

# HANSER



## Leseprobe

zu

## „Samba 4“

von Stefan Kania

ISBN (E-Book): 978-3-446-45735-5

Weitere Informationen und Bestellungen unter  
<http://www.hanser-fachbuch.de/978-3-446-45735-5>

sowie im Buchhandel

© Carl Hanser Verlag, München

# Vorwort

Eine neue Auflage vom Samba-4-Buch bei einem neuen Verlag. Der eine oder andere wird sich fragen, warum ich für diese Auflage den Verlag gewechselt habe. Ich kann Ihnen dazu nur sagen, dass ich mit meinem Samba-4-Buch ganz ohne jeden Streit vom Rheinwerk-Verlag zum Hanser-Verlag gewechselt bin. Die Bücher «Linux-Server» und «Shell-Programmierung» werde ich auch weiterhin für den Rheinwerk-Verlag schreiben.

Nun aber zu diesem Buch. Auch in dieser Ausgabe stecken wieder sehr viele Erfahrungen aus Projekten und Schulungen der letzten Jahre. Samba 4 ist mittlerweile sehr viel weiter, als es bei der letzten Auflage mit der Version 4.3 war. Ich werde hier die Version 4.8.3 verwenden und damit die neuesten Möglichkeiten und Techniken ansprechen. An einigen Stellen im Buch habe ich aber auch schon Neuerungen zu der Version 4.9 beschrieben. Jetzt wird sich der eine oder andere von Ihnen fragen: Warum nicht gleich alles in der Version 4.9? Der Grund ist der: Ein Buch hat immer einen gewissen Vorlauf, und die Korrektur, der Satz und der Druck brauchen auch Zeit. Auch ist es immer besser, eine etwas ausgereifere Version für ein Buch zu verwenden. Wie schon in den ersten zwei Auflagen werde ich hier immer den praktischen Bezug nehmen. Die Kapitel sind logisch aufeinander aufgebaut, Sie können aber gezielt in den einzelnen Kapiteln nach Lösungen für Ihre Aufgaben suchen.

Einige Dinge sind in dieser Auflage komplett neu. Dazu gehört, dass ich die Konfiguration der Domaincontroller jetzt auch mit Bind9 als Nameserver beschrieben habe. Auch die Einbindung des DHCP-Dienstes mit zwei Servern für ein dynamisches DNS ist neu in dieser Auflage. Die Skripte für die Verwaltung über Kommandozeile habe ich auch noch überarbeitet.

Dann habe ich ein ganz neues Kapitel ins Buch aufgenommen. Dieses Kapitel ist aufgrund von konstruktiven Anregungen einiger Leser ins Buch gekommen. Es geht dabei um Fehler, die bei der Einrichtung von Domaincontrollern und Fileservern auftreten können, wie sie sich bemerkbar machen und wie Sie sie beheben können.

Leider musste ich auch ein Kapitel aus dem Buch entfernen: jenes, das die Wiederherstellung von gelöschten Objekten im Active Directory beschreibt. Diese Funktion ist momentan so fehlerhaft, dass ich mich entschieden habe, das Kapitel, zumindest in dieser Auflage, aus dem Buch zu nehmen. Das Wiederherstellen von Objekten klappt nur, wenn Sie lediglich einen Domaincontroller in Ihrem Netz haben.

## **Danksagung**

An dieser Stelle möchte ich mich beim Hanser-Verlag bedanken, der mein Buch aufgenommen und mir freie Hand gelassen hat bei der Gestaltung und den Inhalten. Das Erstellen eines Fachbuchs ist nie die Leistung eines Einzelnen, sondern immer die Arbeit eines Teams.

Da ein Buch immer ein Projekt neben der anderen Arbeit ist, muss man als Autor immer auch Stunden der Freizeit opfern, um alles zu testen und dann schreiben zu können. Aus dem Grund möchte ich hier auch meiner Lebensgefährtin danken, dass sie mich sehr oft in aller Ruhe hat arbeiten lassen. Ohne diese Geduld wäre so ein Projekt nicht möglich.

Jetzt bleibt mir nur noch, Ihnen viel Spaß mit der neuen Auflage zu wünschen, und wie immer freue ich mich über Anregungen und Kritik.

# Inhalt

<b>Vorwort</b> .....	<b>XIII</b>
<b>1 Einleitung</b> .....	<b>1</b>
1.1 Formales .....	1
1.1.1 Kommandozeile vs. grafische Administration .....	1
1.2 Schriftarten .....	2
1.2.1 Eingabe langer Befehle .....	2
1.2.2 Screenshots .....	2
1.2.3 Internetverweise .....	3
1.2.4 Icons .....	3
1.3 Linux-Distributionen .....	3
<b>2 Grundlagen</b> .....	<b>5</b>
2.1 Das Protokoll SMB .....	5
2.2 Das Protokoll NetBIOS .....	8
<b>3 Installation von Samba</b> .....	<b>9</b>
3.1 Unterschiede zwischen den verschiedenen Samba4-Versionen .....	9
3.2 Die verschiedenen Installationsarten .....	12
3.2.1 Installation eines Domaincontrollers aus den Distributionspaketen.....	12
3.2.2 Installation eines Fileservers aus den Distributionspaketen.....	13
3.2.3 Installation aus den Quellen .....	13
3.2.4 Installation der SerNet-Pakete.....	14
3.2.5 Installation der Pakete von Louis van Belle .....	14
3.3 Installationen unter den verschiedenen Distributionen .....	14
3.3.1 Debian 9 .....	15
3.3.2 Ubuntu 18.04 .....	21
3.3.3 CentOS 7.....	26

3.3.4	Suse Leap 15 .....	32
3.3.5	Installation der SerNet-Pakete.....	37
3.3.6	Installation der Pakete von Louis van Belle.....	39
<b>4</b>	<b>Einrichten des ersten Domaincontrollers .....</b>	<b>43</b>
4.1	Allgemeines zum Einrichten des Domaincontrollers.....	43
4.2	Konfiguration des ersten Domaincontrollers (DC Teil 1) .....	45
4.2.1	Erster Start des Samba4-Servers .....	48
4.3	Konfiguration des ersten Domaincontrollers (DC Teil 2) .....	49
4.4	Testen des Domaincontrollers .....	54
4.4.1	Testen der Prozesse .....	54
4.4.2	Testen der Serverports.....	55
4.4.3	Testen des DNS-Servers .....	56
4.4.4	Testen des Verbindungsaufbaus .....	56
4.4.5	Testen des Kerberos-Servers .....	57
4.4.6	Testen des LDAP-Servers .....	59
4.5	Konfiguration des Zeitervers .....	61
<b>5</b>	<b>Die Benutzerverwaltung .....</b>	<b>63</b>
5.1	Benutzer- und Gruppenverwaltung über die Kommandozeile .....	64
5.1.1	Verwaltung von Gruppen über die Kommandozeile .....	65
5.1.2	Verwaltung von Benutzern über die Kommandozeile .....	70
5.1.3	Passwortregeln setzen .....	74
5.1.4	Ändern und Suchen von Benutzern mit den ldb-tools.....	75
5.2	Die Remote Server Administration Tools (RSAT) .....	79
5.2.1	Einrichtung der Remote Server Administration Tools(RSAT) .....	79
5.2.2	Benutzer- und Gruppenverwaltung mit den RSAT .....	82
5.3	Benutzer- und Gruppenverwaltung mit dem LAM .....	83
5.3.1	Installation des LAM.....	83
5.3.2	Konfiguration des LAM.....	85
5.3.3	Arbeiten mit dem LAM .....	89
<b>6</b>	<b>Gruppenrichtlinien .....</b>	<b>91</b>
6.1	Gruppenrichtlinien – Grundlagen.....	91
6.2	Verwaltung der GPOs mit den RSAT.....	92
6.2.1	Erste Schritte mit dem Gruppenrichtlinieneditor .....	92
6.2.2	Erstellen einer Gruppenrichtlinie.....	94
6.2.3	Verknüpfung der Gruppenrichtlinie mit einer OU .....	96
6.2.4	Verschieben der Benutzer und Gruppen.....	100

