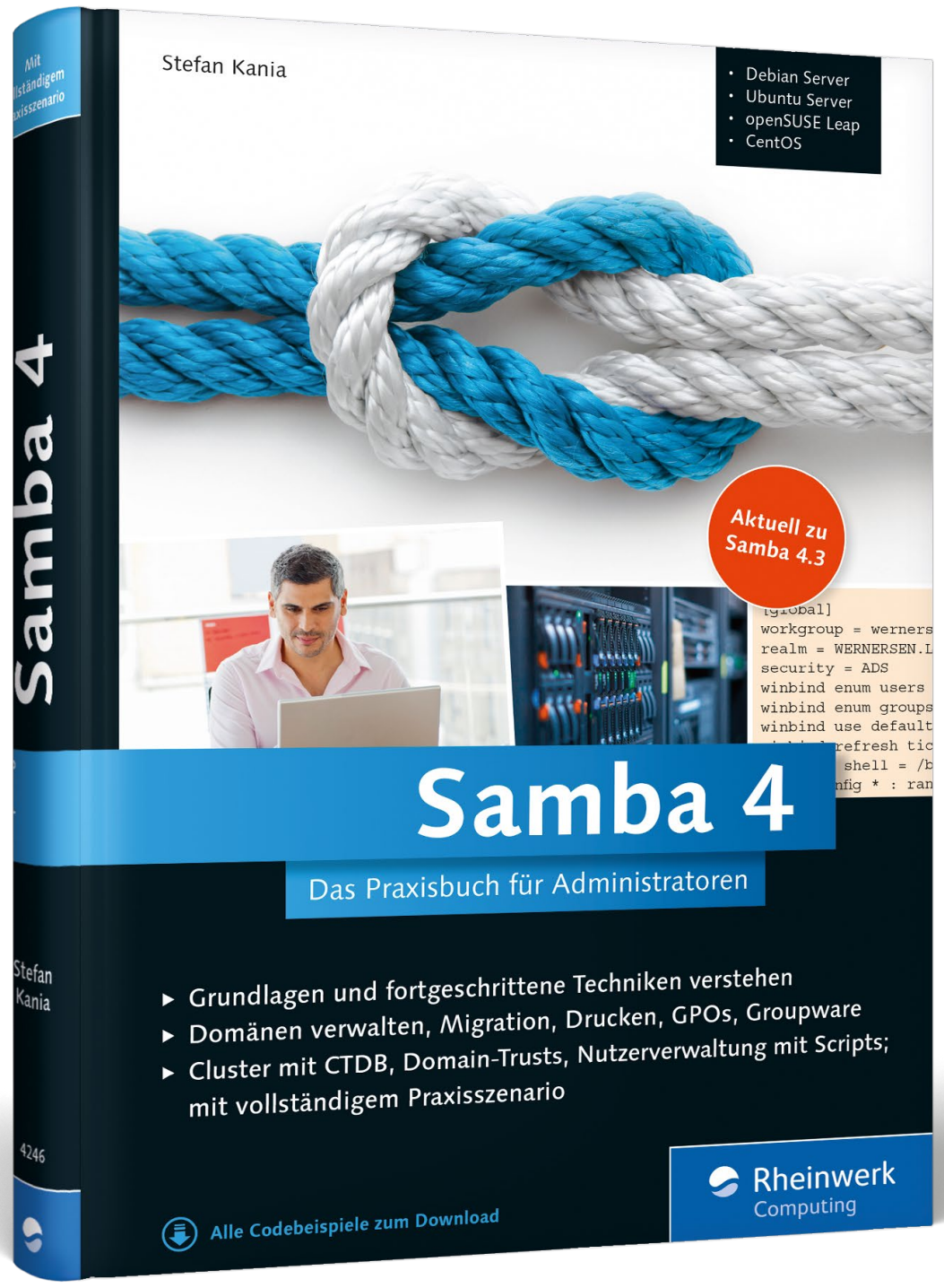


Leseprobe

Diese Buch ist der Leitfaden für Linux- und Windows-Administratoren. Diese Leseprobe zeigt Ihnen den Umgang mit der Benutzerverwaltung und das Einrichten eines Domaincontrollers mit Samba 4. Außerdem können Sie einen Blick in das vollständige Inhalts- und Stichwortverzeichnis des Buches werfen.

