Robert Sander <r.sander@heinlein-support.de>

Samba Active Directory

Windows 10 barrierefrei im LAN

- **Heinlein Support**
  - IT-Consulting und 24/7 Linux-Support mit ~28 Mitarbeitern
  - Eigener Betrieb eines ISPs seit 1992
  - Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen

- 24/7-Notfall-Hotline: 030 / 40 50 5 - 110
  - Spezialisten mit LPIC-2 und LPIC-3
  - Für alles rund um Linux & Server & Netzwerk
  - Akutes: Downtimes, Performanceprobleme, Hackereinbrüche, Datenverlust
  - Strategisches: Revision, Planung, Beratung, Konfigurationshilfe

Teil 1:
Theorie

Samba

- 1992: 1.0, 1999: 2.0, 2003: 3.0, 2012: 4.0, 2015: 4.3, 2016: 4.5
- Windows NT4 Domain PDC („3er-Modus“)
  - separates OpenLDAP-Backend
  - Fileshares
- Active Directory Domain Controller seit 4.0
  - eingebauter Verzeichnisdienst
  - eingebauter DNS-Server
  - Kerberos
  - Fileshares
- Seit 4.3 SMB 3.1.1, seit 4.5 NTLMv1 abgeschaltet

Linux

- OpenLDAP für PAM und NSS
- nslcd
  - libpam-ldapd
  - libnss-ldapd
- Alle Account-Informationen im LDAP-Verzeichnis
- ldapvi
- phpLDAPadmin
- LDAP Account Manager
- Apache Directory Studio

Samba NT4 PDC
OpenLDAP Backend mit smbldap-tools

- Ubuntu 16.04
- https://help.ubuntu.com/lts/serverguide/samba-ldap.html
- smbldap-adduser etc.

- DNS Forward und Reverse Zonen auf anderem Server
- DHCP auf anderem Server

- Home-Verzeichnisse
- Roaming Profiles
- Windows 7 Client mit Registry Patch

Classic Upgrade Vorbereitung

- Gute Beschreibung im Samba Wiki
  - https://wiki.samba.org/index.php/Migrating_a_Samba_NT4_Domain_to_Samba_AD_(Classic_Upgrade)
- In-Place oder auf neuem Server möglich
  - Wenn noch Samba 3 (???) installiert ist, besser auf neuem Server
- Der neue AD DC sollte keine Fileserver-Aufgaben haben
  - Shares und Daten ggfs vorher auf separaten Server migrieren
  - Oder AD DC auf neuem Server aufsetzen

Classic Upgrade Vorbereitung

- Active Directory Domain-Name festlegen
  - (Sub-)Domain einer eigenen DNS-Domain: ad.example.org
  - Nicht example.local oder example.intern o.ä. verwenden!
- Server-Name festlegen
  - AD DC lässt sich praktisch nicht umbenennen
- Benutzernamen und Gruppennamen eindeutig
  - Debian legt Gruppe = Benutzername an → vorher Gruppenname ändern
- Doppelte SIDs machen Probleme
- Domain Admin muß die Windows RID -500 haben

Classic Upgrade
Migration auf AD

- Samba-Services stoppen
- Datenbanken verschieben und aufräumen
- samba-tool domain classicupgrade
- Konfiguration anpassen
- OpenLDAP stoppen
- Samba im AD-Modus starten

- oder Provisionierung neue Domain:
  - samba-tool domain provision

Classic Upgrade Nachbereitung

- Winbind einrichten
- Kerberos einrichten
- OpenLDAP deinstallieren
- LDAP-Attribute migrieren
  - Nur die wichtigsten durch classicupgrade im AD
  - Weitere (z.B. mail, telephoneNumber) durch eigenes Script
- Gruppen prüfen
  - Nur Gruppen mit NT-Groupmapping werden übernommen

Nachbereitung Konfiguration

- dns forwarder = 10.24.4.1
  - nur eine IP möglich :(
- allow dns updates = nonsecure
  - Bug in Samba 4.3
- ldap server require strong auth = no
  - für ldapvi -h ldap://localhost ;)
- winbind enum users = yes
- winbind enum groups = yes
- winbind use default domain = yes

Was noch?