6.3	GPOs über die Kommandozeile .....	101
6.3.1	Prüfen der Gruppenrichtlinienreplikation .....	103
6.3.2	Reparieren der ACLs von Gruppenrichtlinien.....	104
<b>7</b>	<b>Verwaltung von Domaincontrollern.....</b>	<b>107</b>
7.1	Installation des neuen DCs .....	107
7.1.1	Konfiguration des DNS-Servers .....	108
7.2	Konfiguration des zweiten DCs .....	112
7.2.1	Testen des neuen Domaincontrollers .....	120
7.3	Replikation der Freigabe sysvol .....	126
7.3.1	Testen der FSMO-Rolle .....	126
7.3.2	Einrichten von rsync auf dem PDC-Master .....	127
7.3.3	Konfiguration aller anderen DCs.....	129
7.3.4	Einrichtung eines Cron-Jobs .....	131
7.3.5	Anpassen der smb.conf auf den Client-DCs.....	131
7.4	Die FSMO-Rollen .....	133
7.4.1	Verwaltung der FSMO-Rollen mit samba-tool .....	135
7.4.2	Auflisten aller Rollen.....	135
7.4.3	Transferieren der FSMO-Rollen .....	136
7.5	Entfernen eines aktiven Domaincontrollers .....	138
7.6	Entfernen eines ausgefallenen Domaincontrollers .....	139
7.7	Standorte und Subnetze .....	143
7.8	Der read-only Domaincontroller .....	145
7.8.1	Installation des RODC .....	146
7.8.2	Verwalten der Benutzer auf einem RODC .....	151
<b>8</b>	<b>Ausfallsicherer DHCP-Server .....</b>	<b>155</b>
8.1	Der erste DHCP-Server.....	155
8.1.1	Vorbereitungen für den ersten DHCP-Server .....	155
8.1.2	Konfiguration des ersten DHCP-Servers .....	160
8.1.3	Konfiguration des zweiten DHCP-Servers .....	162
8.1.4	Testen der DHCP-Server .....	168
<b>9</b>	<b>Zusätzliche Server in der Domäne .....</b>	<b>173</b>
9.1	Einrichten eines Linux-Fileservers .....	173
9.2	ID-Mapping .....	173
9.3	Einrichten des Fileservers .....	174
9.3.1	Grundkonfiguration des Fileservers .....	175
9.4	Konfiguration über die Registry.....	178
9.5	Die Registry-Datenbank .....	180
9.6	Das Kommando net conf .....	183

<b>10</b>	<b>Verwaltung von Freigaben</b> .....	<b>189</b>
10.1	Freigabenverwaltung über die Datei smb.conf .....	189
10.2	Verwaltung der Freigaben über die Registry .....	191
10.2.1	Erstellen einer Freigabe in der Registry .....	193
10.2.2	Zugriff auf eine Freigabe aus der Registry .....	195
10.2.3	Erweitern einer Freigabe in der Registry .....	197
10.2.4	Sichern der Freigabeeinstellungen aus der Registry .....	198
10.2.5	Löschen einer Freigabe aus der Registry .....	198
10.2.6	Wiederherstellen von Freigaben in der Registry .....	199
10.3	Die Freigabe der Heimatverzeichnisse.....	199
10.3.1	Einrichtung der Freigabe für servergespeicherte Profile .....	202
10.4	Allgemeine Freigaben .....	205
10.4.1	Administrative Freigaben .....	205
10.4.2	Erstellen einer Freigabe unter Windows .....	206
10.4.3	Eine Freigabe mit hide unreadable .....	213
10.4.4	Eine Freigabe mit Netzwerkpapierkorb .....	215
10.5	Zuweisung der Freigaben über Gruppenrichtlinien .....	217
10.5.1	Anlegen der Gruppenrichtlinie.....	217
10.5.2	Zuordnung der Gruppenrichtlinie.....	221
10.5.3	Testen auf der Konsole .....	224
10.6	Samba und das Distributed File System (DFS) .....	226
10.6.1	Grundlagen DFS.....	226
10.6.2	Samba4 als DFS-Proxy.....	226
10.6.3	Einrichtung einer DFS-Freigabe mit DFS-Link .....	227
<b>11</b>	<b>Das Dateisystem</b> .....	<b>229</b>
11.1	Dateisystemberechtigungen .....	229
11.1.1	Vererbung der Rechte.....	229
11.1.2	Aufhebung der Vererbung.....	233
11.1.3	Ändern des Besitzers.....	237
11.2	Dateisystemquotas .....	239
11.2.1	Installation und Aktivierung der Quotas .....	240
11.2.2	Quota-Einträge verwalten .....	241
<b>12</b>	<b>Verwaltung von Clients in der Domäne</b> .....	<b>247</b>
12.1	Hinzufügen eines Windows-Clients in die Domäne .....	247
12.2	Hinzufügen eines Linux-Clients zur Domäne .....	248
12.2.1	Installation und Konfiguration .....	249
12.2.2	Konfiguration des winbind .....	250

12.3	Zugriff von Linux-Clients auf Samba-Freigaben .....	254
12.3.1	Caching der Anmeldeinformationen .....	257
12.4	Sssd versus winbind .....	258
12.4.1	Installation und Konfiguration des sssd .....	259
12.4.2	Abfrage des sssd .....	261
<b>13</b>	<b>Cluster mit CTDB .....</b>	<b>263</b>
13.1	Vorbereiten der Systeme .....	263
13.2	GlusterFS.....	264
13.2.1	Clients und Protokolle .....	265
13.2.2	Die verschiedenen Modi .....	266
13.2.3	Installation der Gluster-Pakete .....	267
13.2.4	Konfiguration der Knoten .....	268
13.2.5	Einrichten der Bricks .....	269
13.2.6	Einrichtung des Volumes.....	270
13.2.7	Verwenden des Volumes .....	272
13.2.8	Gluster-Snapshots .....	275
13.2.9	Erweitern eines Volumes .....	279
13.2.10	Austauschen eines Knotens.....	281
13.3	CTDB .....	284
13.3.1	Installation der Software .....	285
13.3.2	Installation des Kerberos-Clients .....	285
13.3.3	Einträge im DNS-Server erstellen .....	285
13.3.4	Konfiguration von CTDB .....	286
13.3.5	Erstellen der Konfiguration für Samba .....	290
13.3.6	Starten und Testen des CTDB-Cluster.....	292
13.3.7	Das Kommando onnode .....	294
13.3.8	Benutzer und Freigaben.....	296
<b>14</b>	<b>Schemaerweiterung .....</b>	<b>303</b>
14.1	Vorbereitung der Installation .....	303
14.2	Zusätzliche Attribute erstellen .....	304
<b>15</b>	<b>Sicherung der Datenbanken.....</b>	<b>309</b>
15.1	Sicherung der Datenbanken .....	309
15.2	Wiederherstellung der Datenbanken .....	312

<b>16 Vertrauensstellungen</b> .....	<b>315</b>
16.1 Vertrauensstellung zwischen zwei Forests .....	316
16.1.1 Die Einrichtung der Domänen .....	316
16.2 Einrichten eines DNS-Proxys .....	317
16.2.1 Installation und Konfiguration .....	317
16.2.2 Umstellung an den Domaincontrollern.....	318
16.3 Einrichten der Vertrauensstellungen.....	321
16.4 Der Windows-Client.....	326
16.5 Der Linux-Client .....	327
16.6 Verwaltung von Namespaces .....	331
16.7 Einrichtung von Namespaces .....	331
<b>17 Samba4 über die Kommandozeile verwalten</b> .....	<b>335</b>
17.1 Das Kommando samba-tool .....	336
17.1.1 samba-tool dbcheck .....	336
17.1.2 samba-tool drs.....	337
17.1.3 samba-tool dsacl .....	341
17.1.4 samba-tool fsmo .....	341
17.1.5 samba-tool gpo .....	341
17.1.6 samba-tool group .....	341
17.1.7 samba-tool ldapcmp.....	342
17.1.8 samba-tool ntacl .....	343
17.1.9 samba-tool sites .....	343
17.1.10 samba-tool user .....	343
17.1.11 Zusammenfassung.....	344
17.2 Das Kommando net .....	344
17.2.1 net rpc .....	344
17.2.2 net ads .....	344
17.2.3 net status .....	346
17.2.4 Zusammenfassung.....	346
17.3 Die smb-Kommandos.....	346
17.3.1 smbclient.....	347
17.3.2 smbstatus .....	351
17.3.3 smbtree .....	351
17.3.4 Zusammenfassung.....	351
17.4 Skripte.....	352
17.4.1 Anlegen von Benutzern .....	352
17.4.2 Ändern von Benutzern .....	355
17.4.3 Entfernen von gelöschten Objekten .....	359
17.5 Fazit zur Kommandozeile .....	362