Stefan Kania

Samba 4 – Das Praxisbuch für Administratoren

469 Seiten, gebunden, 2. Auflage 2016
49,90 Euro, ISBN 978-3-8362-4246-2

www.rheinwerk-verlag.de/4186

Kapitel 4
Die Benutzerverwaltung

Nach der Installation des ersten Domaincontrollers geht es jetzt um die Verwaltung der Gruppen und Benutzer. Unter Samba 4 haben Sie verschiedene Möglichkeiten, die Benutzer und Gruppen zu verwalten. Da wäre zum einen die Verwaltung auf der Kommandozeile: Diese Möglichkeit ist sehr gut geeignet, um viele Benutzer und Gruppen gleichzeitig anzulegen oder zu ändern. Zum anderen können Sie die von Microsoft frei verfügbaren Remote Server Administration Tools (RSAT) nutzen. Über die RSAT können Sie eine Samba 4-Domäne genau so verwalten wie eine echte Microsoft-Active-Directory-Domäne. Es gibt zusätzlich verschiedene webbasierte Werkzeuge, die Sie nutzen können. Hier im Buch soll der LDAP Account Manager (LAM) als Beispiel zum Einsatz kommen.

Nachdem im vorherigen Kapitel die Konfiguration des ersten Domaincontrollers abgeschlossen wurde und Sie jetzt eine Active Directory-Domäne haben, soll es jetzt um die Verwaltung der Gruppen und Benutzer gehen.

An die Linux-Admins unter Ihnen: Sie müssen hier etwas umlernen, aber einen positiven Punkt möchte ich am Anfang hervorheben. Anders als bei Samba 3 müssen Sie bei Samba 4 kein Linux-Konto extra erstellen, bevor Sie ein Samba-Konto erstellen können. Hier zeigen sich ganz klar die Unterschiede in dem Konzept von Samba 3 und Samba 4. Sie legen nur noch ein Samba-Konto an.

Der Samba 4-Server sorgt später über das ID-Mapping dafür, dass auch Linux-Benutzer das System zur Authentifizierung nutzen können.

Aber wo Licht ist, ist auch irgendwo Schatten: Da Samba 4 für die Verwaltung einer Windows-Umgebung ausgelegt ist, ist die Verwaltung der Linux-Benutzer ganz anderen Regeln unterworfen, als Sie es gewohnt sind. Beim Anlegen der Benutzer werden Sie den ersten Unterschied feststellen, denn das Kommando `useradd` und andere Kommandos zur Benutzerverwaltung werden Sie jetzt nicht mehr benötigen.

Das Hauptaugenmerk liegt hier in erster Linie auf der Verwaltung von Windows-Benutzern und Gruppen. Aber selbstverständlich können sich auch Linux-Benutzer gegen das Active Directory authentifizieren und über Freigaben auf das Dateisystem zugreifen.

Aber die Linux-Benutzer unterliegen jetzt denselben Richtlinien wie die Windows-Benutzer. Das heißt, die Authentifizierung findet über Kerberos statt, alle Benutzer liegen immer im LDAP, und die Freigaben werden über *cifs* verwaltet.

Das größte Augenmerk müssen Sie auf das Mapping der *UID* und *GID* Ihrer Benutzer und Gruppen legen. Die beiden Attribute sind unter Windows keine Standardattribute und werden über das ID-Mapping von Samba 4 bereitgestellt.

Im Verlauf des Buches werde ich das Thema ID-Mapping immer wieder aufgreifen, um Ihnen zu zeigen, wie Sie mit ihm umgehen müssen, um ein einheitliches Mapping in Ihrer Domäne auf allen Linux-Systemen zu bekommen.

Für die Benutzerverwaltung unter Samba 4 gibt es verschiedene Wege:

- Mit dem Samba 4-Werkzeug `samba-tool`:
  Mit dem `samba-tool` können Sie Benutzer und Gruppen über die Kommandozeile verwalten. Damit haben Sie dann auch die Möglichkeit, mehrere Benutzer über Skripte anzulegen, zu ändern oder zu löschen.
- Über einen Windows-Client mit den *Windows Remote Administration Tools (RSAT):*
  Für Windows können Sie die *Windows Remote Server Administration Tools (RSAT)* bei Microsoft herunterladen und dann von Windows aus die Benutzern und Gruppen verwalten.

