Samba - Domena AD

Wstęp

PDC - Primary Domain Controler

SDC - Secondary Domain Controler

PC - komputer

Na PDC/SDC instalujemy Debiana - minimalna/czysta instalacja + serwer OpenSSH. Na PC instalujemy wersję Windowsa Pro - w moim przykładzie wykorzystałem wersję 10 21H2.

Instalacja PDC

I instalujemy pakiety:

```
apt install samba samba-client winbind krb5-user ldb-tools acl net-tools
rsync nfs-kernel-server ntp
```

Podczas instalacji zostaniemy zapytanie o Realm dla Kerberosa - nie wpisujemy nic i zatwierdzamy enterem.

Konfiguracja PDC

Samba

Stopujemy proces Samby po instalacji oraz zachowujemy aktualny poinstalacyjny plik konfiguracji:

```
/etc/init.d/smbd stop
mv /etc/samba/smb.conf /etc/samba/smb.conf.original
```

Tworzymy domenę AD:

```
samba-tool domain provision --use-rfc2307 --interactive
```

Podczas wykonania powyższego polecenia zostaniemy zapytani o nazwę domeny, moja domena to: test-ad.lan. Zostaniemy też zapytani o serwer DNS - wybieramy domyślny czyli SAMBA_INTERNAL - umożliwi to nam zarządzanie DNSami przystawką DNS z poziomu Windowsa. DNS Forwarder to serwery DNS, które będą odpytywane dla wszystkiego do nie jest naszą domeną - czyli na potrzeby internetu.