<b>18 Die Migration einer bestehenden Domäne .....</b>	<b>363</b>
18.1 Migration von Samba .....	363
18.1.1 Migration einer tdb-Backend-Domäne .....	364
18.1.2 Migration der Benutzer und Gruppen aus einem openLDAP .....	370
18.2 Migration eines Windows-Servers .....	374
18.2.1 DNS-Einträge erstellen und prüfen .....	375
18.2.2 Global Catalog umziehen .....	375
18.2.3 Übertragung der FSMO-Rollen .....	376
18.2.4 Prüfen der Gruppenrichtlinien .....	378
<b>19 Samba4 als Printserver .....</b>	<b>379</b>
19.1 Vorbereitungen .....	379
19.1.1 Privilegien für die Druckerverwaltung .....	380
19.2 Vorbereitungen des CUPS-Drucksystems .....	381
19.3 Einrichten der Freigaben .....	383
19.3.1 Einrichten eines Druckers mit CUPS .....	385
19.4 Hochladen der Druckertreiber .....	388
19.5 Zuordnung des Druckertreibers .....	390
19.6 Verbinden mit dem Drucker .....	393
19.7 Gruppenrichtlinien für Drucker .....	393
19.7.1 Gruppenrichtlinien für unsignierte Druckertreiber .....	394
19.7.2 Gruppenrichtlinie für die Druckerzuweisung .....	395
<b>20 WINS und Samba4 .....</b>	<b>397</b>
20.1 Einrichten des Knotentyps .....	398
20.2 Konfiguration des WINS-Servers .....	400
20.3 Einrichten der Replikation .....	400
20.4 Backup und Recovery der WINS-Daten .....	401
20.5 Testen der WINS-Server .....	402
<b>21 Einrichtung von ssh .....</b>	<b>405</b>
21.1 Einrichtung des ssh-Servers .....	405
21.2 Einrichten des Clients .....	406
<b>22 Firewall und Sicherheit .....</b>	<b>407</b>
22.1 Firewall .....	407
22.1.1 Ports auf einem Domaincontroller .....	407
22.1.2 Ports auf einem Fileserver .....	408
22.2 Sicherheit .....	411
22.2.1 Absichern des Betriebssystems .....	411
22.2.2 Absichern des Samba-Dienstes .....	412

<b>23 Hilfe zur Fehlersuche .....</b>	<b>415</b>
23.1 Installations- und Konfigurationsfehler .....	416
23.1.1 Der erste Domaincontroller .....	416
23.1.2 Der zweite Domaincontroller .....	419
23.1.3 Replikation der SYSVOL-Freigabe .....	420
23.1.4 Der Fileserver .....	422
23.2 Fehler im laufenden Betrieb.....	426
23.2.1 Fehler bei der Replikation.....	426
23.2.2 Berechtigungsprobleme bei den ACLs .....	427
23.2.3 Ungleiche Zeit auf den Domaincontrollern .....	428
<b>24 Jetzt alles zusammen .....</b>	<b>431</b>
24.1 Das Unternehmen .....	431
24.2 Planung des Active Directorys .....	433
24.3 Installation des ersten Domaincontrollers .....	434
24.4 Einrichtung des Zeitservers .....	435
24.5 Installation des zweiten Domaincontrollers .....	436
24.5.1 Replikation der Freigabe sysvol .....	437
24.6 Konfiguration von GlusterFS .....	439
24.7 Konfiguration von CTDB .....	442
24.8 Konfiguration von Samba .....	444
24.9 Einrichten der administrativen Freigaben .....	447
24.10 Einrichten des Druckservers .....	448
24.11 Nachwort zum Workshop.....	451
<b>Stichwortverzeichnis .....</b>	<b>453</b>

# 4

## Einrichten des ersten Domaincontrollers

Nachdem ich die Installation im letzten Kapitel ausführlich beschrieben habe, soll jetzt der erste Samba Active-Directory-Domaincontroller eingerichtet werden. Dabei geht es nicht nur um die reine Konfiguration, sondern auch um einige Tests, mit denen Sie die Funktion des Domaincontrollers überprüfen können.

Für Samba4 wird, wie auch bei einem Windows-Domaincontroller, auf jeden Fall ein Kerberos - Server für die Authentifizierung der Benutzer benötigt. Dieser wird von Samba4 bereitgestellt.



### Hinweis

Zurzeit wird hier noch der Heimdal-Kerberos verwendet.

Zusätzlich benötigt Samba4 auf jeden Fall einen DNS-Server, der nicht nur zur Auflösung der Hostnamen dient, sondern auch zur Auflösung der benötigten Dienste in der Domäne. Der DNS-Server kann entweder von Samba4 bereitgestellt werden oder Sie können einen Bind9-Nameserver verwenden. Im Gegensatz zum internen Nameserver unterstützt der Bind9 die Funktion `round robin`, um eventuell unterschiedliche IP-Adressen der Server und Dienste in verschiedenen Reihenfolge an die Clients zu geben.

### ■ 4.1 Allgemeines zum Einrichten des Domaincontrollers

Für die Konfiguration und die Administration eines Samba4-Servers steht Ihnen das Kommando `samba-tool` zur Verfügung. Mit diesem Kommando können Sie die Domäne einrichten und verwalten, aber auch später die Benutzer und Gruppen sowie die Gruppenrichtlinien und den DNS-Server verwalten. Wobei die Verwaltung der DNS-Einträge unabhängig von dem verwendeten DNS-Server ist. Es spielt keine Rolle, ob Sie den internen DNS-Server oder Bind9-DNS-Server verwenden.

In Listing 4.1 sehen Sie eine Übersicht über die Aufgaben in Ihrer Domäne, die Sie mit dem Kommando `samba-tool` durchführen können:

**Listing 4.1** Ein Testlisting

```
root@sambabuch:~# samba-tool
Usage: samba-tool <subcommand>
```

Main samba administration tool.

## Options:

```
-h, --help          show this help message and exit
```

## Version Options:

```
-V, --version      Display version number
```

## Available subcommands:

```
dbcheck      - Check local AD database for errors.
delegation   - Delegation management.
dns          - Domain Name Service (DNS) management.
domain       - Domain management.
drs          - Directory Replication Services (DRS) management.
dsacl       - DS ACLs manipulation.
fsmo         - Flexible Single Master Operations (FSMO) \
              roles management.
gpo          - Group Policy Object (GPO) management.
group        - Group management.
ldapcmp      - Compare two ldap databases.
ntacl       - NT ACLs manipulation.
processes    - List processes (to aid debugging on systems \
              without setproctitle).
rodc         - Read-Only Domain Controller (RODC) management.
sites        - Sites management.
spn          - Service Principal Name (SPN) management.
testparm    - Syntax check the configuration file.
time        - Retrieve the time on a server.
user         - User management.
visualize    - Produces graphical representations of Samba \
              network state
```

For more help on a specific subcommand, please type: \  
samba-tool <subcommand> (-h|--help)

Immer wenn Sie das Kommando *samba-tool* mit einem der Subkommandos angeben, ohne weitere Parameter zu verwenden, bekommen Sie eine Hilfe zu dem entsprechenden Subkommando angezeigt.

Bevor Sie die Konfiguration des Domaincontrollers mit dem Kommando *samba-tool domain provision* durchführen, müssen Sie erst die dafür benötigten Informationen besorgen. Bei der Konfiguration des Domaincontrollers werden sie abgefragt. Die folgenden Informationen sollten Sie für die Konfiguration bereithalten:

- **Den Realm:**

Der Realm wird für den Kerberos-Server benötigt. Der Realm wird bei der Einrichtung des DNS-Servers auch als DNS-Domainname verwendet.

- **Den NetBIOS-Domainname:**

Der NetBIOS-Domainname ist die Adresse, über die der Server per NetBIOS-Protokoll erreichbar ist. Der NetBIOS-Name sollte immer der erste Teil des Realms sein.

- **Die Funktion des Servers:**

Sie sollten wissen, welche Rolle der Server in der Domäne übernehmen soll. In unserem Fall übernimmt er die Rolle des Domaincontrollers.

- **Welcher DNS-Server soll verwendet werden?**

Sie müssen wissen, ob Sie den internen DNS-Server von Samba4 verwenden wollen oder einen Bind9-Server.

- **Die IP-Adresse eines eventuell benötigten DNS-Forwarders:**

An diese IP-Adresse werden alle DNS-Anfragen weitergeleitet, die nicht zur eigenen Zone gehören. Ohne einen Forwarder ist die Namensauflösung der Namen im Internet nicht möglich. Sie können hier auch mehr als eine IP-Adresse angeben. Die einzelnen Server werden durch Leerzeichen voneinander getrennt.

Bevor Sie das Provisioning starten, sollten Sie einen Blick auf alle möglichen Optionen werfen, indem Sie das Kommando `samba-tool domain provision -help` eingeben. Dort finden Sie eine Option, auf die ich hier gesondert eingehen möchte: die Option `-use-rfc2307`. Wenn Sie diese Option beim Provisioning mit angeben, dann werden spezielle Unix-Attribute beim Anlegen von Benutzern und Gruppen mit erzeugt. Es handelt sich, unter anderem, um die Attribute `UID` und `GID`. Diese Attribute können Sie dann bei den Benutzern mit angeben, wenn Sie einen neuen Benutzer oder eine neue Gruppe anlegen. Die Nummerierung der Benutzer und Gruppen müssen Sie aber selbst vornehmen. Im Gegensatz zur Vergabe der SID eines Objekts werden diese Attribute nicht automatisch vergeben. Hier im Buch werde ich Samba immer ohne diese Attribute provisionieren, da die Anmeldung und einheitlichen IDs der Posix-User und Gruppen auch über die SID realisiert werden können. Der Vorteil ist, dass Sie sich bei der SID nicht selbst um die Nummerierung kümmern müssen.

