Stefan Kania
IT-Consulting durch Training

Disaster Recovery einer Samba4 Active Directory Domäne

Autor:
Stefan Kania

Ort:
Berlin

06.05.2024

Inhalt

1 Einführung

Dieses Jahr steht das große Thema Desater Recovery auf der Agenda: Wie kann ich, bei einem Totalausfall meiner Domäne, schnell wieder alle Domaincontroller herstellen? Nach der Theorie werde ich die bestehende Domäne sichern, alle dazugehörigen Datenbanken löschen und die Domäne wieder aus dem Backup herstellen, sodass im Anschluss die Domäne wieder voll funktionsfähig sein wird. Im Vortrag werde ich als Nameserver auf den internen DNS-Server vom Samba zurückgreifen. Aber das Prinzip ist beim Bind9 identisch.

2 Desaster recovery einer Domäne

"Frage nie ob dein System ausfällt, frage immer nur wann es ausfällt". Der Totalausfall der gesamten Domäne ist das Schlimmste was ihre Domäne treffen kann, denn dann kann sich kein Benutzer mehr anmelden, ein Zugriff auf die Daten ist nicht mehr möglich. Treffen Sie frühzeitig Maßnahmen wie Sie in dem Fall reagieren müssen. Sichern Sie regelmäßig ihre Daten der Domäne. Aber, das Sichern der Informationen ist nur die halbe Miete, testen Sie auch, ob und wie Sie die Daten möglichst schnell wiederherstellen können. Erstellen Sie sich einen Ablaufplan für den Fall, dass Ihre Domäne ausfällt.

Im Vortrag soll es genau darum gehen: Wie erstelle ich ein Konzept zur Wiederherstellung meiner Domäne? Es soll die vorher erstellte Domäne aus einem Backup wiederhergestellt werden. Am Ende soll die Domäne, mit allen vorherigen Funktionen funktionieren. Das beinhaltet sowohl alle Benutzerkonten mit Passwörtern, alle GPOs inklusive der Verlinkungen zu den einzelnen OUs, als auch die Mitgliedschaft aller Clients.

2.1 Grundlagen zur Sicherung

Um die Domäne zu sichern, steht Ihnen das Kommando `samba-tool` zur Verfügung. Sie können Ihre Domäne im laufenden Betrieb sichern. Für die Sicherung stehen Ihnen zwei Verfahren zur Verfügung.

1. Das online Backup Beim online Backup sichern Sie die Datenbanken des Active Directories und alle anderen benötigten Dateien in einem tar.bz2-file den Sie dann an einem sicheren Ort, für den Notfall speichern. Das online Backup kann auf einem Domaincontroller selbst, oder remote von einem anderen System aus erstellt werden. Der Domaincontroller, der gesichert werden soll, muss dafür aber laufen und alle Dienste müssen aktiv sein. Das online Backup funktioniert ähnlich wie der *Join* eines neue Domaincontrollers in die Domäne.
2. Das offline Backup Auch das offline Backup sichert alle benötigten Daten, die Sie zur Wiederherstellung benötigen, zusätzlich werden noch weiter Daten gesichert, die ein Debuging ermöglichen. Bei dem offline Backup werden die Dateien des Domaincontrollers so gesichert, wie sie auf dem Domaincontroller existieren. Das offline Backup kann nur lokal auf einem Domaincontroller, als *root*, durchgeführt werden, der Samba-Dienst muss dafür nicht laufen.

Eines ist ganz wichtig: Niemals spielen Sie ein Backup wieder ein, solange noch ein Domaincontroller ordnungsgemäß läuft! Das Backup wird nur dann benötigt, wenn kein Domaincontroller mehr die Dienste der Domäne bereitstellen kann.