  Voraussetzung ist mindestens Windows 7 Professional.
- Mit dem *LDAP-Account-Manager (LAM):*
  Dank dem Einsatz von Roland Gruber gibt es jetzt ein Modul für den LAM, mit dem Sie die Benutzer und Gruppen von Samba 4 über das webbasierte Werkzeug verwalten können, obwohl bei Samba 4 kein *openLDAP* zum Einsatz kommt, sondern ein eigener LDAP-Server.

4.1 Benutzer- und Gruppenverwaltung über die Kommandozeile

Im ersten Teil geht es um die Verwaltung der Benutzer und Gruppen über die Kommandozeile. Die gesamte Verwaltung der Benutzer und Gruppen erfolgt hier über das Kommando `samba-tool`. Das `samba-tool` ist die Zusammenfassung der unter Samba 3 bekannten `net`-Tools und des Kommandos `pdbedit` und ersetzt diese bei der Verwaltung von Gruppen und Benutzern vollständig. In Kapitel 16, »Jetzt alles per Skript«, werde ich diese Kommandos wieder aufgreifen und für Shell-Skripte verwenden.

Als Linux-Administrator werden Sie anfangs versuchen, alle Benutzer und Gruppen über die Kommandozeile zu verwalten, was theoretisch auch möglich ist. Aber Sie werden sehr schnell feststellen, dass es an manchen Stellen einfacher ist, Benutzer

über die RSAT zu verwalten – besonders, wenn es darum geht, die Vielzahl an Attributen eines Benutzers zu verändern.

Als Windows-Administrator werden Sie auf der anderen Seite auch schnell die Vorzüge der Verwaltung der Benutzer und Gruppen über die Kommandozeile schätzen lernen. Besonders dann, wenn Sie mehrere Benutzer auf einmal anlegen wollen, denn dann können Sie das Kommando `samba-tool` recht einfach in Shell-Skripten einsetzen.

Deshalb folgt jetzt eine ausführliche Erklärung der Benutzerverwaltung über die Kommandozeile mit aussagekräftigen Beispielen.

4.1.1 Verwaltung von Gruppen über die Kommandozeile

Mit dem Kommando `samba-tool group` verwalten Sie die Gruppen. Zu dem Kommando gibt es die verschiedenen Optionen für die Verwaltung.

Wenn Sie auf der Kommandozeile nur das Kommando `samba-tool group` eingeben, dann erhalten Sie eine Hilfe zu dem Kommando. In Listing 4.1 sehen Sie die Hilfe:

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

Group management.


Options:
  -h, --help  show this help message and exit


Available subcommands:
  add            - Creates a new AD group.
  addmembers     - Add members to an AD group.
  delete         - Deletes an AD group.
  list           - List all groups.
  listmembers    - List all members of an AD group.
  removemembers  - Remove members from an AD group.

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

Listing 4.1 Hilfe zu »samba-tool group«

In den folgenden Abschnitten werde ich auf alle Subkommandos eingehen, aber nicht in der Reihenfolge, wie sie in der Hilfe aufgelistet sind. So haben Sie die Möglichkeit, alle Beispiele direkt auszuprobieren.

Auflisten der Gruppen mit »group list«

Eine Übersicht über alle Gruppen im System erhalten Sie, wie in Listing 4.2 zu sehen, mit `samba-tool group list`:

```
root@sambabuch:~# samba-tool group list
Allowed RODC Password Replication Group
Enterprise Read-Only Domain Controllers
Denied RODC Password Replication Group
Pre-Windows 2000 Compatible Access
Windows Authorization Access Group
Certificate Service DCOM Access
Network Configuration Operators
Terminal Server License Servers
Incoming Forest Trust Builders
Read-Only Domain Controllers
Group Policy Creator Owners
Performance Monitor Users
Cryptographic Operators
Distributed COM Users
Performance Log Users
Remote Desktop Users
Account Operators
Event Log Readers
RAS and IAS Servers
Backup Operators
Domain Controllers
Server Operators
Enterprise Admins
Print Operators
Administrators
Domain Computers
Cert Publishers
DnsUpdateProxy
Domain Admins
Domain Guests
Schema Admins
Domain Users
Replicator
IIS_IUSRS
DnsAdmins
Guests
Users
```

Listing 4.2 Auflisten der Gruppen

Hier sehen Sie eine Liste aller Gruppen, die nach der Installation des Systems vorhanden sind. Bei diesen Gruppen handelt es sich um Gruppen, die auch für die Verwaltung des AD unter Windows benötigt werden.