**Hinweis**

Wenn Sie die Unix-Attribute verwenden wollen, müssen Sie dieses bei der Provisionierung angeben, eine nachträgliche Einbindung ist nicht so einfach realisierbar.

## ■ 4.2 Konfiguration des ersten Domaincontrollers (DC Teil 1)

Im ersten Teil der Einrichtung eines Samba-Domaincontrollers geht es um die Einrichtung mit dem internen DNS-Server. Im zweiten Teil folgt dann die Einrichtung unter Verwendung des Bind9. Immer wenn Sie für die Lastverteilung einen DNS-Server nutzen wollen, müssen Sie auf jeden Fall den Bind9 als Nameserver verwenden da nur der Bind9 die Funktion Round-Robin unterstützt. In Listing 4.2 sehen Sie den Ablauf der Konfiguration des ersten Domaincontrollers:

**Listing 4.2** Provisioning mit internem DNS-Server

```

root@sambabuch:~# samba-tool domain provision
Realm [EXAMPLE.NET]:
Domain [EXAMPLE]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) \
[SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) \
[8.8.8.8]:
Administrator password:
Retype password:
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.56.31
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

Adding DomainDN: DC=example,DC=net
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=example,DC=net
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba AD has been \
generated at /var/lib/samba/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!
Once the above files are installed, your Samba AD server \

```

```

will be ready to use
Server Role:      active directory domain controller
Hostname:        sambabuch
NetBIOS Domain:  EXAMPLE
DNS Domain:      example.net
DOMAIN SID:      S-1-5-21-1129951053-411964844-750776748

```



#### Hinweis

Das Passwort des Administrators hat unter Samba4, im Gegensatz zu Windows, ein Ablaufdatum.

Wie Sie in dem Listing sehen, wird jetzt der interne DNS verwendet. Aus diesem Grund brauchen Sie hier keine Konfiguration des Nameservers vorzunehmen. Die gesamte Konfiguration wird von Samba 4 selbst durchgeführt – genau wie später die Replikation zur Ausfallsicherheit auf einen weiteren Domaincontroller.

#### Hinweis

Wollen Sie in Zukunft *samba-tool* mit der Authentifizierung über Kerberos verwenden, müssen Sie für alle Debian-basierten Distributionen das Paket *heimdal-clients* installieren. Bei Suse oder CentOS befinden sich die benötigten Programme in dem Paket *krb5-client*.

#### Hinweis

Stellen Sie sicher, dass jetzt in der Datei */etc/resolv.conf* die IP-Adresse des Servers selbst eingetragen ist. Sonst wird nicht der eigene DNS für die Auflösung der Hostnamen und Dienste in der AD-Domäne verwendet. Ohne diesen Eintrag sind die Dienste der Domäne nicht erreichbar. Alle Clients in der Domäne müssen später ebenfalls den Domaincontroller als DNS-Server verwenden, um sich in der Domäne authentifizieren zu können.

Sorgen Sie über die entsprechenden Konfigurationsdateien Ihrer Distribution für die dauerhafte Einstellung des DNS-Servers. Achten Sie auch darauf, dass Ihr Domaincontroller einer festen IP-Adresse besitzt. Stellen Sie sicher, dass der Domaincontroller nach dem Systemstart automatisch gestartet wird. Nach dem Provisioning wird automatisch eine */etc/samba/smb.conf* erzeugt. Listing 4.3 zeigt Ihnen die Datei:

#### Listing 4.3 Die neue smb.conf

```

# Global parameters
[global]
    dns forwarder = 8.8.8.8
    netbios name = SAMBABUCH
    realm = EXAMPLE.NET
    server role = active directory domain controller
    workgroup = EXAMPLE

```

```
[netlogon]
    path = /var/lib/samba/sysvol/example.net/scripts
    read only = No

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No
```

Die beiden Freigaben `netlogon` und `sysvol` werden auf jedem Domaincontroller benötigt und daher auch beim Provisioning automatisch erzeugt.

## 4.2.1 Erster Start des Samba4-Servers

Da Samba4 verschiedene Rollen in einem Netzwerk übernehmen kann, müssen auch verschiedene Prozesse beim Start des Servers gestartet werden. Da alle gängigen Distributionen heute über `Systemd` gestartet werden, müssen Sie jetzt das `Systemd`-Skript für die Funktion des Domaincontrollers aktivieren und starten. Bei Debian müssen Sie seit der Version 9 die Schritte aus Listing 4.4 durchführen, um einen Domaincontroller starten zu können. Diese Schritte müssen Sie auch durchführen, wenn Sie den Domaincontroller auf einem Ubuntu 18.04 einrichten wollen. Da keine andere Distribution derzeit die Funktion eines Domaincontrollers unterstützt, gehe ich hier nicht weiter auf andere Distributionen ein.

### Listing 4.4 System für den Domaincontroller einrichten

```
root@sambabuch:~# systemctl stop smbdc nmbd winbind

root@sambabuch:~# systemctl disable smbdc nmbd winbind
Synchronizing state of smbdc.service with SysV service script \
    with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable smbdc
Synchronizing state of nmbd.service with SysV service script \
    with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable nmbd
Synchronizing state of winbind.service with SysV service script \
    with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable winbind

root@sambabuch:~# systemctl unmask samba-ad-dc
Removed /etc/systemd/system/samba-ad-dc.service.

root@sambabuch:~# systemctl start samba-ad-dc

root@sambabuch:~# systemctl enable samba-ad-dc
Synchronizing state of samba-ad-dc.service with SysV service script \
    with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable samba-ad-dc
```

Jetzt sollten Sie das System einmal neu starten, um sicher zu sein, dass alle Dienste auch nach einem Neustart richtig gestartet werden. Nach dem Neustart können Sie mit den Tests des Domaincontrollers aus Abschnitt 4.4 fortfahren.

## ■ 4.3 Konfiguration des ersten Domaincontrollers (DC Teil 2)

Im zweiten Teil geht es um die Einrichtung des Domaincontrollers mit dem Bind9 als DNS-Backend. Diesen Teil benötigen Sie nur, wenn Sie den Bind9 als Nameserver verwenden wollen. Den Bind9 sollten Sie immer dann verwenden, wenn Sie später einen Cluster als Fileserver nutzen oder weitere Zonen für andere Dienste auf demselben Nameserver einrichten wollen. Wenn Sie den Bind9 verwenden wollen, müssen Sie vor dem Provisioning auf jeden Fall die drei Pakete `bind9`, `bind9utils` und `dnsutils` installieren.



### Hinweis

Auch hier gilt: Wenn bei der Installation der Samba-Pakete eine `smb.conf` erzeugt wurde, müssen Sie diese auf jeden Fall löschen, bevor Sie das Provisioning durchführen.

Nachdem Sie Samba installiert haben, können Sie jetzt das Provisioning, so wie in Listing 4.5, durchführen. Achten Sie bei den Abfragen darauf, jetzt als *DNS-Backend* den Wert `BIND9_DLZ` anzugeben. Der Wert muss großgeschrieben werden.

### Listing 4.5 Provisioning mit bind9

```
root@sambabuch:~# samba-tool domain provision
Realm [EXAMPLE.NET]:
Domain [EXAMPLE]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) \
[SAMBA_INTERNAL]: BIND9_DLZ
Administrator password:
Retype password:
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.56.31
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

Adding DomainDN: DC=example,DC=net
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=example,DC=net
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
See /var/lib/samba/bind-dns/named.conf for an example \
    configuration include file for BIND
and /var/lib/samba/bind-dns/named.txt for further \
    documentation required for secure DNS updates
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba AD has been \
    generated at /var/lib/samba/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!
Once the above files are installed, your Samba AD server \
    will be ready to use
Server Role:      active directory domain controller
Hostname:        sambabuch
NetBIOS Domain:  EXAMPLE
DNS Domain:      example.net
DOMAIN SID:      S-1-5-21-1129951053-411964844-750776748

```

Im Listing sehen Sie die zwei in Listing 4.6 herausgestellten Zeilen:

**Listing 4.6** Hinweis auf die DNS-Konfiguration

```

See /var/lib/samba/bind-dns/named.conf for an example \
    configuration include file for BIND
and /var/lib/samba/bind-dns/named.txt for further \
    documentation required for secure DNS updates

```

Diese beiden Zeilen geben Ihnen eine Konfigurationsdatei und eine Datei mit genauen Installationshinweisen. In den nächsten Schritten werde ich Ihnen zeigen, wie Sie jetzt den Bind9 konfigurieren müssen.

