15 Sicherung der Datenbanken

Denken Sie immer auch an den Fall, dass mal etwas schiefgehen kann. Welche Konfigurationsdaten benötigen Sie unbedingt, um Ihr System wiederherstellen zu können? Deshalb beschäftigt sich dieses Kapitel mit der Sicherung und Wiederherstellung eines Domaincontrollers. Dazu gehören die LDAP-Datenbanken und die *tdb*-Datenbanken Ihres Systems sowie auch die Datei `smb.conf` und nicht zuletzt die Gruppenrichtlinien.

In diesem Kapitel geht es nicht um die Sicherung Ihrer Daten, sondern um die Sicherung und Wiederherstellung der Konfiguration des DCs. Wie können Sie die Informationen des LDAP und der anderen Datenbanken, die für den Betrieb der Domäne und des Samba-4-Servers relevant sind, sichern? Denn auch hinsichtlich einer Disaster Recovery müssen Sie sich bei Samba 4 mehr Gedanken machen als vielleicht noch bei Samba 3.

Das Wiederherstellen der Datenbank aus den gesicherten Daten ist immer nur der letzte Weg, um Ihr Active Directory wiederherzustellen: wenn Ihre Datenbank gänzlich unbrauchbar ist, weil zum Beispiel das Einspielen von Attributen komplett fehlgeschlagen ist, oder versucht wurde, ein Schema, das für Samba nicht geeignet ist (zum Beispiel das Exchange-Schema) zu installieren. Nur dann brauchen Sie die gesicherten Datenbanken, um Ihr Active Directory wiederherstellen zu können. Unter keinen Umständen spielen Sie das Backup der Datenbanken ein, solange noch ein Domaincontroller ordnungsgemäß arbeitet. Denn solange Sie noch einen Domaincontroller mit einer funktionierenden und vollständigen Datenbank haben, können Sie alle anderen Domaincontroller einfach neu aufsetzen und in die Domain bringen.

15.1 Sicherung der Datenbanken

Beim Sichern der Datenbanken hat sich so einiges getan: Das alte Skript aus der vorherigen Auflage des Buches gibt es nicht mehr, und es wird auch nicht mehr benötigt. Das Sichern und Wiederherstellen der Datenbanken und der Gruppenrichtlinien können Sie jetzt mit dem `samba-tool` durchführen.

Als Vorbereitung habe ich einen neuen Domaincontroller aufgesetzt und eine neue Domain mit dem Bind9 als DNS-Server eingerichtet. Um später die Kontrolle zu haben, ob alle Objekte nach einem Recovery wieder vorhanden sind, habe ich Benutzer und Gruppen und eine Gruppenrichtlinie angelegt.

15.1.1 Möglichkeiten zur Sicherung der Datenbanken

Mit Samba 4.9 wurde das erste Mal die Möglichkeit bereitgestellt, mit dem `samba-tool` die Datenbank zu sichern und wiederherzustellen. Die erste Möglichkeit war es, die Datenbanken *online* zu sichern, sprich der Domaincontroller, auf dem Sie die Datensicherung durchführen, muss laufen. Seit der Version 4.10 ist dann auch eine *offline*-Sicherung möglich. Die Vorteile der offline-Sicherung sind, dass der Vorgang schneller ist und dass mehr Daten gesichert werden. Dieses Mehr an Daten ermöglicht eine erweiterte forensische Analyse der Daten. Der Domaincontroller-Dienst muss für die offline-Sicherung nicht laufen. Alle Aktionen werden mittels des `samba-tool` durchgeführt. Dazu finden Sie im Submenü *domain* den Unterpunkt *backup*. In Listing 15.1 sehen Sie die Unterpunkte:

Listing 15.1 Unterpunkte des samba-tool

```
root@addc-01:~# samba-tool domain backup
Usage: samba-tool domain backup <subcommand>

Available subcommands:
  offline  - Backup the local domain directories safely into a tar file.
  online   - Copy a running DC's current DB into a backup tar file.
  rename   - Copy a running DC's DB to backup file, \
             renaming the domain in the process.
  restore  - Restore the domain's DB from a backup-file.
```