Löschen Sie keine der Gruppen

Löschen Sie keine der hier aufgelisteten Gruppen aus Ihrem System. Alle diese Gruppen haben eine feste Bedeutung in der Windows-Welt und werden immer mit einem festen *Security Identifier (SID)* verwaltet.

Löschen Sie eine der Gruppen, kann das dazu führen, dass Sie Ihre Domäne neu aufsetzen müssen.

Auflisten der Gruppenmitglieder einer Gruppe mit »group listmembers <group>«

Wenn Sie wissen wollen, welche Benutzer Mitglied einer Gruppe sind, können Sie, wie in Listing 4.3 zu sehen, dies mit `samba-tool group listmembers <group>` überprüfen:

```
root@sambabuch:~# samba-tool group listmembers administrators
Administrator
Enterprise Admins
Domain Admins
```

Listing 4.3 Auflisten der Gruppenmitglieder

Beim Auflisten der Gruppe `administrators` sehen Sie, dass die Gruppe `Domain Admins` Mitglied der Gruppe ist. Samba 4 kann mit den verschachtelten Gruppen umgehen. Auch Sie können später bei der Administration Gruppen verschachteln.

Im Gegensatz zu Samba 3 müssen Sie bei Samba 4 die Möglichkeit der verschachtelten Gruppen nicht mehr in der Datei *smb.conf* aktivieren.

Anlegen einer neuen Gruppe mit »group add <groupname>«

Eine neue Gruppe können Sie mit dem Kommando `samba-tool group add <groupname>` zu Ihrer Gruppenliste hinzufügen. Listing 4.4 zeigt das Anlegen einer neuen Gruppe:

```
root@sambabuch:~# samba-tool group add datengruppe
Added group datengruppe
```

Listing 4.4 Anlegen einer neuen Gruppe

Die gerade angelegte Gruppe ist eine reine Windows-Gruppe. Sie können die Gruppe mit dem Kommando `wbinfo -g` sehen, aber im Moment noch nicht mit `getent group`. In Listing 4.5 sehen Sie die Liste der Gruppen:

```
root@sambabuch:~# wbinfo -g
EXAMPLE\cert publishers
EXAMPLE\ras and ias servers
EXAMPLE\allowed rodc password replication group
EXAMPLE\denied rodc password replication group
EXAMPLE\dnsadmins
EXAMPLE\enterprise read-only domain controllers
EXAMPLE\domain admins
EXAMPLE\domain users
EXAMPLE\domain guests
EXAMPLE\domain computers
EXAMPLE\domain controllers
EXAMPLE\schema admins
EXAMPLE\enterprise admins
EXAMPLE\group policy creator owners
EXAMPLE\read-only domain controllers
EXAMPLE\dnsupdateproxy
EXAMPLE\datengruppe
```

Listing 4.5 Liste der Gruppen

Auch können Sie mit `chgrp <neu-Gruppe> <Eintrag>` keine Berechtigungen setzen. Das Setzen der Rechte wäre im Moment nur über die GID möglich, da die Namen noch nicht aufgelöst werden können.

Für die Verwendung der Gruppe unter Linux müssen Sie das ID-Mapping aktivieren. Hier müssen Sie zwischen dem ID-Mapping auf einem Domaincontroller und dem ID-Mapping auf einem Fileserver oder einem Linux-Client unterscheiden. Auf einem Domaincontroller bis zur Version 4.1.x übernimmt Samba 4 das ID-Mapping über einen integrierten *winbind* selbst, und weist den Windows-Benutzern und -Gruppen eigene IDs zu. Auf einem Domaincontroller mit einer Version ab 4.2.x läuft zwar ein eigenständiger *winbindd*, aber trotzdem bleibt das ID-Mapping auf einem Domaincontroller immer unterschiedlich zu dem aller anderen Samba-Hosts. Bei einem Fileserver oder einem Linux-Client übernimmt der *winbindd* diese Aufgabe vollständig und lässt sich auch konfigurieren. Mehr zu dieser Problematik erfahren Sie in Kapitel 10, »Verwaltung von Clients in der Domäne«, und Kapitel 7, »Zusätzliche Server in der Domäne«.