Nachdem Sie das Provisioning durchgeführt haben, könne Sie jetzt die Datei `/etc/bind/named.conf.options` anpassen. In Listing 4.7 sehen Sie die geänderten Zeilen und Bereiche:

**Listing 4.7** Einstellungen in der `named.conf.options`

```
forwarders {
    1.1.1.1;
};
tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
```

Anstelle der IP-Adresse `1.1.1.1` können Sie auch den DNS-Server Ihres Providers oder einen anderen DNS-Server in Ihrem Netz als Forwarder eintragen. Da der DNS-Server später Änderungen an der AD-Datenbank durchführen muss, muss er sich über einen Kerberos-Schlüssel authentifizieren. Mit dem Parameter `tkey-gssapi-keytab` definieren Sie die Kerberos-Schlüsseldatei. Diese Datei wurde beim Provisioning erstellt. Jetzt müssen Sie dem Bind9 noch die Zonen-Dateien übergeben. Da Sie hier keine statischen Zonen im üblichen Format einrichten, sondern auf Zonen im Active Directory zugreifen, müssen Sie in der Datei `/etc/bind/named.conf.local` nur eine Zeile eintragen. In Listing 4.8 sehen Sie die Zeile:

**Listing 4.8** Änderungen an der Datei `named.conf.local`

```
include "/var/lib/samba/bind-dns/named.conf";
```

Diese Zeile verweist auf eine Datei, die beim Provisioning erstellt wurde. Wenn Sie sich diese Datei einmal ansehen, werden Sie feststellen, dass dort nur eine Zeile aktiv ist, alle anderen Zeilen sind auskommentiert. Es ist immer nur die Zeile aktiv, die auf die Version des Bind9 verweist, der bei Ihnen auf dem System installiert ist.

Damit ist die Konfiguration des Bind9 abgeschlossen. Je nach verwendeter Distribution und verwendeter Samba-Installationsart müssen Sie eventuell noch Dateisystemrechte anpassen, sodass der Bind9 auch Änderungen an der Datenbank durchführen kann. In Listing 4.9 sehen Sie die Rechte, die Sie prüfen müssen, und wie sie gesetzt sein müssen:

**Listing 4.9** Prüfen der Berechtigungen

```
root@sambabuch:~# ls -ld /var/lib/samba/private/
drwxr-xr-x 5 root root 4096 Jun 17 16:12 \
/var/lib/samba/private/

root@sambabuch:~# ls -l /var/lib/samba/private/dns.keytab
-rw-r----- 2 root bind 777 Jun 17 16:12 \
/var/lib/samba/private/dns.keytab

root@sambabuch:~# ls -ld /var/lib/samba/bind-dns/
drwxrwx--- 3 root bind 4096 Jun 17 16:12 /var/lib/samba/bind-dns/

root@sambabuch:~# ls -l /var/lib/samba/bind-dns/
insgesamt 16
drwxrwx--- 3 root bind 4096 Jun 17 16:12 dns
-rw-r----- 2 root bind 777 Jun 17 16:12 dns.keytab
-rw-r--r-- 1 root root 781 Jun 17 16:12 named.conf
-rw-r--r-- 1 root root 2092 Jun 17 16:12 named.txt
```

```

root@sambabuch:~# ls -l /var/lib/samba/bind-dns/dns
insgesamt 2952
-rw-rw---- 1 root bind 3014656 Jun 17 16:12 sam.ldb
drwxrwx--- 2 root bind  4096 Jun 17 16:12 sam.ldb.d

root@sambabuch:~# ls -l /var/lib/samba/bind-dns/dns/sam.ldb.d/
insgesamt 24096
-rw-rw---- 1 root bind 6807552 Jun 17 16:12 \
    CN=CONFIGURATION,DC=EXAMPLE,DC=NET.ldb
-rw-rw---- 1 root bind 7237632 Jun 17 16:12 \
    CN=SCHEMA,CN=CONFIGURATION,DC=EXAMPLE,DC=NET.ldb
-rw-rw---- 2 root bind 4247552 Jun 17 16:12 \
    DC=DOMAINDNSZONES,DC=EXAMPLE,DC=NET.ldb
-rw-rw---- 1 root bind 1286144 Jun 17 16:12 \
    DC=EXAMPLE,DC=NET.ldb
-rw-rw---- 2 root bind 4247552 Jun 17 16:12 \
    DC=FORESTDNSZONES,DC=EXAMPLE,DC=NET.ldb
-rw-rw---- 2 root bind  831488 Jun 17 16:12 metadata.tdb

```

Wichtig sind hier die Berechtigungen für die Gruppe *bind*. Sollte eine oder mehrere der Berechtigungen nicht stimmen, müssen Sie sie anpassen.



#### Hinweis

Bei den Paketen aus der Distribution befinden sich die DNS-Informationen und Datenbanken im Verzeichnis `/var/lib/samba/private/dns`.

Wenn Sie Ubuntu 18.04 als Domaincontroller einsetzen, müssen Sie jetzt noch Apparmor für den Bind9 konfigurieren. Dazu erweitern Sie die Datei `/etc/apparmor.d/usr.sbin.named` um die Zeilen aus Listing 4.10.

#### Listing 4.10 Änderungen in Apparmor

```

/var/lib/samba/lib/** rm,
/var/lib/samba/private/dns/** rwmk,
/var/lib/samba/private/dns.keytab r,
/var/lib/samba/private/named.conf r,
/var/lib/samba/private/dns/** rwk,
/usr/lib/**/samba/bind9/** rmk,
/usr/lib/**/samba/gensec/* rmk,
/usr/lib/**/samba/ldb/** rmk,
/usr/lib/**/ldb/modules/ldb/** rmk,
/var/lib/samba/ntp_signd/socket rw,

```

Ohne diese Änderungen wird der Bind9 nicht starten, da der Dienst nicht auf die Dateien zugreifen darf.

Jetzt können Sie den Bind9 mit dem Kommando `systemctl restart bind9` neu starten. Prüfen Sie anschließend in der Datei `/var/log/syslog`, ob Sie die Zeilen aus Listing 4.11 sehen:

**Listing 4.11** Erster Test des Bind9

```
root@sambabuch:~# systemctl restart bind9

root@sambabuch:~# tail -n 200 /var/log/syslog
...
Jun 17 16:41:55 sambabuch named[1339]: Loading 'AD DNS Zone' \
    using driver dlopen
Jun 17 16:41:55 sambabuch named[1339]: samba_dlz: started for \
    DN DC=example,DC=net
Jun 17 16:41:55 sambabuch named[1339]: samba_dlz: starting \
    configure
Jun 17 16:41:55 sambabuch named[1339]: samba_dlz: configured \
    writeable zone 'example.net'
Jun 17 16:41:55 sambabuch named[1339]: samba_dlz: configured \
    writeable zone '_msdcs.example.net'
...
```

Erst wenn Sie diese Zeilen sehen, können Sie mit der weiteren Einrichtung des Domaincontrollers fortfahren.

Damit auf einem Debian- oder Ubuntu-System auch die richtige Dienste gestartet werden, müssen Sie noch die Konfiguration des Systemd so wie in Listing 4.12 anpassen:

**Listing 4.12** Anpassen des Systemd

```
root@sambabuch:~# systemctl stop smbd nmbd winbind

root@sambabuch:~# systemctl disable smbd nmbd winbind
Synchronizing state of smbd.service with SysV service script \
    with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable smbd
Synchronizing state of nmbd.service with SysV service script \
    with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable nmbd
Synchronizing state of winbind.service with SysV service script \
    with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable winbind

root@sambabuch:~# systemctl unmask samba-ad-dc
Removed /etc/systemd/system/samba-ad-dc.service.

root@sambabuch:~# systemctl start samba-ad-dc

root@sambabuch:~# systemctl enable samba-ad-dc
Synchronizing state of samba-ad-dc.service with SysV service script \
    with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable samba-ad-dc
```



### Wichtig

Stellen Sie vor dem folgenden Systemstart sicher, dass die eigene IP-Adresse des Servers als DNS-Server als Resolver eingetragen ist.

Um sicherzugehen, dass alle Dienste auch nach Neustart des System ordnungsgemäß starten, sollten Sie jetzt das System einmal neu starten. Im Anschluss können Sie dann mit den Tests beginnen.

## ■ 4.4 Testen des Domaincontrollers

Jetzt wird es Zeit, die einzelnen Funktionen des Domaincontrollers zu testen, bevor Sie mit den weiteren Schritten fortfahren. Testen Sie alle Funktionen genau, um sicher zu sein, dass Sie alles richtig konfiguriert haben. Wenn Sie jetzt einen Fehler finden, lässt dieser sich einfacher beseitigen, als wenn Sie schon eine komplette Domäne mit weiteren Domaincontrollern, Fileservern und Clients eingerichtet haben.