Przykładowy log:

```
Realm:  test-ad.lan
Domain [test-ad]:
```

```
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [8.8.8.8]:
8.8.8.8
Administrator password:
Retype password:
INFO 2021-12-22 11:36:41,699 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2122: Looking up IPv4 addresses
INFO 2021-12-22 11:36:41,699 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2139: Looking up IPv6 addresses
WARNING 2021-12-22 11:36:41,700 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2146: No IPv6 address will be assigned
INFO 2021-12-22 11:36:41,992 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2290: Setting up share.ldb
INFO 2021-12-22 11:36:42,339 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2294: Setting up secrets.ldb
INFO 2021-12-22 11:36:42,518 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2299: Setting up the registry
INFO 2021-12-22 11:36:43,137 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2302: Setting up the privileges
database
INFO 2021-12-22 11:36:43,568 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2305: Setting up idmap db
INFO 2021-12-22 11:36:43,783 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2312: Setting up SAM db
INFO 2021-12-22 11:36:43,832 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #897: Setting up sam.ldb partitions and
settings
INFO 2021-12-22 11:36:43,833 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #909: Setting up sam.ldb rootDSE
INFO 2021-12-22 11:36:43,899 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1322: Pre-loading the Samba 4 and AD
schema
Unable to determine the DomainSID, can not enforce uniqueness constraint on
local domainSIDs

INFO 2021-12-22 11:36:43,984 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1400: Adding DomainDN: DC=test-
ad,DC=lan
INFO 2021-12-22 11:36:44,033 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1432: Adding configuration container
INFO 2021-12-22 11:36:44,152 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1447: Setting up sam.ldb schema
INFO 2021-12-22 11:36:47,137 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1465: Setting up sam.ldb configuration
data
INFO 2021-12-22 11:36:47,257 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1506: Setting up display specifiers
INFO 2021-12-22 11:36:49,112 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1514: Modifying display specifiers and
```

```
extended rights
INFO 2021-12-22 11:36:49,145 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1521: Adding users container
INFO 2021-12-22 11:36:49,147 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1527: Modifying users container
INFO 2021-12-22 11:36:49,148 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1530: Adding computers container
INFO 2021-12-22 11:36:49,149 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1536: Modifying computers container
INFO 2021-12-22 11:36:49,151 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1540: Setting up sam.ldb data
INFO 2021-12-22 11:36:49,273 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1570: Setting up well known security
principals
INFO 2021-12-22 11:36:49,326 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1584: Setting up sam.ldb users and
groups
INFO 2021-12-22 11:36:49,452 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1592: Setting up self join
Repacking database from v1 to v2 format (first record CN=ms-DS-Object-
Reference,CN=Schema,CN=Configuration,DC=test-ad,DC=lan)
Repack: re-packed 10000 records so far
Repacking database from v1 to v2 format (first record CN=trustedDomain-
Display,CN=412,CN=DisplaySpecifiers,CN=Configuration,DC=test-ad,DC=lan)
Repacking database from v1 to v2 format (first record CN=ab402345-
d3c3-455d-9ff7-40268a1099b6,CN=Operations,CN=DomainUpdates,CN=System,DC=test
-ad,DC=lan)
INFO 2021-12-22 11:36:50,778 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/sambadns.py #1143: Adding DNS accounts
INFO 2021-12-22 11:36:50,875 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/sambadns.py #1177: Creating
CN=MicrosoftDNS,CN=System,DC=test-ad,DC=lan
INFO 2021-12-22 11:36:50,892 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/sambadns.py #1190: Creating DomainDnsZones and
ForestDnsZones partitions
INFO 2021-12-22 11:36:50,980 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/sambadns.py #1195: Populating DomainDnsZones and
ForestDnsZones partitions
Repacking database from v1 to v2 format (first record DC=k.root-
servers.net,DC=RootDNSServers,CN=MicrosoftDNS,DC=DomainDnsZones,DC=test-
ad,DC=lan)
Repacking database from v1 to v2 format (first record
DC=_ldap._tcp.dc,DC=_msdcs.test-
ad.lan,CN=MicrosoftDNS,DC=ForestDnsZones,DC=test-ad,DC=lan)
INFO 2021-12-22 11:36:51,470 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2026: Setting up sam.ldb rootDSE
marking as synchronized
INFO 2021-12-22 11:36:51,491 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2031: Fixing provision GUIDs
INFO 2021-12-22 11:36:52,176 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2364: A Kerberos configuration
```

```
suitable for Samba AD has been generated at /var/lib/samba/private/krb5.conf
INFO 2021-12-22 11:36:52,176 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2366: Merge the contents of this file
with your system krb5.conf or replace it with this one. Do not create a
symlink!
INFO 2021-12-22 11:36:52,255 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2096: Setting up fake yp server
settings
INFO 2021-12-22 11:36:52,394 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #489: Once the above files are
installed, your Samba AD server will be ready to use
INFO 2021-12-22 11:36:52,394 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #494: Server Role:           active
directory domain controller
INFO 2021-12-22 11:36:52,394 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #495: Hostname:              dc1
INFO 2021-12-22 11:36:52,394 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #496: NetBIOS Domain:        TEST-AD
INFO 2021-12-22 11:36:52,395 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #497: DNS Domain:            test-
ad.lan
INFO 2021-12-22 11:36:52,395 pid:3479 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #498: DOMAIN SID:
S-1-5-21-1844402430-801422403-354558641
```

Kopiujemy nadpisując plik /etc/krb5.conf:

```
cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Włączamy usługę:

```
systemctl stop smbd nmbd winbind
systemctl disable smbd nmbd winbind
systemctl unmask samba-ad-dc
systemctl start samba-ad-dc
systemctl enable samba-ad-dc
```

Sprawdzamy czy Samba się uruchomiła:

```
systemctl status samba-ad-dc
```

DNS

Modyfikujemy plik /etc/hosts:

```
127.0.0.1       dc1.test-ad.lan dc1
```

Gdzie dc1 to nazwa naszego serwera.

Edytujemy nasze DNSy w /etc/resolv.conf:

```
domain test-ad.lan
search test-ad.lan
nameserver 127.0.0.1
nameserver 8.8.8.8
```

NTP

Edytujemy /etc/ntp.conf (plik serwera czasu):

```
...
server wlasnyserverntp
...
ntpsigndsocket /var/lib/samba/ntp_signd/
...
restrict default kod nomodify notrap nopeer limited mssntp
...
```

Uprawnienia do katalogu oraz restart usługi:

```
chown root:ntp /var/lib/samba/ntp_signd/
chmod 750 /var/lib/samba/ntp_signd/
/etc/init.d/ntp restart
```

Udziały sieciowe

Pod koniec pliku /etc/samba/smb.conf dopisujemy:

```
[naszudzial]
        path = /path/to/udzial
        read only = No
```

Następnie na systemie plików ustawiamy domyślne uprawnienia:

```
chmod 775 /path/to/udzial
chown root:users /path/to/udzial
setfacl -m g:3000014:rwx /path/to/udzial
```

Gdzie 3000014 wskazuje na grupę Domain Admins, może być ona inna - przykład:

```
root@dc1:~# wbinfo -n "Domain Admins"
S-1-5-21-2989454373-3082771434-955187009-512 SID_DOM_GROUP (2)
root@dc1:~# wbinfo -Y S-1-5-21-2989454373-3082771434-955187009-512
3000014
```

Wszystkie grupy można wyświetlić za pomocą polecenia:

```
samba-tool group list
```

Generalnie przydatne polecenie w zarządzaniu Sambą to:

```
samba-tool
```

Konfiguracja PC

Aby móc zarządzać PDC z poziomu PC należy zainstalować narzędzia dla Windowsa Pro:

- Windows 10: https://www.microsoft.com/en-us/download/details.aspx?id=45520
- Windows 8.1: http://www.microsoft.com/en-us/download/details.aspx?id=39296
- Windows 8: http://www.microsoft.com/en-us/download/details.aspx?id=28972
- Windows 7: http://www.microsoft.com/en-us/download/details.aspx?id=7887
- Windows Vista: http://www.microsoft.com/en-us/download/details.aspx?id=21090

Aktualnie dla Windows 10 instalowanie narzędzi odbywa się z poziomu: Start → Ustawienia → Aplikacje → Funkcje opcjonalne i dodajemy wyszukując: active directory, zasadami grupy i DNS.

Podłączenie do domeny:

- w DNSach ustawiamy adres IP naszego PDC, w sufiks przeszukiwania ustawiamy test-ad.lan
- Start → Ustawienia → System → Informacje → Zaawansowane ustawienia systemu → Nazwa komputera → Zmień → Domena: test-ad.lan (poprosi nas o podanie uprawnień - wpisujemy: administrator oraz hasło, które ustaliliśmy przy tworzeniu domeny - może to też być inny użytkownik, którego stworzyliśmy i jest dodany do odpowiednich grup).

Po zrestartowaniu komputera domyślnie jest wybrany użytkownik lokalny, klikamy na Inny i wpisujemy nasz login i hasło do domeny. Poniżej pól tekstowych będzie napisane czy logujemy się do domeny (test-ad.lan) czy do komputera (PC123). Jak wpiszemy użytkownika takiego, który jest też lokalnie (np: administrator) to zmieni się miejsce logowania na komputer lokalny., aby wymusić logowanie na użytkownika domenowego należy login poprzedzić nazwą domeny, np: test-ad\administrator.

Po zalogowaniu należy sprawdzić czy czas jest synchronizowany z serwerem czasu domeny:

```
w32tm /monitor
```

Konfiguracja zapasowego kontrolera domeny (SDC)

Instalacja

Powtarzamy krok z instalacji PDC.

Samba

Stopujemy proces Samby oraz zachowujemy oryginalny plik konfiguracji:

```
/etc/init.d/smbd stop
mv /etc/samba/smb.conf /etc/samba/smb.conf.original
```

Kopiujemy plik z PDC /etc/krb5.conf, w naszym przypadku powinien on wyglądać tak:

```
[libdefaults]
        default_realm = TEST-AD.LAN
        dns_lookup_realm = false
        dns_lookup_kdc = true

[realms]
TEST-AD.LAN = {
        default_domain = test-ad.lan
}

[domain_realm]
        dc1 = TEST-AD.LAN
```

Ustawiamy serwer DNS wskazujący na PDC (lub tam gdzie skonfigurowaliśmy DNSy) w pliku /etc/resolv.conf:

```
domain test-ad.lan
search test-ad.lan
nameserver adresipPDC
nameserver 8.8.8.8
```

Sprawdzamy czy widać domenę w sieci:

```
root@dc2:~# kinit administrator
Password for administrator@TEST-AD.LAN:
Warning: Your password will expire in 41 days on wto, 21 mar 2021, 14:29:35
```

Dodajemy SDC do domeny:

```
root@dc2:~# samba-tool domain join test-ad.lan DC -U"TEST-AD\administrator"
--dns-backend=SAMBA_INTERNAL
INFO 2021-12-22 14:17:55,161 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #107: Finding a writeable DC for domain 'test-ad.lan'
INFO 2021-12-22 14:17:55,167 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #109: Found DC dc1.test-ad.lan
Password for [TEST-AD\administrator]:
INFO 2021-12-22 14:18:01,355 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1543: workgroup is TEST-AD
INFO 2021-12-22 14:18:01,356 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1546: realm is test-ad.lan
Adding CN=DC2,OU=Domain Controllers,DC=test-ad,DC=lan
Adding CN=DC2,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test-ad,DC=lan
Adding CN=NTDS Settings,CN=DC2,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test-ad,DC=lan
```

```
Adding SPNs to CN=DC2,OU=Domain Controllers,DC=test-ad,DC=lan
Setting account password for DC2$
Enabling account
Calling bare provision
INFO 2021-12-22 14:18:02,523 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2122: Looking up IPv4 addresses
INFO 2021-12-22 14:18:02,524 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2139: Looking up IPv6 addresses
WARNING 2021-12-22 14:18:02,524 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2146: No IPv6 address will be assigned
INFO 2021-12-22 14:18:02,798 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2290: Setting up share.ldb
INFO 2021-12-22 14:18:03,185 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2294: Setting up secrets.ldb
INFO 2021-12-22 14:18:03,280 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2299: Setting up the registry
INFO 2021-12-22 14:18:03,955 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2302: Setting up the privileges
database
INFO 2021-12-22 14:18:04,354 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2305: Setting up idmap db
INFO 2021-12-22 14:18:04,499 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2312: Setting up SAM db
INFO 2021-12-22 14:18:04,530 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #897: Setting up sam.ldb partitions and
settings
INFO 2021-12-22 14:18:04,531 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #909: Setting up sam.ldb rootDSE
INFO 2021-12-22 14:18:04,556 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #1322: Pre-loading the Samba 4 and AD
schema
Unable to determine the DomainSID, can not enforce uniqueness constraint on
local domainSIDs

INFO 2021-12-22 14:18:04,618 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2364: A Kerberos configuration
suitable for Samba AD has been generated at /var/lib/samba/private/krb5.conf
INFO 2021-12-22 14:18:04,618 pid:3401 /usr/lib/python3/dist-
packages/samba/provision/__init__.py #2366: Merge the contents of this file
with your system krb5.conf or replace it with this one. Do not create a
symlink!
Provision OK for domain DN DC=test-ad,DC=lan
Starting replication
Schema-DN[CN=Schema,CN=Configuration,DC=test-ad,DC=lan] objects[402/1739]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=test-ad,DC=lan] objects[804/1739]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=test-ad,DC=lan] objects[1206/1739]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=test-ad,DC=lan] objects[1608/1739]
linked_values[0/0]
```