Spielen Sie ein Backup auf einen Domaincontroller ein wenn noch ein Domaincontroller voll funktionsfähig ist, zerstören Sie damit Ihre Domäne, denn dann hätten Sie zwei Domaincontroller mit unterschiedlichen Datenbankständen. Diese unterschiedlichen Stände würden dann repliziert und es käme auf jeden Fall zu einem Konflikt der nicht mehr auflösbar ist.

Für welche Art des Backups Sie sich entschieden, spielt keine große Rolle, wichtig ist nur, dass Sie überhaupt ein Backup erstellen. Wie oft Sie ein Backup erstellen ist davon abhängig, wie viele Änderungen in Ihrer Domäne durchgeführt werden. Wichtig sind nur die folgenden Punkte:

1. Führen Sie überhaupt ein Backup aus.
2. Speichern Sie das Backup an einem sichern Ort. Nicht auf dem Domaincontroller selbst. Denken Sie daran, alle Passwörter sind in dem Backup gespeichert. JEDER, der das Backup in in die Hände bekommt, kann damit ihre Domäne wieder herstellen.
3. Wenn Sie den *Bind9* als Nameserver einsetzen, dann sichern Sie zusätzlich all Konfigurationsdateien für den *bind9*. Die Datenbanken werde automatisch gesichert.
4. Testen Sie, in regelmäßigen Abständen, ob Sie Ihre Domäne aus dem Backup wiederherstellen können. Nutzen Sie dafür eine Testumgebung.

2.2 Sicherung der Domäne

Wie eingangs beschrieben, stellen Sie das Backup mit dem Kommando `samb-tool` her. In Listing 2.2.1 sehen Sie den Vorgang für die Erstellung eines online Backups:

```
root@dc01:~# samba-tool domain backup online --server=dc01 --targetdir . -Uadministrator
Password for [EXAMPLE\administrator]:
...
Creating backup file ./samba-backup-example.net-2024-04-15T17-55-57.379101.tar.bz2...
```

Listing 2.2.1: Erstellung eines online Backups

Um sich den Inhalt der Datei anzusehen, kopieren Sie die Datei in ein Verzeichnis und entpacken Sie es dort. Nach dem Entpacken der Datei können Sie sehen, welche Informationen gesichert wurden. Nicht nur die Datenbanken des Active Direcories wurden gesichert, sondern auch alle Daten aus der Freigabe sysvol und die Datei smb.conf. Schauen Sie sich einmal die Datei backup.txt an, dort finden Sie alle wichtigen Informationen zur der Sicherung.

Zur Wiederherstellung benötigen Sie aber unbedingt die gepackten Daten!

Um Ihnen auch den Unterschied zu zeigen, sehen Sie in Listing 2.2.2 das Kommando für das offline Backup:

```
root@dc01:~# samba-tool domain backup offline  --targetdir .
...
Backup succeeded.
```

Listing 2.2.2: Description

Im Gegensatz zum online Backup sehen Sie hier, dass Sie keine Servernamen angeben müssen und auch keine Authentifizierung durchgeführt wird. Das liegt daran, dass das offline Backup nur lokal auf dem Domaincontroller vom Benutzer *root* durchgeführt werden kann.

Das Backup können Sie auch bei deaktivierten Samba-Dienst durchführen.

Wichtig für beide Arten des Backups: Denken Sie daran, dass sich in dem Backup auch alle Anmeldeinformationen aller Benutzer befinden, kopieren Sie die Datensicherung daher immer an einen sicheren Ort.

3 Wiederherstellen der Domäne

Für die Wiederherstellung der Domäne kopieren Sie eine der Datensicherungen auf den zusätzlichen Server mit dem Namen *dcrecover*. Stoppen Sie unbedingt den Samba-Dienst *samba-ad-dc* auf den dem ursprünglichen Domaincontroller. Löschen Sie dort noch keine Daten!

