Replika / Beitritt (Joining)
eines Samba ADC zu einer bestehenden
Active Directory Samba AD mit Opensuse leap 15

==========

Konvention: dc1 bestehender Samba 4 ADC
dc2 zweiter Samba 4 ADC
Domäne: ZION2.SITE

1) /*etc*/resolv.conf des dc2 muss IP des dc1 eingetragen werden

2) /etc/krb5.conf

```
[libdefaults]
dns_lookup_realm = false
dns_lookup_kdc = true
default_realm = ZION2.SITE
```

2a) /etc/hosts auf dem neuen dc2

```
127.0.0.1 localhost

192.168.0.224          zion2-joined.zion2.site zion2-joined
```

3) Test:

```
kinit administrator

Password for administrator@ZION2.SITE

klist

.....
```

4) /etc/samba/smb.conf auf dem dc2 löschen (sonst erhält man eine Fehlermeldung)

5) Join dc2 to dc1 (Domain ZION2.SITE)

```
samba-tool domain join ZION2.SITE DC -U"ZION2\administrator" /

--option='idmap_ldb:use rfc2307=yes' –dns-backend=SAMBA_INTERNAL
```

6) Built-in User & Group ID Mappings übernehmen

auf dc1:

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

dann idmap.ldb.bak auf dc2 kopieren und original idmap.ldb ersetzen

7) samba-tool ntacl sysvolreset

8) systemctl start samba-ad-dc.service

8a) Testen des neuen Sambaservers

```
samba-tool domain info 192.168.0.224     ##ip addr  of dc2
```

9) Kontrolle der Replikation

samba-tool drs showrepl

10) auf dc2 resolv.conf

nameserver 127.0.0.1

nameserver 192.168.0.222   #### ip addr of dc1

search zion2.site

11) auf dc1 resolv.conf

nameserver 127.0.0.1

nameserver 192.168.0.224   ### ip addr of new dc2

nameserver 1.1.1.1

12) Test des DNS auf dc1 und dc2

host -t A zion2.site localhost

Sollte folgendes Ergebnis liefern (entsprechend angepasste IP)

Using domain server:

Name: localhost

Address: 127.0.0.1#53

Aliases:

zion2.site has address 192.168.0.222

zion2.site has address 192.168.0.224

13) sysvol muss per Hand (cronjob oder Dämon) mit rsync übertragen werden

14) Falls ADC gleich Master für Freigaben:

Sync auch hier per Cronjob (rsync ar ...usw)

Ergänzung:

Zeitserver auf beiden dc nicht vergessen:

/etc/ntp.conf

==========

server 127.127.1.0

fudge 127.127.1.0 stratum 10

server 0.pool.ntp.org iburst prefer

server 1.pool.ntp.org iburst prefer

driftfile /var/lib/ntp/ntp.drift

logfile /var/log/ntp

ntpsigndsocket /var/lib/samba/ntp_signd/

restrict default kod nomodify notrap nopeer mssntp

restrict 127.0.0.1

restrict 0.pool.ntp.org mask 255.255.255.255 nomodify notrap nopeer noquery

restrict 1.pool.ntp.org mask 255.255.255.255 nomodify notrap nopeer noquery

--→ dann service starten