### 4.4.1 Testen der Prozesse

Im ersten Test soll sichergestellt werden, dass auch alle Prozesse gestartet wurden. In Listing 4.13 sehen Sie die Tests mit den zu erwartenden Ergebnissen:

**Listing 4.13** Testen der Prozesse

```
root@sambabuch:~# ps ax | grep samba
 327 ?      Ss      0:00 avahi-daemon: running [sambabuch.local]
 497 ?      Ss      0:00 samba: root process
 548 ?      S       0:00 samba: task[s3fs_parent]
 549 ?      S       0:00 samba: task[dcesrv]
 550 ?      S       0:00 samba: task[nbtd]
 551 ?      S       0:00 samba: task[wrepl]
 552 ?      S       0:00 samba: task[ldapsrv]
 553 ?      S       0:00 samba: task[cldapd]
 554 ?      S       0:00 samba: task[kdc]
 555 ?      S       0:00 samba: task[dreplsrv]
 556 ?      S       0:00 samba: task[winbindd_parent]
 557 ?      S       0:00 samba: task[ntp_signd]
 558 ?      S       0:00 samba: task[kccsrv]
 559 ?      S       0:00 samba: tfork waiter process
 561 ?      S       0:00 samba: tfork waiter process
 563 ?      S       0:00 samba: task[dnupdate]

root@sambabuch:~# ps ax | grep named
 494 ?      Ssl     0:00 /usr/sbin/named -f -u bind
```

## 4.4.2 Testen der Serverports

Testen Sie als Erstes mit dem Kommando `ss`, ob alle Ports für Samba 4 geöffnet wurden und somit die entsprechenden Dienste bereitgestellt werden. In Listing 4.14 sehen Sie den Test:

**Listing 4.14** Testen der Ports

```
root@sambabuch:~# ss -tln | awk '{print $1" "$2" "$3" "$4}'
State Recv-Q Send-Q Local
LISTEN 0 10 *:464
LISTEN 0 10 192.168.56.31:53
LISTEN 0 10 10.0.2.15:53
LISTEN 0 10 127.0.0.1:53
LISTEN 0 128 *:22
LISTEN 0 5 127.0.0.1:631
LISTEN 0 10 *:88
LISTEN 0 128 127.0.0.1:953
LISTEN 0 10 *:636
LISTEN 0 50 *:445
LISTEN 0 10 *:49152
LISTEN 0 10 *:49153
LISTEN 0 10 *:49154
LISTEN 0 10 *:3268
LISTEN 0 10 *:3269
LISTEN 0 10 *:389
LISTEN 0 10 *:135
LISTEN 0 50 *:139
LISTEN 0 10 :::464
LISTEN 0 10 :::53
LISTEN 0 128 :::22
LISTEN 0 5 :::1:631
LISTEN 0 10 :::88
LISTEN 0 128 :::1:953
LISTEN 0 10 :::636
LISTEN 0 50 :::445
LISTEN 0 10 :::49152
LISTEN 0 10 :::49153
LISTEN 0 10 :::49154
LISTEN 0 10 :::3268
LISTEN 0 10 :::3269
LISTEN 0 10 :::389
LISTEN 0 10 :::135
LISTEN 0 50 :::139
```



### Hinweis

Da hier nur die Portnummer interessant sind, habe ich die Ausgabe gekürzt.

In der Liste sehen Sie anhand der geöffneten Ports, dass die Dienste `domain` für den DNS-Server, `ldap/ldaps` für den LDAP-Server und `kerberos/kpasswd` für den Kerberos-Server bereitgestellt werden. Sie sehen auch, dass alle Dienste sowohl über IPv4 als auch über IPv6 erreichbar sind.

### 4.4.3 Testen des DNS-Servers

Im nächsten Test überprüfen Sie, ob Ihr Domaincontroller die Einstellungen für den Nameserver richtig übernommen hat und ob der Nameserver die Namen richtig auflöst. In Listing 4.15 sehen Sie verschiedene Tests:

**Listing 4.15** Die verschiedenen DNS-Tests

```
root@sambabuch:~# host sambabuch
sambabuch.example.net has address 192.168.56.31

root@sambabuch:~# host -t SRV _kerberos._tcp.example.net
_kerberos._tcp.example.net has SRV record 0 100 88 \
    sambabuch.example.net.

root@sambabuch:~# host -t SRV _ldap._tcp.example.net
_ldap._tcp.example.net has SRV record 0 100 389 \
    sambabuch.example.net.

root@sambabuch:~# host -t SRV _gc._tcp.example.net
_gc._tcp.example.net has SRV record 0 100 3268 \
    sambabuch.example.net.
```

Mit dem ersten Test prüfen Sie, ob Ihr Resolver den richtigen DNS-Server verwendet, indem Sie die IP-Adresse des Domaincontrollers auflösen. In den drei anderen Tests prüfen Sie, ob Ihr DNS-Server auch die Dienste LDAP, Kerberos und `global catalog` auflösen kann. Dieses ist zwingend erforderlich, da später die Clients in der Domäne diese Dienste immer über DNS suchen werden.

### 4.4.4 Testen des Verbindungsaufbaus

Jetzt können Sie den Verbindungsaufbau zum Samba4-Server testen.

In Listing 4.16 sehen Sie den Test des Verbindungsaufbaus mit dem Kommando `smbclient`:

**Listing 4.16** Ein erster Verbindungsaufbau

```
root@sambabuch:~# smbclient -L sambabuch
Enter EXAMPLE\root's password:
Anonymous login successful
```

```

Sharename      Type      Comment
-----
netlogon      Disk
sysvol        Disk
IPC$          IPC       IPC Service (Samba 4.8.3-Debian)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

Server          Comment
-----
Workgroup       Master
-----
WORKGROUP      SAMBABUCH

```

Im Listing sehen Sie, dass bereits zwei Freigaben auf dem Domaincontroller bereitgestellt werden: *sysvol* und *netlogon*. Diese beiden Freigaben werden auf einem Domaincontroller immer benötigt und somit bei der Erstkonfiguration auch immer angelegt. Die Verwendung der beiden Freigaben werde ich im Verlauf des Buches genau erklären.

Weiter sehen Sie in dem Listing, dass keine NetBIOS-Informationen über Server und Workgroup angegeben werden. Das ist auch korrekt so, denn der Domaincontroller kann später in der Netzwerkumgebung der Clients nicht gesehen werden.

Sie sollten auch auf dem Domaincontroller keine weiteren Freigaben einrichten, sondern alle Daten immer auf einem Fileserver speichern. Der Grund dafür ist das unterschiedliche ID-Mapping der UIDs und GIDs der Linux-Benutzer. Auch darauf werde ich im Verlauf des Buches noch genauer eingehen.

#### 4.4.5 Testen des Kerberos-Servers

Jetzt fehlt noch der Test des Kerberos-Servers. Um den Kerberos-Server zu testen, können Sie mit dem Kommando *kinit* ein Ticket für den *administrator* der Domäne vom Kerberos-Server beziehen und anschließend mit *klist* testen.

Während der Installation des Pakets wird eine Datei */etc/krb5.conf* erzeugt. Diese Datei können Sie so aber nicht verwenden. Sie müssen die Datei von Samba4 an diese Stelle kopieren. Die Datei wird während des Provisionings erzeugt, dort wird auch angezeigt, wo Sie diese Datei finden.

Im Verzeichnis */var/lib/samba/private/* finden Sie die Datei *krb5.conf* Ihres Samba4-Servers. Den Inhalt der Datei sehen Sie in Listing 4.17:

##### Listing 4.17 Inhalt der Datei *krb5.conf*

```

[libdefaults]

    default_realm = EXAMPLE.NET
    dns_lookup_realm = false
    dns_lookup_kdc = true

```

In Listing 4.18 sehen Sie jetzt das Ergebnis eines Kerberos-Tests:

**Listing 4.18** Testen des Kerberos-Servers

```
root@sambabuch:~# kinit administrator
administrator@EXAMPLE.NET's Password:
root@sambabuch:~# klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: administrator@EXAMPLE.NET

Issued                Expires                Principal
Jun 17 17:16:10 2018  Jun 18 03:16:10 2018  \
krbtgt/EXAMPLE.NET@EXAMPLE.NET
```

Das Passwort für den administrator haben Sie bei der Konfiguration des DCs festgelegt. Jetzt können Sie das Ticket des Administrators schon für die Authentifizierung verwenden. In Listing 4.19 sehen Sie ein Beispiel für die Authentifizierung mit Kerberos:

**Listing 4.19** Verbindung mit Kerberos

```
root@sambabuch:~# smbclient -L sambabuch -k

Sharename      Type      Comment
-----      -
netlogon       Disk
sysvol         Disk
IPC$           IPC       IPC Service (Samba 4.8.3-Debian)
Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Master
-----
WORKGROUP      SAMBABUCH

root@sambabuch:~# klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: administrator@EXAMPLE.NET

Issued                Expires                Principal
Jun 17 17:16:10 2018  Jun 18 03:16:10 2018  \
krbtgt/EXAMPLE.NET@EXAMPLE.NET
Jun 17 17:19:18 2018  Jun 18 03:16:10 2018  \
cifs/sambabuch@EXAMPLE.NET
```

Anstelle des Benutzernamens wird hier die Option `-k` verwendet. Diese sorgt dafür, dass jetzt das zuvor erstellte Kerberos-Ticket des Administrators für die Authentifizierung Verwendung findet. Ein weiterer wichtiger Punkt ist der, dass Sie nicht mehr mit `localhost` arbeiten können, sondern immer den Hostnamen verwenden müssen, da nur dieser im Kerberos als Principal eingetragen ist.