Für die Wiederherstellung ist es unbedingt erforderlich, dass Sie den Vorgang auf einem Host mit einem neuen Hostnamen durchführen, der Hostname darf in der Domäne nicht als aktiver Domaincontroller vorhanden sein. Beachten Sie die folgenden Schritte:

1. Setzen Sie einen neuen Host auf. Verwenden Sie, wenn möglich, die selbe Distribution wie auf den anderen Domaincontrollern.
2. Installieren Sie die Samba-Pakete, hier ist es wichtig, dass Sie die selbe Samba-Version wie in Ihrer Produktivumgebung installieren.
3. Wenn Sie den *bind9* als Nameserver nutzen, installieren Sie die Pakete und kopieren Sie die gesicherten Konfigurationen auf den neuen Host.
4. Kopieren Sie Ihre Datensicherung auf den neuen Host. Die Datei darf nicht entpackt werden.
5. Löschen Sie alle Daten im Verzeichnis /var/lib/samba, nicht aber das Verzeichnis selbst.
6. Löschen Sie eine eventuell vorhandene smb.conf

Führen Sie jetzt das Kommando, zur Wiederherstellung der Datenbank, aus Listing 3.1 aus:

```
root@dcrecover:~# samba-tool domain backup restore --backup-file=\
    samba-backup-2022-03-28T16-12-01.035389.tar.bz2 \
    --targetdir=/var/lib/samba --newservername=dcrecover
Adding new DC to site 'Default-First-Site-Name'
...
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.
```

Listing 3.1: Wiederherstellung der Datenbanken

Damit wurden alle Daten wieder hergestellt. Das reicht aber noch nicht aus um die Domäne wieder voll funktionsfähig zu bekommen. Um die vollständige Funktion wiederherzustellen, führen Sie die folgenden Schritte aus:

1. Deaktivieren Sie die Dienste *smbd*, nmbd und winbind.
2. Sorgen Sie dafür, dass die eigen IP-Adresse des Hosts als Nameserver verwendet wird.
3. Passen Sie die smb.conf aus dem Verzeichnis /var/lib/samba/etc an den neuen Host an. Besonders wichtig ist das, wenn Sie die Variablen *interfaces=IP* und *bind interfaces only = yes* nutzen.
4. Kopieren Sie die Datei smb.conf in das Verzeichnis /etc/samba. Führen sie hier keine Änderungen an den Pfadnamen durch, für die Wiederherstellung liegen einige Dateien in anderen Verzeichnissen.
5. Kopieren Sie die Datei /var/lib/samba/private/krb5.conf in das Verzeichnis /etc. Achten Sie darauf, dass der Hostname in der Datei korrekt ist.
6. Führen Sie das Kommando `samba-tool ntacl sysvolreset` aus. Damit stellen Sie die Rechte in der der Freigaben sysvol wieder her.
7. Wenn Sie den *bind9* als Nameserver nutzen, stellen Sie erst einmal auf den Internen Nameserver um, so werden dann auch die NS-Records für die forward-Zonen wieder erzeugt. Ergänzen Sie hierzu die Zeile *server services* in der smb.conf um den Wert *dns*. Führen Sie anschließend das Kommando `samba_upgradedns`, ohne weitere Parameter, aus.
8. Sorgen Sie dafür, dass der Dienst *samba-ad-dc* wieder starten kann und starten den Dienst.
9. Testen Sie alle Dienste. Prüfen Sie auch, ob alle Benutzer und Gruppen vorhanden sind.
10. Die Freigabe sysvol befindet sich jetzt im Verzeichnis /var/lib/samba/state/sysvol. Prüfen Sie auch hier, ob alle Gruppenrichtlinien vorhanden sind.

Wenn Sie den internen DNS-Server nutzen, haben Sie die Wiederherstellung abgeschlossen. Jetzt können Sie Ihre ursprünglichen Domaincontroller wieder neu in die Domäne aufnehmen. Anschließend übertragen Sie die FSMO-Rollen auf den ursprünglichen Domaincontroller. Dann können Sie den Domaincontroller den Sie für die Wiederherstellung genutzt haben, aus der Domäne entfernen.