Zusätzlich zu den Optionen `online`, `offline` und `restore` sehen Sie hier noch eine Option `rename`. Mit der Option `rename` können Sie eine bestehende Domäne sichern und gleichzeitig umbenennen. Dabei werden alle Objekt-DNs umgeschrieben. Die Domäne kann hinterher parallel zur bestehenden Domäne wiederhergestellt werden. Aber Achtung! Die sysvol-Daten und die Gruppenrichtlinie müssen von Hand angepasst werden. Verwenden Sie die Option nur, wenn Sie wirklich wissen, was Sie vorhaben. Lesen Sie auf jeden Fall die Hilfe zu der Option. Hier im Buch werde ich diese Option nicht besprechen.

15.1.1.1 Die online-Sicherung

Beginnen möchte ich mit der *online*-Sicherung der Domäne. Wenn Sie die online-Sicherung durchführen, benötigen Sie auf jeden Fall einen laufenden Domaincontroller. Vor der Sicherung führen Sie auf jeden Fall ein `samba-tool dbcheck --cross-ncs` durch und beheben alle eventuell angezeigten Fehler, denn was nützt eine fehlerhafte Sicherung? Die Option `--cross-nsc` prüft auch alle DNS-Datenbanken auf Fehler. Die Sicherung kann nicht auf einem RODC durchgeführt werden, da dieser nicht alle benötigten Daten für die Wiederherstellung besitzt.

Nach der fehlerfreien Datenbankprüfung können Sie dann die Sicherung so wie in Listing 15.2 durchführen. Vor dem Backup habe ich noch die Prüfung der Datenbank durchgeführt:

Listing 15.2 Das online-Backup

```
root@addc-01:~# samba-tool dbcheck --cross-ncs
```

```
Checking 3643 objects
Checked 3643 objects (0 errors)

root@addc-01:~# samba-tool domain backup online --server=addc-01 --
    targetdir=. -k yes
... workgroup is EXAMPLE
... realm is example.net
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
Unable to determine the DomainSID, can not enforce uniqueness \
    constraint on local domainSIDs

... A Kerberos configuration suitable for Samba AD has been generated \
    at /root/tmp5ksda6fg/private/krb5.conf
 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=example,DC=net
Starting replication
Using DS_BIND_GUID_W2K3
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net] \
       objects[402/1739] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net] \
       objects[804/1739] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net] \
       objects[1206/1739] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net] \
       objects[1608/1739] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net] \
       objects[1739/1739] linked_values[0/0]
Analyze and apply schema objects
Partition[CN=Configuration,DC=example,DC=net] \
       objects[402/1622] linked_values[0/1]
Partition[CN=Configuration,DC=example,DC=net] \
       objects[804/1622] linked_values[0/1]
Partition[CN=Configuration,DC=example,DC=net] \
       objects[1206/1622] linked_values[0/1]
Partition[CN=Configuration,DC=example,DC=net] \
       objects[1608/1622] linked_values[0/1]
Partition[CN=Configuration,DC=example,DC=net] \
       objects[1622/1622] linked_values[18/18]
Replicating critical objects from the base DN of the domain
```

```
Partition[DC=example,DC=net] objects[97/97] linked_values[23/23]
Partition[DC=example,DC=net] objects[224/224] linked_values[27/27]
Done with always replicated NC (base, config, schema)
Replicating DC=DomainDnsZones,DC=example,DC=net
Partition[DC=DomainDnsZones,DC=example,DC=net] objects[40/40] \
   linked_values[0/0]
Replicating DC=ForestDnsZones,DC=example,DC=net
Partition[DC=ForestDnsZones,DC=example,DC=net] objects[18/18] \
   linked_values[0/0]
Committing SAM database
Repacking database from v1 to v2 format (first record \
   CN=Print-Max-Copies,CN=Schema,CN=Configuration,DC=example,DC=net)
Repack: re-packed 10000 records so far
Repacking database from v1 to v2 format (first record \
   CN=lostAndFound-Display,CN=40B,CN=DisplaySpecifiers,\
   CN=Configuration,DC=example,DC=net)
Repacking database from v1 to v2 format (first record \
   DC=g.root-servers.net,DC=RootDNSServers,CN=MicrosoftDNS,\
   DC=DomainDnsZones,DC=example,DC=net)
Repacking database from v1 to v2 format
   (first record DC=e7fcb9c0-0f3c-475a-a30d-663eeb74baf7,\
   DC=_msdcs.example.net,CN=MicrosoftDNS,DC=ForestDnsZones,\
   DC=example,DC=net)
Repacking database from v1 to v2 format (first record \
   CN=Dfs-Configuration,CN=System,DC=example,DC=net)
... Setting isSynchronized and dsServiceName
... Cloned domain EXAMPLE (SID S-1-5-21-3818853491-1829902833-3083116257)
... Backing up sysvol files (via SMB)...
Password for [administrator@EXAMPLE.NET]:
 Creating backup file ./samba-backup-example.net-2021-03-\
          03T19-17-32.890546.tar.bz2...
```