Um die Gruppen auch im Linux-System sehen und nutzen zu können, muss die Datei */etc/nsswitch.conf* wie in Listing 4.6 angepasst werden:

```
passwd compat winbind
group compat winbind
```

Listing 4.6 Anpassen der Datei »nsswitch.conf«

Bei CentOS müssen Sie die Datei *nsswitch.conf* wie in Listing 4.7 anpassen:

```
passwd files winbind
group files winbind
```

Listing 4.7 Die Datei »nsswitch.conf« unter CentOS

Nach der Anpassung der Datei */etc/nsswitch.conf* können Sie jetzt mit dem Kommando `getent group <Gruppenname>` einzelne Gruppen sehen und auch Rechte an die Gruppen über die Kommandozeile vergeben.

Wenn Sie später auf dem Domaincontroller keine Daten speichern wollen oder die Rechte über die Kommandozeile verwalten möchten, brauchen Sie die Datei */etc/nsswitch.conf* nicht anzupassen.

In Listing 4.8 sehen Sie, dass die Domänengruppen mit aufgelistet werden:

```
root@sambabuch:~# getent group datengruppe
EXAMPLE\datengruppe:x:3000019:
```

Listing 4.8 Auflisten der Gruppen mit »getent group«

Wollen Sie alle Benutzer und Gruppen aus der Domäne mit dem Kommando `getent` sehen, müssen Sie die Datei *smb.conf* wie in Listing 4.9 anpassen:

```
winbind enum users = yes
winbind enum groups = yes
```

Listing 4.9 Anpassung der Datei »smb.conf«

Ich rate davon aber ab, da gerade in großen Umgebungen mit sehr vielen Benutzern und Gruppen der Aufwand für das System nicht unerheblich ist, die Liste aller Benutzer und Gruppen mit ihren IDs zu cachen. Für die Vergabe von Rechten ist das auch nicht notwendig.

Hinzufügen eines oder mehrerer Benutzer zu einer bestehenden Gruppe mit »group addmembers <groupname> <members>«

Über das Kommando `samba-tool group addmembers <groupname> <members>` können Sie mehrere Benutzer gleichzeitig zu einer Gruppe hinzufügen. Listing 4.10 zeigt dieses Vorgehen:

```
root@sambabuch:~# samba-tool group addmembers datengruppe "Domain Users"
Added members to group datengruppe

root@sambabuch:~# samba-tool group listmembers datengruppe
Domain Users
```

Listing 4.10 Gruppenmitglieder hinzufügen

Da Sie Gruppen verschachteln können, können Sie auch eine oder mehrere der Standardgruppen zu Ihrer Gruppe hinzufügen.

Achten Sie darauf, dass einige der Gruppen ein Leerzeichen im Namen haben. Dann müssen Sie den Gruppennamen beim Hinzufügen in Hochkommata setzen.

[+] Sie können mit dem Kommando `samba-tool group addmembers <groupname> <members>` keine lokalen Gruppen des Systems zu den AD-Gruppen hinzufügen, da diese Gruppen nur auf dem System vorhanden sind und nicht im AD.

Keine Verwendung von lokalen Gruppennamen

Verwenden Sie für neue Gruppen keine Namen, die in der lokalen Gruppenverwaltung über die Datei */etc/group* Verwendung finden.

Die lokalen Gruppen haben immer Priorität vor den Gruppen aus dem AD. Wenn Sie jetzt also eine Gruppe im AD anlegen, die denselben Namen hat wie eine lokale Gruppe, wird das System bei der Rechtevergabe immer die lokale Gruppe verwenden.

