# Samba - Domena AD

## Wstęp

**PDC** - Primary Domain Controler

**PC** - komputer

Na PDC instalujemy Ubuntu serwer - minimalna/czysta instalacja + serwer OpenSSH. Na PC instalujemy wersję Windowsa Pro - w moim przykładzie wykorzystałem wersję 7.

## Instalacja PDC

Instalujemy program aptitude:

```
apt-get install aptitude
```

Uaktualniamy system:

```
aptitude upgrade
```

Wykonujemy reboot PDC i instalujemy Sambe i Binda:

```
aptitude install samba smbclient bind9 krb5-user winbind ldb-tools acl
```

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

## Konfiguracja PDC

### Samba

```
root@pdc:~# mv /etc/samba/smb.conf /etc/samba/smb.conf.original
root@pdc:~# samba-tool domain provision --use-rfc2307 --interactive
Realm: test-ad.lan
 Domain [test-ad]:
 Server Role (dc, member, standalone) [dc]:
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]: BIND9_FLATFILE
Administrator password:
Retype password:
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
Adding DomainDN: DC=test-ad,DC=lan
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=test-ad,DC=lan
rndc: connect failed: 127.0.0.1#953: connection refused
rndc: connect failed: 127.0.0.1#953: connection refused
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
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at
/var/lib/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              pdc
NetBIOS Domain:        TEST-AD
DNS Domain:            test-ad.lan
DOMAIN SID:            S-1-5-21-3956395406-4288503155-3671512556

root@pdc:~# rm /etc/krb5.conf
root@pdc:~# ln -s /var/lib/samba/private/krb5.conf /etc/krb5.conf
root@pdc:/var/log# /etc/init.d/samba-ad-dc restart
[ ok ] Restarting samba-ad-dc (via systemctl): samba-ad-dc.service.
```

**Bind**

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

```
/etc/bind/named.conf
```

Edytujemy plik /etc/apparmor.d/usr.sbin.named i dopisujemy do niego na samym końcu przed }:

```
  # Samba
  /var/lib/samba/private/named.conf r,
  /var/lib/samba/private/named.conf.update r,
  /var/lib/samba/private/dns/test-ad.lan.zone r,
```

I wykonujemy restart AppArmora i Binda:

```
/etc/init.d/apparmor reload
/etc/init.d/bind9 restart
```

Zmieniamy serwer DNS na lokalny.

### 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:

```
setfacl -m g:3000014:rwx /path/to/udzial
```

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

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

Wszystkie grupy mozna wyświetlić za pomocą polecenia:

```
samba-tool group list
```

### Autostart usługi

```
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
```

## 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

Podłączenie do domeny:

Panel sterowania → System → Zaawansowane ustawienia systemu → Nazwa komputera → Zmień → Domena: test-ad.lan, OK i restart komputera.

## Konfiguracja zapasowego PDC

### Instalacja

Powtarzamy krok z instalacji PDC.

### Samba

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
```

Ustawiamy serwer DNS wskazujący na PDC (lub tam gdzie skonfigurowaliśmy Binda). Sprawdzamy czy widać domenę w sieci:

```
root@pdc2:~# kinit administrator
Password for administrator@TEST-AD.LAN:
Warning: Your password will expire in 41 days on wto, 21 mar 2017, 14:29:35
```

Dodajemy PDC2 do domeny:

```
root@pdc2:~# mv /etc/samba/smb.conf /etc/samba/smb.conf.original
root@pdc2:~# samba-tool domain join test-ad.lan DC -U"TEST-AD\administrator"
--dns-backend=SAMBA_INTERNAL
Finding a writeable DC for domain 'test-ad.lan'
Found DC pdc.test-ad.lan
Password for [TEST-AD\administrator]:
NO DNS zone information found in source domain, not replicating DNS
workgroup is TEST-AD
```