Die Meldung zur *DomainSID* können Sie ignorieren, es handelt sich um eine Meldung, die schon längst entfernt werden sollte. Wichtig ist die letzte Zeile, die anzeigt, dass das Backup erstellt wurde und wie die Datei mit den Daten heißt.

Kopieren Sie die Datei testweise in ein anderes Verzeichnis und entpacken die Datei dort; so sehen Sie, was alles gesichert wurde.

Die Sicherung sollten Sie auf gar keinen Fall auf dem Domaincontroller lassen! Kopieren Sie die Datei an einen sicheren Ort. In der Datei befinden sich alle Passwörter, zwar verschlüsselt, aber jemand, der die Datei auf irgendeine Art und Weise in Besitz nehmen kann, wäre in der Lage, die verschlüsselten Passwörter auszuwerten. Ein weiterer Grund ist der, dass wenn die Datei dort liegt und der Domaincontroller nicht mehr startet und Sie keine Möglichkeit haben, auf die Platte zuzugreifen, dann nützt auch das Backup nichts. Dadurch, dass Sie die Datei von Domaincontroller entfernen, kann auch keiner auf die Idee kommen, "schnell mal" das Backup einzuspielen, weil ein Objekt gelöscht wurde.

15.1.1.2 Die offline-Sicherung

Auch bei der *offline*-Sicherung prüfen Sie als Erstes die Datenbank und beheben Sie eventuelle Fehler. Anschließend führen Sie die Sicherung so durch wie in Listing 15.3:

Listing 15.3 Die offline-Sicherung

```
root@addc-01:~# samba-tool dbcheck --cross-ncs
Checking 3643 objects
Checked 3643 objects (0 errors)

root@addc-01:~# samba-tool domain backup offline  --targetdir=.
...
```

Leider musste ich das offline-Backup an der Stelle abbrechen, denn es gibt einen Bug *https://bugzilla.samba.org/show_bug.cgi?id=14027*, der im Moment dafür sorgt, dass das offline-Backup nicht in Verbindung mit dem Bind9 funktioniert. Sie können das offline-Backup im Moment nur zusammen mit dem internen DNS-Server nutzen.

15.1.2 Wiederherstellung der Domäne aus dem Backup

Da ich für die Domaincontroller in meiner Domäne den Bind9 nutze, verwende ich zur Wiederherstellung die Daten aus dem online-Backup. Sorgen Sie dafür, dass der Hostname des neuen Domaincontrollers nicht identisch ist mit dem Domaincontroller, auf dem Sie die Sicherung erstellt haben.

