



Migration Windows-AD zu Samba4



Inhaltsübersicht

Aktuelle Infrastruktur

Entscheidungsprozess Samba4

Samba4-Tests

Kompatibilitätstests

Migrationstests

~~Samba4 im täglichen produktiven Einsatz~~

Fazit



Aktuelle Infrastruktur

Domäne:	Windows Server 2008 R2
Nutzerzahl:	ca. 20 000 Nutzer (12 000 Studenten)
Führendes IdMS:	OpenLDAP 2.4
DNS:	Bind9.8
DHCP:	ISC-DHCP
VDI:	VMware Horizon View





Entscheidungsprozess Samba4

Pro

Lizenzkosten

GPOs werden unterstützt

Kompatibilität mit Windows Server 2003/2008 R2

Domänen-Verwaltung für Windows AD-Admins unverändert



Entscheidungsprozess Samba4

Contra

Administrationsaufwand unbekannt

Tatsächliche Kompatibilität unbekannt

Zuverlässigkeit in großer Umgebungen unbekannt

Kompatibilität mit vorhandener Infrastruktur unbekannt



Samba4 Tests

Sernet-Paket vs. Quellen

Test in privatem Netzbereich

2 Samba4 DC (Debian Wheezy)

1 Fileserver (Debian Wheezy)

Verschiedene Clients (XP, Windows 7, Ubuntu 13.10)



Samba4 Tests

Vorbereitung DC / Fileserver / Linux Clients

Pakete deinstallieren

samba-common, samba-common-bin, smbclient

Pakete installieren

heimdal-clients, apt-transport-https



Samba4 Tests

Installation DC

```
aptitude install sernet-samba-ad
```

```
samba-tool domain provision
```

Editieren der /etc/default/sernet

Samba_Start_Mode="ad"

Automatisch erstellte **krb5.conf** nach **/etc** kopieren

```
service sernet-samba-ad start
```



Samba4 Tests

Installation zusätzlicher DC

krb5.conf vom ersten DC nach **/etc** kopieren

```
aptitude install sernet-samba-ad
```

```
samba-tool domain join example.net DC \  
-U administrator --realm=example.net
```

Editieren der `/etc/default/sernet`

Samba_Start_Mode="ad"

```
service sernet-samba-ad start
```



Samba4 Tests

Installation Fileserver / Linux Clients

```
aptitude install sernet-samba, sernet-samba-winbind
```

krb5.conf vom DC nach **/etc** kopieren

/etc/samba/smb.conf anlegen

/etc/nsswitch.conf editieren

```
passwd: compat winbind
```

```
group:  compat winbind
```

```
net rpc join example.net -U administrator
```

Editieren der `/etc/default/sernet`

Samba_Start_Mode="classic"

```
service sernet-samba-winbind start
```



Samba4 Tests

Funktionstests

```
kinit administrator@EXAMPLE.NET  
klist
```

DOMAIN in **GROßBUCHSTABEN!!**

```
wbinfo -u  
wbinfo -g  
getent passwd  
getent group
```



Samba4 Tests

Probleme und Besonderheiten

Bei mehr als einem DC sollte der Fileserver auf einem eigenen Server liegen

Freigabename der Home-Directorys MUSS **users** heißen

/var/lib/samba/private und **/var/lib/samba/sysvol** sichern!!

Bei zusätzlichen DCs **/var/lib/samba/sysvol** synchronisieren
via **rsync/xinetd / csync2**

Desktop.ini im Autostart-Order des Profils



Kompatibilitätstests

Externer BIND9-Server

CNAME-Record **objectGUID._msdcs.domain.net**

SRV-Record **_ldap._tcp.domain.net**

SRV-Record **_kerberos._tcp.domain.net**

BIND9-Version

9.7 -> funktioniert, aber komplizierter bzgl. Kerberos
wenn möglich 9.8 oder 9.9 verwenden

Externer LDAP/DHCP



Kompatibilitätstests

VMware Horizon View

Verbindung mit der Samba4-Infrastruktur möglich

Virtueller Desktop kann ausgerollt werden

Leeres Computerkonto im AD

Fehlende Vertrauensstellung, daher keine Anmeldung
am Client möglich

VMware: Kein Support für Samba4!



Migrationstests

Schritte

Samba4 als zusätzlichen DC an der Windows Domäne anmelden

DNS-Einträge hinzufügen

FSMO-Rollen übertragen (`samba-tool fsmo transfer --role=all`)

Windows AD Server vom Netz nehmen



Migrationstests

Vorbereitung

Klonen der Windows AD Server

Neuen Samba4-Server anlegen

Windows 7 Client



Migrationstests

Durchführung mit Sernet-Paketen

```
samba-tool domain join example.net DC \  
-U administrator --realm=example.net
```

Join failed - cleaning up

```
...  
checking sAMAccountNameERROR(ldb): uncaught exception - attribute 'isRecycled': invalid modify  
flags on 'CN=NTDS  
Settings\0ADEL:f0a27911-d9d3-4752-afd6-217c289b5baf,CN=SMB1\0ADEL:67680fef-790d-452c-ac87-95c546e54f81,  
CN=Servers,CN=Uni-Greifswald,CN=Sites,CN=Configuration,DC=uni-greifswald,DC=de':  
0x0  
File "/usr/lib/python2.7/dist-packages/samba/netcmd/__init__.py", line 175, in _run  
    return self.run(*args, **kwargs)  
File "/usr/lib/python2.7/dist-packages/samba/netcmd/domain.py", line 552, in run  
    machinepass=machinepass, use_ntvfs=use_ntvfs, dns_backend=dns_backend)  
File "/usr/lib/python2.7/dist-packages/samba/join.py", line 1172, in join_DC  
    ctx.do_join()  
File "/usr/lib/python2.7/dist-packages/samba/join.py", line 1077, in do_join  
    ctx.join_replicate()  
File "/usr/lib/python2.7/dist-packages/samba/join.py", line 851, in join_replicate  
    ctx.local_samdb.transaction_commit()
```



Migrationstests

Durchführung mit Samba-Quellen

Entwickler-Patch eingespielt

Samba4 kompiliert

```
samba-tool domain join example.net DC \  
-U administrator --realm=example.net
```

Dauer: ca. 6 Stunden (2 Kerne, 4GB RAM)



Fazit

Pro

Samba4 funktioniert (prinzipiell)

GPO, Home & Profile Directorys

Sernet Pakete

Lizenzkosten



Fazit

Contra

AD-Papierkorb (noch) ein Problem

Kein Support durch VMware für VDI

Fehleranfällig?

Fehlermeldungen

Fehlende Bash-Completion bei **samba-tool**

Manuelle Synchronisation des Sysvol-Verzeichnisses

Links

Samba Wiki:

<https://wiki.samba.org/>

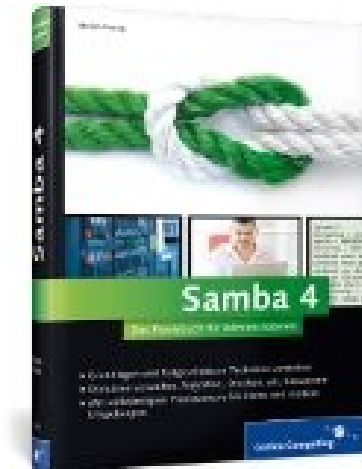
Samba Mailing Liste:

<https://lists.samba.org/>

Sernet Enterprise:

<http://enterprisesamba.com/>

**Samba 4:
Das Praxisbuch
Für Administratoren**





Fragen? Fragen!