- samba-tool
  - CLI für Samba AD (Accounts, DNS, etc.)
- Zweiter AD Domain Controller sinnvoll
  - Redundanz für Verzeichnis und DNS
- Aber: keine eingebaute SysVol-Replikation
  - rsync von /var/lib/samba/sysvol
  - Primärer DC schreibt Group Policies und Netlogon-Skripte
- DNS
  - Keine automatische Abhängigkeit von A zu PTR möglich
  - CNAME nur innerhalb der AD-DNS-Domain

Windows-Clients

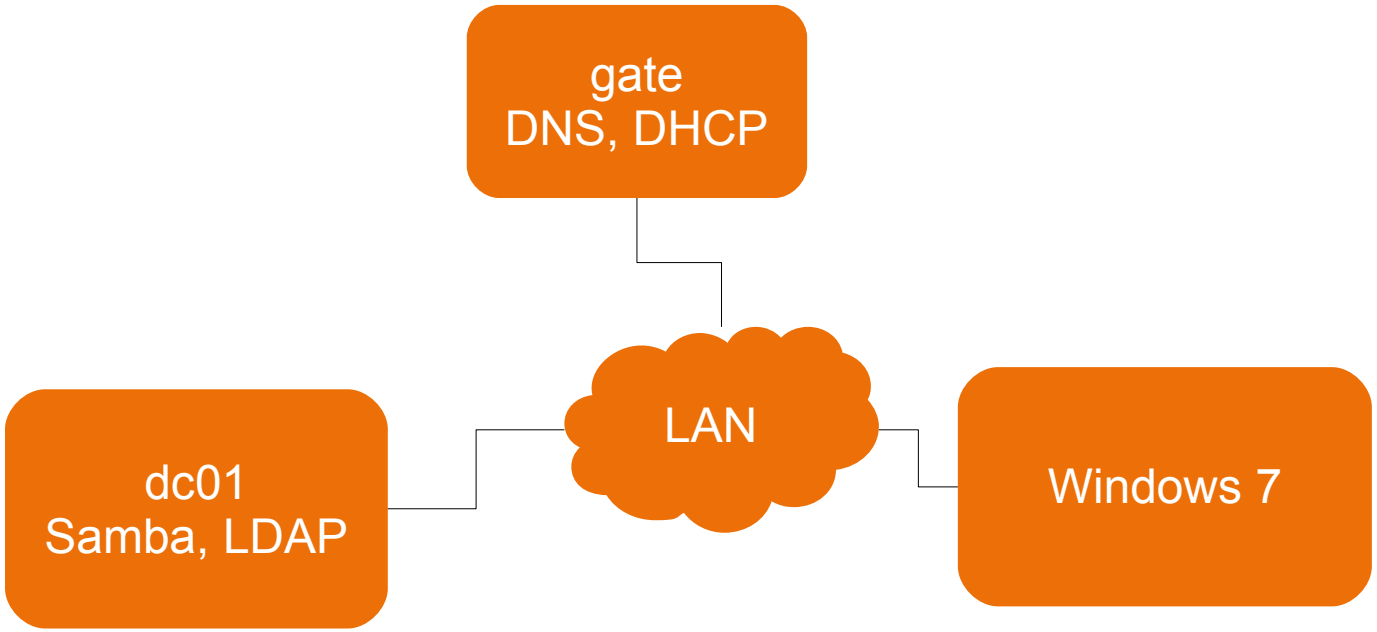
- Mitglieder der NT4-Domain
  - integrieren sich automatisch ins AD
  - nur Neustart notwendig
  - Empfehlung: Ausschalten während des Classic-Upgrades
- Neue Windows-Rechner
  - Können vom Domain-Admin in die AD-Domain aufgenommen werden
- Windows RSAT Verwaltungstools
  - AD Benutzer + Gruppen
  - Group Policies
  - DNS
  - Funktionieren wie am Microsoft AD-Server