Um den Totalausfall der Domäne zu simulieren, lösche ich den Inhalt des Verzeichnisses /var/lib/samba/, aber nicht das Verzeichnis selbst. Anschließend können Sie das Backup wieder einspielen. Beim Einspielen des Backups ist es unbedingt notwendig, dass Sie dem Domaincontroller einen neuen Namen geben – siehe Listing 15.4:

Listing 15.4 Wiederherstellung der Domäne

```
root@addc-01:~# samba-tool domain backup restore --backup-file \
                samba-backup-example.net-2021-03-03T19-17-32.\
                890546.tar.bz2 --targetdir=/var/lib/samba \
                --newservername=addc-01a
Adding new DC to site 'Default-First-Site-Name'
Updating basic smb.conf settings...
Creating account with SID: S-1-5-21-3818853491-1829902833-3083116257-1109
Adding CN=ADDC-01A,OU=Domain Controllers,DC=example,DC=net
...
Setting account password for ADDC-01A$
Enabling account
Seizing rid FSMO role...
FSMO seize of 'rid' role successful
Seizing pdc FSMO role...
FSMO seize of 'pdc' role successful
Seizing naming FSMO role...
FSMO seize of 'naming' role successful
Seizing infrastructure FSMO role...
FSMO seize of 'infrastructure' role successful
Seizing schema FSMO role...
FSMO seize of 'schema' role successful
...
```

```
Removing computer account: CN=ADDC-01,OU=Domain Controllers,\
   DC=example,DC=net (and any child objects)
...
Fixing up any remaining references to the old DCs...
Backup file successfully restored to /var/lib/samba
Please check the smb.conf settings are correct \
before starting samba.
```

Die Ausgabe ist hier verkürzt dargestellt, aber Sie sehen, es gibt noch den alten Domaincontroller in der Sicherung. Daher ist es notwendig, für den neuen Domaincontroller einen neuen Namen zu vergeben. Der alte Domaincontroller wird aus der Datenbank gelöscht.

Damit ist die Wiederherstellung aber noch nicht abgeschlossen. Die folgenden Punkte müssen unbedingt vor dem Starten des Domaincontrollers durchgeführt werden.

Hinweis

Wenn Sie den internen DNS-Server nutzen, dann können Sie die Schritte 3 bis 5 überspringen.

1. Prüfen Sie die smb.conf auf die korrekten Einstellungen.
2. Im Backup der Domäne finden Sie eine Datei sysvol.tar.gz. Entpacken Sie die Datei, erstellen Sie das Verzeichnis /var/lib/samba/sysvol und kopieren Sie den Inhalt des tar-Files in das Verzeichnis.
3. Führen Sie ein `samba-tool ntacl sysvolreset` aus, um die Rechte des sysvol-Verzeichnisses wieder korrekt zu setzen.
4. Führen Sie ein `samba_upgradedns` aus, um den internen DNS-Server zu konfigurieren. Dadurch werden die NS-Records für die Zonen angelegt. Den Hinweis auf die Anpassung der smb.conf können Sie ignorieren, da im nächsten Schritt die Umstellung auf den Bind9 stattfindet. Führen Sie diesen Schritt nicht aus, startet der Bind9 nicht, da er keinen NS-Record für Ihre Domäne findet
5. Wenn Sie den Bind9 als DNS-Server nutzen, führen Sie das Kommando `samba_upgradedns --dns-backend=BIND9_DLZ` aus, um das Verzeichnis /var/lib/samba/bind-dns wieder zu füllen und die dns.keytab-Datei wiederherzustellen.
6. Passen Sie die Konfigurationsdateien des Bind9 an. Starten Sie anschließend den Bind9 neu und prüfen Sie das Log.
7. Prüfen Sie die Rechte am Verzeichnis /var/lib/samba. Die Rechte müssen dort auf *755* stehen.

Starten Sie den Domaincontroller neu und prüfen Sie, ob alle Benutzer, Gruppen und Gruppenrichtlinien vorhanden sind. Stellen Sie die Verknüpfungen der Gruppenrichtlinien wieder her.

Es ist geschafft, Sie haben Ihre Domäne wiederhergestellt. Jetzt können Sie nach und nach alle Domaincontroller aufsetzen und wieder in die Domäne joinen.