```
realm is test-ad.lan
checking sAMAccountName
Adding CN=PDC2,OU=Domain Controllers,DC=test-ad,DC=lan
Adding CN=PDC2,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test-ad,DC=lan
Adding CN=NTDS Settings,CN=PDC2,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test-ad,DC=lan
Adding SPNs to CN=PDC2,OU=Domain Controllers,DC=test-ad,DC=lan
Setting account password for PDC2$
Enabling account
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=test-ad,DC=lan
Starting replication
Schema-DN[CN=Schema,CN=Configuration,DC=test-ad,DC=lan] objects[402/1550]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=test-ad,DC=lan] objects[804/1550]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=test-ad,DC=lan] objects[1206/1550]
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=test-ad,DC=lan] objects[1550/1550]
linked_values[0/0]
Analyze and apply schema objects
Partition[CN=Configuration,DC=test-ad,DC=lan] objects[402/1612]
linked_values[0/0]
Partition[CN=Configuration,DC=test-ad,DC=lan] objects[804/1612]
linked_values[0/0]
Partition[CN=Configuration,DC=test-ad,DC=lan] objects[1206/1612]
linked_values[0/0]
Partition[CN=Configuration,DC=test-ad,DC=lan] objects[1608/1612]
linked_values[0/0]
Partition[CN=Configuration,DC=test-ad,DC=lan] objects[1612/1612]
linked_values[20/0]
Replicating critical objects from the base DN of the domain
Partition[DC=test-ad,DC=lan] objects[98/98] linked_values[23/0]
Partition[DC=test-ad,DC=lan] objects[372/274] linked_values[23/0]
Done with always replicated NC (base, config, schema)
Committing SAM database
```

```
Sending DsReplicaUpdateRefs for all the replicated partitions
Setting isSynchronized and dsServiceName
Setting up secrets database
Joined domain TEST-AD (SID S-1-5-21-3956395406-4288503155-3671512556) as a
DC
root@pdc2:~#
```

Kopiujemy katalog /var/lib/samba/sysvol z PDC do PDC2 oraz robimy backup pliku na PDC:

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

i podmieniamy go na PDC2.

Resetujemy uprawnienia do katalogu /var/lib/samba/sysvol:

```
samba-tool ntacl sysvolreset
```

**Bind**

Na PDC szukamy wpisów PDC2:

```
root@pdc:~# ldbsearch -H /var/lib/samba/private/sam.ldb '(invocationId=*)' -
-cross-ncs objectguid
# record 1
dn: CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test-ad,DC=lan
objectGUID: 17387053-8b0b-40dc-abe7-3fb9d936b5f1

# record 2
dn: CN=NTDS Settings,CN=PDC2,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test-ad,DC=lan
objectGUID: 468e9819-8b34-4fb7-85ab-34db6b83c789

# returned 2 records
# 2 entries
# 0 referrals
root@pdc:~#
```

Zapamiętujemy objectGUID rekordu drugiego.

Na PDC edytujemy plik /var/lib/samba/private/dns/test-ad.lan.zone i dodajemy na końcu linie:

```
pdc2        IN A    1.2.3.4 ;IP PDC2
468e9819-8b34-4fb7-85ab-34db6b83c789._msdcs CNAME pdc2
```

oraz na początku pliku zmieniamy serial. Plik zapisujemy oraz restartujemy Binda:

```
/etc/init.d/bind9 restart
```

Sprawdzamy czy poprawnie są rozwiązywane nazwy:

```
root@pdc:~# host -t CNAME 17387053-8b0b-40dc-abe7-3fb9d936b5f1._msdcs.test-ad.lan.
17387053-8b0b-40dc-abe7-3fb9d936b5f1._msdcs.test-ad.lan is an alias for pdc.test-ad.lan.
root@pdc:~# host -t CNAME 468e9819-8b34-4fb7-85ab-34db6b83c789._msdcs.test-ad.lan.
468e9819-8b34-4fb7-85ab-34db6b83c789._msdcs.test-ad.lan is an alias for pdc2.test-ad.lan.
root@pdc:~# host -t A pdc2.test-ad.lan.
pdc2.test-ad.lan has address 1.2.3.4
```

**Samba uruchomienie i sprawdzenie**

Uruchomienia:

```
/etc/init.d/samba-ad-dc start
```

Replikacja:

```
root@pdc2:/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 /froce
```

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
```