3.0.1 Wenn Sie bind9 als DNS-Server nutzen

Wenn Sie *Bind9* als DNS-Server einsetzen, dann führen Sie auf jeden Fall noch die nachfolgenden Schritte durch:

1. Prüfen Sie, ob die Rechte am Verzeichnis /var/lib/samba auf 755 gesetzt sind.
2. Ändern Sie das DNS-Backend auf *BIND9_DLZ* mit dem Kommando `samba_upgradedns --dns-backend=BIND9_DLZ`.
3. Entfernen Sie den Service *dns* aus der Zeile *server services* in der smb.conf.
4. Prüfen Sie, dass die Gruppe *bind* Schreibrecht an dem Verzeichnis /var/lib/samba/bind-dns und allen Unterverzeichnissen besitzt.
5. Starten Sie den *bind9* neu und prüfen Sie das Log-file /var/Log/syslog ob dort Fehler aufgeführt werden.
6. Starten Sie den Samba-Dienst neu.

Damit wäre dann die Umstellung auf den *bind9* als DNS-Server abgeschlossen.

Sollten Sie bei Neustart des *bind9* die Fehlermeldung aus Listing 3.1 sehen, dann benötigen Sie weitere Schritte um den *bind9* wieder ohne Fehler starten zu können:

```
: Loading 'AD DNS Zone' using driver dlopen
: samba_dlz: started for DN DC=example,DC=net
: samba_dlz: starting configure
: samba_dlz: configured writeable zone 'example.net'
: zone 56.168.192.in-addr.arpa/NONE: has no NS records
: samba_dlz: Failed to configure zone '56.168.192.in-addr.arpa'
: loading configuration: bad zone
: exiting (due to fatal error)
```

Listing 3.1: Description

Dieser Fehler taucht immer dann auf, wenn Sie *revers-zonen* auf Ihrem *bind9* eingerichtet haben. Das Problem ist, dass zwar für die *forward-zonen* die *NS-records* auf allen DCs erstellt werden, nicht aber für die *revers-zonen*. Da in diesem Fall der *bind9* nicht mehr startet, können Sie auch keine neuen *NS-records* anlegen. Schalten Sie daher erst wieder auf den Internen DNS-Server um, erzeugen dann die *NS-records*, so wie Sie es in Listing 3.2 sehen:

```
root@recover-dc:~# samba-tool dns add recover-dc1 \
                   56.168.192.in-addr.arpa @ NS \
                   recover-dc1.example.net -U administrator
Password for [EXAMPLE\administrator]:
Record added successfully
```

Listing 3.2: Description

Führen Sie diesen Vorgang für alle *revers-Zonen* aus. Anschließend stellen Sie die Konfiguration wieder auf den *bind9* um und starten den Dienst neu. Jetzt sollte der *bind9* wieder ohne Fehlermeldung starten und Ihre *revers-Zonen* sind wieder vorhanden.

Damit wäre der Vorgang des Recoveries auch abgeschlossen. Jetzt können Sie auch hier die ursprünglichen Domaincontroller wieder in die Domäne aufnehmen, die FSMO-Rollen umziehen und den recovery Domaincontroller wieder aus der Domäne entfernen. Nach dem Entfernen des Recovery-Domaincontrollers können Sie alle weiteren Domäncontroller wieder in die Domäne aufnehmen. Dabei können Sie sowohl die alten Hostnamen als auch die alten IP-Adressen der Domäncontroller nutzen. Alle ursprünglichen Daten der bestehenden Domäncontroller werden bei der Wiederherstellung entfernt.

3.1 Fazit zum Recovery

Ein Domäne aus der Sicherung wiederherzustellen ist kein großes Problem, aber Sie sollten den Vorgang auf jeden Fall immer mal wieder in einer Testumgebung testen, dann gehen Ihnen die einzelnen Schritte im Falle eines Ausfalls auch leicht von der Hand.