```
Schema-DN[CN=Schema,CN=Configuration,DC=test-ad,DC=lan] objects[1739/1739]
linked_values[0/0]
Analyze and apply schema objects
Partition[CN=Configuration,DC=test-ad,DC=lan] objects[402/1624]
linked_values[0/1]
Partition[CN=Configuration,DC=test-ad,DC=lan] objects[804/1624]
linked_values[0/1]
Partition[CN=Configuration,DC=test-ad,DC=lan] objects[1206/1624]
linked_values[0/1]
Partition[CN=Configuration,DC=test-ad,DC=lan] objects[1608/1624]
linked_values[0/1]
Partition[CN=Configuration,DC=test-ad,DC=lan] objects[1624/1624]
linked_values[30/30]
Replicating critical objects from the base DN of the domain
Partition[DC=test-ad,DC=lan] objects[97/97] linked_values[23/23]
Partition[DC=test-ad,DC=lan] objects[274/274] linked_values[24/24]
Done with always replicated NC (base, config, schema)
Replicating DC=DomainDnsZones,DC=test-ad,DC=lan
Partition[DC=DomainDnsZones,DC=test-ad,DC=lan] objects[41/41]
linked_values[0/0]
Replicating DC=ForestDnsZones,DC=test-ad,DC=lan
Partition[DC=ForestDnsZones,DC=test-ad,DC=lan] objects[18/18]
linked_values[0/0]
Exop on[CN=RID Manager$,CN=System,DC=test-ad,DC=lan] objects[3]
linked_values[0]
Committing SAM database
Repacking database from v1 to v2 format (first record CN=ms-DS-Object-
Reference,CN=Schema,CN=Configuration,DC=test-ad,DC=lan)
Repack: re-packed 10000 records so far
Repacking database from v1 to v2 format (first record CN=trustedDomain-
Display,CN=412,CN=DisplaySpecifiers,CN=Configuration,DC=test-ad,DC=lan)
Repacking database from v1 to v2 format (first record
DC=DESKTOP-6HMOEBR,DC=test-ad.lan,CN=MicrosoftDNS,DC=DomainDnsZones,DC=test-
ad,DC=lan)
Repacking database from v1 to v2 format (first record
DC=_ldap._tcp.dc,DC=_msdcs.test-
ad.lan,CN=MicrosoftDNS,DC=ForestDnsZones,DC=test-ad,DC=lan)
Repacking database from v1 to v2 format (first record
CN=networks,CN=ypServ30,CN=RpcServices,CN=System,DC=test-ad,DC=lan)
INFO 2021-12-22 14:18:09,664 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1116: Adding 1 remote DNS records for DC2.test-
ad.lan
INFO 2021-12-22 14:18:09,690 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1179: Adding DNS A record DC2.test-ad.lan for IPv4
IP: 10.100.1.135
INFO 2021-12-22 14:18:09,828 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1207: Adding DNS CNAME record
8bd398ee-2314-45b9-941a-136ee7b81ea4._msdcs.test-ad.lan for DC2.test-ad.lan
INFO 2021-12-22 14:18:09,967 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1232: All other DNS records (like _ldap SRV records)
will be created samba_dnsupdate on first startup
```

```
INFO 2021-12-22 14:18:09,968 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1238: Replicating new DNS records in
DC=DomainDnsZones,DC=test-ad,DC=lan
Partition[DC=DomainDnsZones,DC=test-ad,DC=lan] objects[2/2]
linked_values[0/0]
INFO 2021-12-22 14:18:10,026 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1238: Replicating new DNS records in
DC=ForestDnsZones,DC=test-ad,DC=lan
Partition[DC=ForestDnsZones,DC=test-ad,DC=lan] objects[2/2]
linked_values[0/0]
INFO 2021-12-22 14:18:10,084 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1253: Sending DsReplicaUpdateRefs for all the
replicated partitions
INFO 2021-12-22 14:18:10,214 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1283: Setting isSynchronized and dsServiceName
INFO 2021-12-22 14:18:10,241 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1298: Setting up secrets database
INFO 2021-12-22 14:18:10,313 pid:3401 /usr/lib/python3/dist-
packages/samba/join.py #1560: Joined domain TEST-AD (SID
S-1-5-21-1844402430-801422403-354558641) as a DC
```

Robimy backup pliku na PDC:

```
tdbbackup -s .bak /var/lib/samba/private/idmap.ldb
```

i podmieniamy go na SDC.

Dodajemy w /etc/samba/smb.conf:

```
[global]
...
        dns forwarder = 8.8.8.8
...
```

Uruchamiamy:

```
systemctl stop smbd nmbd winbind
systemctl disable smbd nmbd winbind
systemctl unmask samba-ad-dc
systemctl start samba-ad-dc
systemctl enable samba-ad-dc
```

Synchronizacja sysvol

Na PDC dopisujemy do /etc/exports:

```
/var/lib/samba/sysvol adresIPSDC(ro,no_root_squash,subtree_check)
```

Oraz na PDC wykonujemy przeładowanie usługi NFS:

```
exportfs -a
/etc/init.d/nfs-kernel-server reload
```

Na SDC tworzymy katalog:

```
mkdir /mnt/dc1_sysvol
```

Na SDC dopisujemy do /etc/fstab zasób sieciowy NFS i montujemy:

```
echo "adresIPPDC:/var/lib/samba/sysvol /mnt/dc1_sysvol nfs defaults 0 0" >>
/etc/fstab
mount /mnt/dc1_sysvol
```

Na SDC synchronizujemy oba katalogi:

```
rsync -a /mnt/dc1_sysvol/ /root/test/
```

Resetujemy uprawnienia do sysvol:

```
samba-tool ntacl sysvolreset
```

Dopisujemy do crona synchronizację do pliku /etc/crontab:

```
echo "15 * * * *      root    rsync -a /mnt/dc1_sysvol/ /root/test/ &&
samba-tool ntacl sysvolreset" >> /etc/crontab
```

Przeładowujemy crona:

```
/etc/init.d/cron reload
```

DNS

Zmieniamy /etc/resolv.conf:

```
domain test-ad.lan
search test-ad.lan
nameserver 127.0.0.1
nameserver 8.8.8.8
```

NTP

Edytujemy /etc/ntp.conf (plik serwera czasu):

```
...
server wlasnyserverntp
...
ntpsigndsocket /var/lib/samba/ntp_signd/
```

```
...
restrict default kod nomodify notrap nopeer limited mssntp
...
```

Uprawnienia do katalogu oraz restart usługi:

```
chown root:ntp /var/lib/samba/ntp_signd/
chmod 750 /var/lib/samba/ntp_signd/
/etc/init.d/ntp restart
```

Sprawdzenie replikacji

Przykład:

```
root@sdc:/var/lib/samba/sysvol# samba-tool drs showrepl
Default-First-Site-Name\PDC2
DSA Options: 0x00000001
DSA object GUID: 468e9819-8b34-4fb7-85ab-34db6b83c789
DSA invocationId: 77cf0f4f-0557-4926-b973-e88e52d7ba13

==== INBOUND NEIGHBORS ====

CN=Configuration,DC=test-ad,DC=lan
        Default-First-Site-Name\PDC via RPC
                DSA object GUID: 17387053-8b0b-40dc-abe7-3fb9d936b5f1
                Last attempt @ Wed Feb  8 14:55:30 2017 CET was successful
                0 consecutive failure(s).
                Last success @ Wed Feb  8 14:55:30 2017 CET

DC=test-ad,DC=lan
        Default-First-Site-Name\PDC via RPC
                DSA object GUID: 17387053-8b0b-40dc-abe7-3fb9d936b5f1
                Last attempt @ Wed Feb  8 14:55:30 2017 CET was successful
                0 consecutive failure(s).
                Last success @ Wed Feb  8 14:55:30 2017 CET

CN=Schema,CN=Configuration,DC=test-ad,DC=lan
        Default-First-Site-Name\PDC via RPC
                DSA object GUID: 17387053-8b0b-40dc-abe7-3fb9d936b5f1
                Last attempt @ Wed Feb  8 14:55:30 2017 CET was successful
                0 consecutive failure(s).
                Last success @ Wed Feb  8 14:55:30 2017 CET

==== OUTBOUND NEIGHBORS ====

CN=Configuration,DC=test-ad,DC=lan
        Default-First-Site-Name\PDC via RPC
                DSA object GUID: 17387053-8b0b-40dc-abe7-3fb9d936b5f1
                Last attempt @ NTTIME(0) was successful
```

```
                0 consecutive failure(s).
                Last success @ NTTIME(0)

DC=test-ad,DC=lan
        Default-First-Site-Name\PDC via RPC
                DSA object GUID: 17387053-8b0b-40dc-abe7-3fb9d936b5f1
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

CN=Schema,CN=Configuration,DC=test-ad,DC=lan
        Default-First-Site-Name\PDC via RPC
                DSA object GUID: 17387053-8b0b-40dc-abe7-3fb9d936b5f1
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

==== KCC CONNECTION OBJECTS ====

Connection --
        Connection name: e82ab7ba-f605-4cd2-a838-e43cf687262c
        Enabled        : TRUE
        Server DNS name : pdc.test-ad.lan
        Server DN name  : CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=test-ad,DC=lan
                TransportType: RPC
                options: 0x00000001
Warning: No NC replicated for Connection!
```

Odłączenie PDC

Na nowym PDC:

```
samba-tool fsmo transfer --role=all
```

Na starym PDC:

```
samba-tool domain demote -Uadministrator
```

Group Policy

Ustawienia haseł

```
root@pdc:/var/log# samba-tool domain passwordsettings show
Password informations for domain 'DC=test-ad,DC=lan'

Password complexity: on
```

```
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
root@pdc:/var/log#
```

Problemy z delegowaniem GPO

Każde GPO musi mieć dodane Delegowanie dla uwierzytelnionych użytkowników do odczytu.

Polecenie do ręcznego uaktualnienia GPO na końcówce Windows:

```
gpupdate /force
```

Lista GPO dla komputera/użytkownika:

```
gpresult /R
```

Znane problemy

Problemy z podłączeniem się do serwera, aby móc przeglądać zasoby sieciowe

- Błąd: 0x80070035 - należy włączyć udostępnianie plików i drukarek w Panelu Sterowania → Centrum sieci i udostępniania → Zmień zaawansowane ustawienia udostępniania → Udostępnianie plików i drukarek: Włącz udostępnianie plików i drukarek. Jeśli nadal występuje to należy sprawdzić czy usługa: „Pomoc TCP/IP NetBIOS” jest włączona i Typ uruchomienia ma ustawiony na: Ręczny.
- Błąd: 0x80004005 - należy zezwolić na ruch wychodzący, wykonać: uruchomić gpedit.msc i ustawić opcje: Konfiguracja komputera → Ustawienia systemu Windows → Ustawienia zabezpieczeń → Zasady lokalne → Opcje zabezpieczeń → Zabezpieczenie sieciowe: Ograniczenie ruchu NTLM: Wychodzący ruch NTLM do serwerów zdalnych - ustawić na: Zezwalaj na cały ruch. Opcja w rejestrze: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0\RestrictSendingNTLMTraffic (REG_DWORD): 0.

Problemy z logowaniem się do udziałów sieciowych

Jeśli prosi nas system o hasło do zasobu sieciowego pomimo iż komputerem jesteśmy wpięci do domeny i poprawnie się zalogowaliśmy to możliwe iż ten problem powoduje VPN, którym się podpięliśmy do innej lokalizacji z poziomu właśnie tej stacji. Należy rozłączyć się z VPNem lub usunąć poświadczenia z poziomu Panelu Sterowania.

Problem z uprawnieniami udziału sieciowego - explorer crash

Przy tworzeniu katalogu pod udział sieciowy należy nadać jemu uprawnienia:

```
chmod 775 /path/to/share
chown root:users /path/to/share
```

Problem z uprawnieniami udziału sieciowego - brak zakładki

Jeśli nie widać zakładki z uprawnieniami udziału sieciowego w jego właściwościach to zapewne do serwera dostaliśmy się poprzez \\test-ad.lan - wystarczy wpisać po IP: \\1.2.3.4 lub po samej nazwie: \\dc1

Zmiana danych użytkownika

Służą do tego narzędzia takie jak:

```
ldbsearch
ldbedit
ldbrename
```

Najpierw wyszukujemy:

```
ldbrename -H /var/lib/samba/private/sam.ldb
'sAMAccountName=loginuzytkownika'
```

Edycja danych - uwaga, nie wszystkie dane da radę edytować i należy robić to z rozwagą!!!:

```
ldbedit -H /var/lib/samba/private/sam.ldb 'sAMAccountName=loginuzytkownika'
```

Zmiana nazwy użytkownika (imię i nazwisko):

```
ldbrename -H /var/lib/samba/private/sam.ldb "CN=User
Name,OU=Spedycja,DC=test-ad,DC=lan" "CN=NewUser NewName,OU=Spedycja,DC=test-
ad,DC=lan"
```

From:
https://kamil.orchia.pl/ - **kamil.orchia.pl**

Permanent link:
https://kamil.orchia.pl/doku.php?id=samba_-_domena_ad&rev=1643740645

Last update: **2022/02/01 19:37**