Linux-Clients

- Authentifizierung gegen AD
  - nslcd
  - sssd
  - winbind
- wichtig: RFC2307bis-Schema im AD
  - uidNumber
  - unixHomedirectory
  - wird durch Classic-Upgrade angelegt
- Neue Nutzer brauchen UID + Home-Directory
  - Provisionierungsskript empfehlenswert

Teil 2:
Praxis

Demo-Netzwerk



- Migration auf Samba 4 AD

gate
====

```
vim /etc/dhcp/dhcpd.conf
        option domain-name-servers 10.24.4.2;
service isc-dhcp-server restart
```

dc01
====

```
service nmbd stop
service smbd stop
service samba stop

mkdir -pv /root/samba.PDC/etc

find /var/cache/samba/ /run/samba /var/lib/samba -type f -print0 |xargs -0 mv -
vi --target-directory=/root/samba.PDC/

mv -v /etc/samba/smb.conf /root/samba.PDC/etc

rm -rfv /var/cache/samba/* /var/spool/samba/* /var/lib/samba/* /run/samba/* /
etc/samba/*

mkdir /var/lib/samba/private

chmod 0750 /var/lib/samba/private

mkdir -pv /root/samba.PDC/dbdir

cd /root/samba.PDC

mv -v secrets.tdb schannel_store.tdb passdb.tdb group_mapping.tdb
account_policy.tdb gencache_notrans.tdb wins.dat dbdir/

samba-tool domain classicupgrade --verbose  --dbdir=/root/samba.PDC/dbdir/ --
use-xattrs=yes --realm=ad.example.org --dns-backend=SAMBA_INTERNAL /root/
samba.PDC/etc/smb.conf


vim /etc/samba/smb.conf
        [global]
        dns forwarder = 10.24.4.1
        # Bug in Samba 4.3
        allow dns updates = nonsecure
        load printers = No
        printcap name = /dev/null
        log level = 2
        max log size = 8192
        winbind enum users = yes
        winbind enum groups = yes
        winbind use default domain = yes
        ldap server require strong auth = no

        [homes]
        # available = No
        comment = Home Directories
        browseable = yes
        read only = no
        create mask = 0700
        directory mask = 0700
        valid users = %S

        [profiles]
        path = /srv/samba/profiles
        read only = No
        profile acls = Yes
        map hidden = Yes
        map system = Yes
```

```
        map archive = Yes
        browseable = No
        dos filetime resolution = No
        create mask = 0600
        directory mask = 0700

service slapd stop

systemctl disable slapd.service

apt purge nslcd

slapcat > /root/backup.ldif

apt install winbind libnss-winbind libpam-winbind

vim /etc/nsswitch.conf
        passwd:  compat winbind
        group:   compat winbind
        shadow:  compat

vim /etc/resolv.conf
        nameserver 10.24.4.2
        search ad.example.org example.org

reboot
service samba-ad-dc stop
service samba-ad-dc start

wbinfo -t
getent passwd
ln -s /var/lib/samba/private/krb5.conf /etc/krb5.conf
apt install krb5-user
smbpasswd Administrator
kinit Administrator
klist
ln -s /var/lib/samba/sysvol/ad.example.org/scripts /etc/samba/netlogon


host -a ad.example.org
host -t srv _ldap._tcp.ad.example.org
host gate
```

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.
  - Robert Sander
  - Mail: r.sander@heinlein-support.de
  - Telefon: 030/40 50 51 - 43
- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

Wir suchen:
Admins, Consultants, Trainer!

Wir bieten:
Spannende Projekte, Kundenlob, eigenständige Arbeit, keine Überstunden, Teamarbeit

...und natürlich: Linux, Linux, Linux...

http://www.heinlein-support.de/jobs

Robert Sander <r.sander@heinlein-support.de>

heinlein

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN ELEMENTS

Hard- und Software-Appliances und speziell für den Serverbetrieb konzipierte Software rund ums Thema eMail.