### Hinweis

Im Kerberos werden Dienste, Benutzer und Hosts als Principals eingetragen. Nur gegen einen Host, der im Kerberos einen Principal-Eintrag besitzt, kann eine Kerberos-Authentifizierung durchgeführt werden. Da `localhost` aber nie einen Principal-Eintrag im Kerberos erhält, kann eine Kerberos-Authentifizierung auch nicht gegen `localhost` durchgeführt werden.

## 4.4.6 Testen des LDAP-Servers

Als letzter Test fehlt noch der Test des LDAP-Servers. Diesen Test können Sie mit dem Kommando `ldbsearch` durchführen. Das Kommando `ldbsearch` wird von Samba4 bereitgestellt und greift direkt auf den LDAP-Server von Samba4 zu. Sie können aber auch das Paket `ldap-utils` installieren und dann das Kommando `ldapsearch` verwenden. In Kapitel 5, «Die Benutzerverwaltung», gehe ich noch genauer auf die beiden Werkzeuge ein. Hier geht es nur darum zu testen, ob der LDAP-Server läuft. In Listing 4.20 sehen Sie einen Test:

### Listing 4.20 Testen des LDAP-Servers

```
root@sambabuch:~# ldbsearch -H ldap://sambabuch "cn=administrator" -k yes
# record 1
dn: CN=Administrator,CN=Users,DC=example,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Administrator
description: Built-in account for administering the \
            computer/domain
instanceType: 4
whenCreated: 20180617141220.0Z
uSNCreated: 3624
name: Administrator
objectGUID: dd57a402-7e78-4e77-a245-0d106ff63249
userAccountControl: 512
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
pwdLastSet: 131737183409644550
primaryGroupID: 513
objectSid: S-1-5-21-113282409-686688155-1353482721-500
adminCount: 1
accountExpires: 9223372036854775807
sAMAccountName: Administrator
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,\
                DC=example,DC=net
```

```

isCriticalSystemObject: TRUE
memberOf: CN=Domain Admins,CN=Users,DC=example,DC=net
memberOf: CN=Schema Admins,CN=Users,DC=example,DC=net
memberOf: CN=Enterprise Admins,CN=Users,DC=example,DC=net
memberOf: CN=Group Policy Creator Owners,CN=Users,\
        DC=example,DC=net
memberOf: CN=Administrators,CN=Builtin,DC=example,DC=net
lastLogonTimestamp: 131737221708339410
whenChanged: 20180617151610.0Z
uSNChanged: 3916
lastLogon: 131737221708479740
logonCount: 2
distinguishedName: CN=Administrator,CN=Users,DC=example,DC=net

# Referral
ref: ldap://example.net/CN=Configuration,DC=example,DC=net

# Referral
ref: ldap://example.net/DC=DomainDnsZones,DC=example,DC=net

# Referral
ref: ldap://example.net/DC=ForestDnsZones,DC=example,DC=net

# returned 4 records
# 1 entries
# 3 referrals

```



#### Hinweis

Sie sehen hier, dass ich wieder Kerberos für die Authentifizierung verwendet habe, diesmal aber mit der Option *-k yes*. Das liegt daran, dass es sich bei *ldbsearch* nicht um ein Binary wie *smbclient* handelt, sondern um ein in Python geschriebenes Programm. Für die in Python geschriebenen Programme müssen Sie für Kerberos-Authentifizierung immer die Option *-k yes* angeben. Das gilt auch für das Kommando *samba-tool*.

Jetzt ist der Domaincontroller so weit konfiguriert, dass er alle Dienste bereitstellen kann, und Sie haben auch alle Dienste überprüft.

## ■ 4.5 Konfiguration des Zeitservers

Da sämtliche Zugriffe auf den Kerberos-Dienst sehr zeitkritisch sind, sollte in Ihrem Netz auf jeden Fall ein Zeitserver laufen. Der Zeitserver wird über den Dienst NTP bereitgestellt. Achten Sie darauf, dass der `ntpd` mindestens die Version 4.2.6 hat, da ältere Versionen keine Signierung erlauben. Die Signierung des Zeitservers wird aber vom AD benötigt. Ein Zeitserver ohne Signierung kann nicht mit dem AD zusammenarbeiten. Installieren Sie das `ntp`-Paket für Ihre Distribution. Anschließend müssen Sie die Datei `/etc/ntp.conf` wie in Listing 4.21 anpassen:

### Listing 4.21 Konfiguration des Zeitservers

```
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
```

Vor dem Neustart des Zeitservers müssen Sie dem NTP noch das Recht geben, auf den signierten Socket vom Samba4 zuzugreifen. Dazu ändern Sie die besitzende Gruppe am Verzeichnis `/var/lib/samba/ntp_signd` so, wie in Listing 4.22 zu sehen ist:

### Listing 4.22 Rechte für den Zeitserver setzen

```
root@sambabuch:~# chgrp ntp /var/lib/samba/ntp_signd

root@sambabuch:~# chmod g+rx /var/lib/samba/ntp_signd
```

Die Gruppe muss nur die Rechte `r` und `x` besitzen. Nach dem Erstellen der Konfiguration starten Sie den Zeitserver neu. Jetzt können alle Windows-Clients und alle Windows-Server in der Domäne den Zeitserver für die Zeitsynchronisation nutzen.

Jetzt ist Ihr Domaincontroller vollständig installiert und konfiguriert. Im nächsten Kapitel geht es dann um die Verwaltung von Benutzern und Gruppen.

# Stichwortverzeichnis

/etc/hosts 263, 268  
[global]-Section 179

## A

acl 104  
aclcheck 104  
Active-Directory-Domaincontroller 12  
ad 174  
ADDC 12  
Aktiv/Aktiv-Cluster 273  
Apparmor 4, 52, 118  
Authentifizierung 156

## B

Backup 401  
Baumstruktur 182  
Benutzerverwaltung 63  
bind9 15, 43, 45, 49, 50, 111, 115, 117, 317  
Brick 264, 269, 440  
Build-Umgebung 16

## C

CentOS 26  
cifs 63, 255, 266  
Client 247, 265  
– DNS-Server 247  
Cluster Trivial Database 263  
cn=Users 221  
CNAME 420  
CNAME-Record 124  
Computersuchdienst 5, 397  
configure 16, 22, 28, 33  
Cron 131  
Cron-Job 131  
CSV 353, 354  
CTDB 263, 266, 284, 442  
ctdb 286  
CTDB\_NODES 287  
CTDB\_RECOVERY\_LOCK 287

CUPS 379, 381  
– cupsd.conf 381

## D

Dateisystem 229  
Dateisystemquota 239  
Dateisystemrechte 229  
– Besitzer 237  
– Vererbung 233  
DDNS 155  
Debian 9 15  
Desktopmanager 256  
DFS 226  
DFS-Link 226, 227  
DFS-Proxy 226  
DFS-Server 227  
DHCP-Server 155  
Disaster Recovery 309  
Dispersed 266  
Distribute 266  
Distribute Replicate 266  
Distributed File System 226  
Distribution 9  
DNS-Proxy 317  
dnssec 318  
dnssec-key 166  
DNS-Server 45, 111  
dnsupdate 424  
dnsutils 419  
Domaincontroller 12, 107, 247  
Domainnamemaster 133  
Domain-Suffix 331  
Domain-Trust 315  
Druckerserver 389  
Druckertreiber 388

## E

edquota 243  
enum groups 69

enum users 69  
 exportkeytab 260  
 external trust 316  
 externale trust 315

## F

Failover 286  
 Festplattenkontingent 239  
 Fileserver 422  
 Filesystemcluster 284  
 Firewall 407  
 – netstat 407, 408  
 – Ports DC 407  
 – Ports Fileserver 408  
 Flexible Single Master Operation 133  
 foreignSecurityPrincipal 331  
 Forest 315  
 Forest-Trusts 315, 331  
 Forwarder 51, 317  
 Forward-Lookupzone 108  
 Forward-Zone 318  
 Freigabe 189  
 – directory security mask 191  
 – hide unreadable 190  
 – HKLM 193  
 – read only = yes 190  
 – Registry 191  
 – rpc 192  
 – security mask 191  
 – smbclient 195  
 – tdbtool 192  
 – template homedir 199  
 Freigabeverwaltung 189  
 FSMO 126, 133, 420  
 – DomainDNSZones 134  
 – ForestDNSZones 134  
 – Infrastrukturmaster 134  
 – PDC-Master 126  
 – RID-Master 133  
 – Schemamaster 133  
 FSMO-Rolle 135  
 fuse 273  
 fuse-mount 265

