file /var/log/sysvol-sync.log --delete-after
-f"+ */" -f"- *" /var/lib/samba/sysvol root@bdc:/var/lib/samba && /usr/bin/unison &>
/dev/null
building file list ... done
sysvol/
sysvol/unlis.local/
sysvol/unlis.local/Policies/
sysvol/unlis.local/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/
sysvol/unlis.local/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/
sysvol/unlis.local/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/USER/
sysvol/unlis.local/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/
sysvol/unlis.local/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/
sysvol/unlis.local/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/USER/
sysvol/unlis.local/scripts/

sent 5,193 bytes received 65 bytes 10,516.00 bytes/sec
total size is 0 speedup is 0.00
```

Судя по выводу, что-то скопировалось. Можно зайти на \\bdc\SYSVOL и посмотреть.





Как видим, каталог SYSVOL ~~скопировался~~ синхронизировался.

Вручную все работает, теперь настраиваем периодический запуск синхронизации с помощью **Cron**. С ***crontab -e*** оно у меня что-то не заработало (потом я понял почему, но было уже поздно), поэтому создаем файл ***/etc/cron.d/sysvol*** (имя может быть любое) и пишем туда следующее:

```
*/5 * * * * root /usr/bin/rsync -XAavz --log-file /var/log/sysvol-sync.log
--delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol root@bdc:/var/lib/samba/ &&
/usr/bin/unison &> /dev/null
```

То есть создаем задачу для синхронизации, которая будет запускаться каждые пять минут, смотреть изменения в каталогах и реплицировать их, если обнаружатся различия.

Можно для проверки установить периодичность запуска раз в минуту, затем командой ***cat /var/log/syslog | grep CRON*** посмотреть запускается ли задача вообще:

```
root@pdc:~# cat /var/log/syslog | grep CRON
<...>
Nov 12 01:39:01 pdc CRON[1505]: (root) CMD (/usr/bin/rsync -XAavz --log-file /var/log
/sysvol-sync.log --delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol root@bdc:/var
/lib/samba/ && /usr/bin/unison &> /dev/null)
Nov 12 01:40:01 pdc CRON[1512]: (root) CMD (/usr/bin/rsync -XAavz --log-file /var/log
/sysvol-sync.log --delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol root@bdc:/var
/lib/samba/ && /usr/bin/unison &> /dev/null)
Nov 12 01:41:01 pdc CRON[1519]: (root) CMD (/usr/bin/rsync -XAavz --log-file /var/log
/sysvol-sync.log --delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol root@bdc:/var
/lib/samba/ && /usr/bin/unison &> /dev/null)
Nov 12 01:42:01 pdc CRON[1534]: (root) CMD (/usr/bin/rsync -XAavz --log-file /var/log
/sysvol-sync.log --delete-after -f"+ */" -f"- *" /var/lib/samba/sysvol root@bdc:/var
/lib/samba/ && /usr/bin/unison &> /dev/null)
```

Ну и конечно же, посмотрим логи в ***/var/log/sysvol-sync.log***, предварительно положив какой-нибудь новый файлик в каталог SYSVOL на один из серверов:

```
root@pdc:~# cat /var/log/sysvol-sync.log
2016/11/12 01:16:02 [1318] building file list
2016/11/12 01:16:02 [1318] done
2016/11/12 01:16:02 [1318] .d..t...... sysvol/unlis.local/scripts/
2016/11/12 01:16:02 [1318] sent 1,218 bytes received 14 bytes 821.33 bytes/sec
2016/11/12 01:16:02 [1318] total size is 0 speedup is 0.00
UNISON 2.40.102 started propagating changes at 01:16:02.29 on 12 Nov 2016
[BGN] Copying sysvol/unlis.local/scripts/logon.bat from //bdc//var/lib/samba to
/var/lib/samba
/usr/bin/rsync -XAavz --rsh='ssh -p 22' --inplace --compress 'root@bdc:'\''/var
/lib/samba/sysvol/unlis.local/scripts/logon.bat'\''' '/var/lib/samba/sysvol/unlis.local
/scripts/.unison.logon.bat.9afeb99c6c74c1f5e896a5c951212192.unison.tmp'
[END] Copying sysvol/unlis.local/scripts/logon.bat
UNISON 2.40.102 finished propagating changes at 01:16:02.53 on 12 Nov 2016
Synchronization complete at 01:16:02 (1 item transferred, 0 skipped, 0 failed)
2016/11/12 01:17:02 [1336] building file list
2016/11/12 01:17:02 [1336] done
2016/11/12 01:17:02 [1336] .d..t...... sysvol/unlis.local/scripts/
2016/11/12 01:17:02 [1336] sent 1,218 bytes received 14 bytes 2,464.00 bytes/sec
2016/11/12 01:17:02 [1336] total size is 0 speedup is 0.00
```

Из логов видно, что файл ***sysvol/unlis.local/scripts/logon.bat*** скопирован с резервного контроллера домена на основной. Кто не верит - заходим на сервер и смотрим. Ну и конечно же нужно поиграться - создать на PDC в каталоге SYSVOL файл, дождаться синхронизации, обнаружить его в том же месте на BDC, затем удалить его с BDC, опять дождаться синхронизации и не найти его на том месте, где мы его создавали. Если все так - заначит It Works!

Если надо ресинхронизировать SYSVOL, то стоит сделать следующее:

1. Запретить задачу в **Cron** на первичном контроллере
2. Убедиться в том, что **Rsync** или **Unison** в данный момент не выполняется
3. Удалить хэш-файлы на обоих контроллерах домена в каталогах ***/root/.unison***
4. Проверить SYSVOL и пересинхронизироваться вручную
5. Убедиться в том, что все ок
6. Разрешить задачу **Cron** на первичном контроллере

А еще нам надо настроить общие сетевые ресурсы и сделать так, чтобы пользователи домена воспринимались ОС как локальные. Читаем статью Настройка прав доступа к общим ресурсам сервера Samba AD DC

← Предыдущая запись Следующая запись →

2 Комментарии

Вячеслав 28.11.2016 в 01:05

Спасибо за статью, все взлетело! Но при подключении через виндовую mmc-dns предлагает выбрась сервер к тороромy подключится, а после пишет "Access was denied.Would you like add it anyway".Куда копать?

ub4acj (Автор записи) 28.11.2016 в 02:37

К резервному контроллеру хотите подключиться или к основному? Обычно он неавторизованных пользователей так шлет, либо нет соответствующих прав (насколько я помню пользователь должен быть членом DNSADMINS)