## G

get 349  
 getent passwd 178  
 GID 10, 45, 63, 173  
 GID-Mapping 173  
 Global Catalog 56, 134, 375  
 GlusterFS 263, 264  
 – Modi 266

GPO 91  
 Groupmapping 365  
 Gruppenrichtlinien 91  
 – samba-tool gpo 91  
 – Verknüpfung 97  
 Gruppenrichtlinieneditor 92, 217  
 Gruppenrichtlinienverwaltung 92, 94, 217  
 Gruppenrichtlinienverwaltungs-Editor 94

## H

Heartbeat-Netzwerk 263  
 Heimatverzeichnis 199  
 Heimdal-Kerberos 10  
 Hive 181  
 HKLM 181  
 hostname 416

## I

ID-Mapping 57, 63, 67, 173, 254, 328  
 id-mapping 9  
 INBOUND 122  
 InfiniBand 264  
 interfaces 412  
 iptables 409

## K

KDC 176  
 Kerberos 56, 175, 418  
 Kerberos-Server 43, 57  
 Kerberos-Ticket 320  
 Key Distribution Center 176  
 Keytab 156  
 kinit 57  
 klist 57  
 Knoten 264  
 Knotentyp 398  
 krb5.conf 15, 57

## L

LAM 83, 84  
 – Baumansicht 90  
 – ldaps 85  
 ldap 75  
 LDAP 9, 56  
 LDAP Account Manager 63, 64, 83  
 – installieren 84  
 – konfigurieren 85  
 ldaps 75, 418  
 ldbdel 359  
 ldbedit 77, 401  
 ldbmodify 78, 361  
 ldbsearch 59, 75

ldb-tools 75  
.ldif-Datei 78  
ldif-Datei 304  
lightdm 256  
Linux-Client 247, 248  
– winbind 250  
Linux-Fileserver 173  
LMhosts 398  
Load Balancing 286  
log.ctdb 288  
LVM2 265, 275, 299

## M

make 17, 23  
make install 18, 23  
Masterbrowser 397, 403  
mget 349  
Migration 363  
– /etc/group 369  
– FSMO 375, 377  
– FSMO-Rollen 376  
– Global Catalog 375  
– In Place 363  
– openLDAP 370  
– Provisioning 364  
– .tdb-Datei 363  
– Windows-Server 374  
– wins support = yes 365  
MIT-Kerberos 3, 10  
Mountpoint 255  
mput 349

## N

Name Service Switch 253  
Namensraum 264  
Nameserver 47  
Namespace 331  
net 335  
– ads 344  
– info 346  
– lookup 346  
– status 346  
– rpc 344  
– status 346  
net conf 215  
NetBEUI 8  
NetBIOS 5, 8, 397, 412  
NetBIOS-Domainname 45  
NETLOGON 325  
netlogon 48, 57  
netplan 120  
Netzwerkumgebung 397

nmbd 8, 19, 25, 31, 36, 449  
nmblookup 402  
nodes 287  
NOTAUTH 424  
NSS 253, 259, 329  
nsswitch.conf 326  
NTDS-Setting 375  
ntlm 256  
NTLN 9  
ntp 61, 126  
ntp.conf 61

## O

objectGUID 124, 420  
OMAPI 166  
onnode 294  
Organisational Unit 93  
OU 93  
OUTBOUND 122

## P

PAM 259  
pam\_mount 255  
pam\_mount.conf.xml 255  
Passwort 71  
Passwortregeln 74  
pdbedit 64  
PDC-Emulator 133  
PDC-Master 126  
Peer 268, 269  
Point'n'Print 379  
Port 139 412  
Principal 58  
Printserver 379  
– Point'n'Print 390  
– print\$ 383  
– printers 383  
– Privilegien 380  
– rpcclient 392  
– Systemprivilegien 380  
Profile 202  
Protokoll 5  
Provisioning 47, 364, 416  
PSO 10  
PTR-Record 110  
public\_addresses 287  
put 349

## Q

Quorum 270  
Quota 239  
– aquota.group 241

- aquota.user 241
  - edquota 242
  - fstab 240
  - grace period 242
  - grpquota 240
  - Hardlimit 242
  - Inode 242
  - quotacheck 240
  - quotaon 241
  - repquota 244
  - Softlimit 242
  - usrquota 240
- Quota-Einträge 241

## R

- RDMA 264
- read-only 412
- readonly-Domaincontroller 145
- Realm 44, 416
- Recovery 401
- recycle 215
- Regedit 179, 185, 209
- Registrierungs-Editor 399
- Registry 178, 182, 189, 191, 311
  - binaries 180
  - Hive 180
  - HKLM 180
  - integer 180
  - net conf 183
  - registry shares = yes 179
  - samba-regedit 182
  - Schlüssel 181
  - string 180
- Remote Direct Memory Access 264
- Remote Server Administration Tools 63, 79
- Replicate 266
- Replikation 126, 400
- repquota 243
- resolv.conf 47, 319, 417
- Resolver 54, 56
- Reverse-Lookupzonen 108
- rfc2307 45
- RID 133, 253
- rid 174
- RODC 145
- round robin 43
- RSAT 63, 79, 80, 326
- rsync 126, 127, 420
  - dry-run 130
- rsyncd 129
- rsyncd.conf 128

## S

- samba 292
- samba4wins 398
- Samba-Freigaben 254
- Samba-Ports 55
- samba-tool 43, 44, 64, 336, 352
  - create username 71
  - dbcheck 336
  - disable user 73
  - drs 337
  - dsacl 341
  - fsmo 341
  - gpo 341
  - group 341
  - group add 67
  - group addmembers 69
  - group list 65
  - group listmembers 66
  - ldapcmp 342
  - ntacl 343
  - provision 44
  - sites 343
  - user 70, 343
  - user delete 74
  - user enable 73
  - user list 70
- Schemamaster 303
- seize 138
- SELinux 4, 26
- SerNet 37
- Server 173, 264
- Serverport 55
- Service-Records 123
- shadow\_copy2 9, 299
- Sicherheit 407
- Sicherung 309
- Single Sign-on 405
- SMB 5
- SMB2 6
- SMB3 7
- smbclient 56, 335, 349
- smb.conf 182, 247, 290, 311
- smbd 19, 25, 31, 36, 449
- smbd-Prozess 189
- smb-Kommandos 346
- smbstatus 335, 351
- smbtree 351
- Snapshot 265, 275, 299
- Split Brain 272
- split-brain 270
- Spooling 379
- SRV-Record 317, 319

SRV-Records 56  
ss 55, 129, 407  
ssh 405  
– net ads keytab 406  
ssh\_config 406  
sshd\_config 405  
ssh-Server 405  
SSSD 247, 258  
Standort 143  
Sticky Bit 203  
Storage-Pool 268  
Stripe 266  
Subnetz 143  
Subvolume 264  
Suse Leap 15 32  
System Security Services Daemon 258  
systemd 18, 53, 119, 273, 441  
sysvol 48, 57, 104, 126, 311  
– Replikation 126

## T

Tar 350  
.tar-File 350  
tdb 174  
.tdb-Datei 311  
tdb-Datenbank 191  
tdbdump 192  
tdbtool 192  
testparm 186  
TGT 405  
thinly-provision 269, 275  
Ticket Granting Ticket 405  
tkey-gssapi-keytab 51  
transitiv 316

## U

Ubuntu 21  
UID 45, 63, 173  
UID-Mapping 173  
UPN 331  
User Principal Name 331  
Userspace 265, 273

## V

Verbindungsaufbau 56  
Vererbung 233  
Vertrauensstellung 315  
vfs-Modul 297  
– glusterf 297  
Volume 264

## W

wbinfo 67, 253, 296, 323  
wbinfo -g 252  
wbinfo -u 252  
Wiederherstellung 312  
winbind 173, 247, 258, 292, 323, 449  
winbindd 19, 25, 31, 36, 68  
Windows Remote Server Administration Tools  
(RSAT) 64, 80  
Windows-Client 247  
Windows-Domaincontroller 43  
Windows-Server 247  
WINS 397  
– Replikation 401  
Workshop 431  
– Forwarder 435  
– Namensstandard 433  
– netlogon 439  
– Provisioning 434  
– Replikationsbenutzer 438  
– Reverse-Lookupzone 436  
– sysvol 439  
– sysvol-Replikation 437  
– Zeitserver 435

## X

xinetd 127, 129, 420  
xinetd.d 127

## Z

Zeitserver 61, 435  
zypper 32