Benutzer mit »group removemembers <groupname> <members>« aus einer Gruppe entfernen

Wenn Sie einen oder mehrere Benutzer aus einer Gruppe entfernen möchten, geht das mit dem Kommando `samba-tool group removemembers <groupname> <members>`. In Listing 4.11 sehen Sie ein Beispiel:

```
root@sambabuch:~# samba-tool group removemembers datengruppe "Domain Users"
Removed members from group datengruppe
```

Listing 4.11 Entfernen von Mitgliedern

Sie können hier auch mehrere Mitglieder, durch Leerzeichen getrennt angeben, aus der Gruppe entfernen.

4.1.2 Verwaltung von Benutzern über die Kommandozeile

Für die Verwaltung der Benutzer verwenden Sie das Kommando `samba-tool user`. Genau wie bei der Verwaltung der Gruppen gibt es auch hier wieder Subkommandos für die verschiedenen Aufgaben. Dies Sehen Sie in Listing 4.12:

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

User management.

Options:
  -h, --help  show this help message and exit


Available subcommands:
  add          - Create a new user.
  create       - Create a new user.
  delete       - Delete a user.
  disable      - Disable an user.
  enable       - Enable an user.
  list         - List all users.
  password     - Change password for a user account \
                 (the one provided in authentication).
  setexpiry    - Set the expiration of a user account.
  setpassword  - Set or reset the password of a user account.
For more help on a specific subcommand, please type: \
                 samba-tool user <subcommand> (-h|--help)
```

Listing 4.12 Hilfe zum Kommando »samba-tool user«

Auch hier werde ich wieder auf alle Subkommandos näher eingehen, sodass Sie die Beispiele gleich testen können.

Auflisten der Benutzer mit »user list«

Alle Benutzer können Sie sich mit den Kommando `samba-tool user list` anzeigen lassen. In Listing 4.13 sehen Sie eine Liste alle Benutzer nach der Installation des Systems:

```
root@sambabuch:~# samba-tool user list
Administrator
krbtgt
Guest
```

Listing 4.13 Auflistung aller Benutzer

Wie schon zuvor bei den Gruppen sehen Sie hier alle Benutzer, die während der Installation angelegt werden. Auch hier gilt: Löschen Sie keinen dieser Benutzer.

Anlegen eines Benutzers mit »user create <username> <password>«

Um einen neuen Benutzer über die Kommandozeile anzulegen, verwenden Sie das Kommando `samba-tool user create <username> <password>`. Achten Sie bei dem Passwort auf die Komplexitätsregeln. In Listing 4.14 sehen Sie ein Beispiel mit einem Passwort, das diesen Regeln nicht entspricht.

```
root@sambabuch:~# samba-tool user create Stefan geheim --given-name=Stefan \
                  --surname=Kania
ERROR(ldb): Failed to add user 'Stefan':  - 00000052D: Constraint violation \
      - check_password_restrictions: the password is too short. It should \
      be equal or longer than 7 characters!
```

Listing 4.14 Passwort, das nicht den Komplexitätsregeln entspricht

Komplexitätsregeln bei Passwörtern

Für die Komplexitätsregeln gilt: Es müssen mindestens Groß- und Kleinbuchstaben und Zahlen verwendet werden oder aber mindestens ein Sonderzeichen. Sie müssen also immer drei verschiedene Zeichengruppen beim Passwort verwenden, und die Mindestlänge eines Passworts ist sieben Zeichen.

Alle Benutzer, die Sie über die Kommandozeile anlegen, werden in der Organisationseinheit `cn=Users,DC=example,DC=net` angelegt. Wenn Sie später eine komplexe AD-Struktur angelegt haben, müssen Sie die neuen Benutzer auf jeden Fall immer verschieben.

Ab der Samba-Version 4.2 können Sie mit dem Kommando `samba-tool` und der Option `-userou=USEROU` den Kontext festlegen in dem der Benutzer angelegt werden soll.

In Listing 4.15 sehen Sie das erfolgreiche Anlegen eines neuen Benutzers:

```
root@sambabuch:~# samba-tool user create Stefan geheim\!123 \
                  --given-name=Stefan --surname=Kania
User 'Stefan' created successfully

root@sambabuch:~# samba-tool user list
Administrator
Stefan
krbtgt
Guest
```

Listing 4.15 Erfolgreiches Anlegen eines Benutzers

Wie Sie in dem Beispiel sehen, können Sie beim Anlegen des Benutzers gleich weitere Parameter mit angeben. In diesem Beispiel sind es der Vor- und der Nachname. Alle Werte, die im AD verwendet werden, können hier mit übergeben werden. Da es sich dabei um eine größere Anzahl von Parametern handelt, kann an dieser Stelle nicht darauf eingegangen werden.

Bei der Benutzerverwaltung mit grafischen Werkzeugen werden Sie alle Parameter sehen und anpassen können.

Wenn Sie alle Parameter sehen wollen, die Sie beim Anlegen von Benutzern verwenden können, dann geben Sie das Kommando `samba-tool user create -help` ein. Dann erhalten Sie eine Liste aller verfügbaren Optionen. Welche Optionen Sie beim Anlegen eines Benutzers vergeben können, ist abhängig von der Samba-Version, die Sie auf dem Domaincontroller einsetzen.

In Listing 4.16 legen Sie einen Benutzer ohne weitere Parameter an:

```
root@sambabuch:~#  samba-tool user create ktom
New Password:
Retype Password:
User 'ktom' created successfully
```

Listing 4.16 Ein weiterer Benutzer

Da dieses Mal kein Passwort beim Anlegen des Benutzers mitgegeben wurde, wird jetzt nach dem Passwort für den Benutzer gefragt.

Das Heimatverzeichnis des Benutzers wird nicht mit angelegt, das müssen Sie selbst auf dem entsprechenden Server anlegen und mit Rechten versehen. Auch müssen Sie das Heimatverzeichnis noch dem Benutzer zuweisen. Mehr dazu finden Sie in Kapitel 8, »Verwaltung von Freigaben«

Nach dem Anlegen des Benutzers können Sie sich den Benutzer wieder mit `samba-tool user list` auflisten lassen. Auch die Benutzer sehen Sie wieder mit `wbinfo -u`. Wie schon bei den Gruppen werden die neuen Benutzer mit `getent passwd` nur angezeigt, wenn Sie die Datei */etc/nsswitch.conf* angepasst haben. In Listing 4.17 sehen Sie das Ergebnis sowohl von `wbinfo -u` als auch von `getent passwd`:

```
root@sambabuch:~# wbinfo -u
EXAMPLE\administrator
EXAMPLE\stefan
EXAMPLE\krbtgt
EXAMPLE\guest
EXAMPLE\ktom

root@sambabuch:~# getent passwd ktom
EXAMPLE\ktom:*:3000045:100::/home/EXAMPLE/ktom:/bin/false
```

Listing 4.17 Auflisten der Benutzer

Deaktivieren eines Benutzers mit »samba-tool user disable <username>«

Wenn Sie einen bestehenden Benutzer nur kurzzeitig aussperren wollen, weil der Benutzer sich zurzeit nicht anmelden darf oder soll, können Sie den Benutzer einfach deaktivieren und müssen ihn nicht gleich löschen. In Listing 4.18 sehen Sie ein Beispiel für das Deaktivieren eines Benutzers:

```
root@sambabuch:~# samba-tool user disable stefan
```

Listing 4.18 Deaktivieren eines Benutzers

Leider erhalten Sie bei `samba-tool user disable stefan` keine Meldung.

Eine deaktivierten Benutzer mit »samba-tool user enable <username>« aktivieren

Um einen zuvor deaktivierten Benutzer wieder zu aktivieren, verwenden Sie das Kommando `samba-tool user enable <username>` so, wie Sie in Listing 4.19 sehen:

```
root@sambabuch:~# samba-tool user enable stefan

Enabled user 'stefan'
```

Listing 4.19 Aktivieren eines Benutzers

Hier bekommen Sie eine Meldung, dass der Benutzer wieder aktiviert wurde.

Ändern des Passworts mit »samba-tool user setpassword <username>«

Für den Fall, dass ein Benutzer sein Passwort vergessen hat, oder wenn Sie einem Benutzer aus einem anderen Grund ein neues Passwort zuweisen wollen, verwenden Sie das Kommando `samba-tool user setpassword <username>`. In Listing 4.20 sehen Sie ein Beispiel dafür:

```
root@sambabuch:~# samba-tool user setpassword stefan
New Password:

Changed password OK
```

Listing 4.20 Setzen des Passworts eines Benutzers

Beim Setzen eines neuen Passworts müssen Sie wieder auf die Komplexitätsregeln achten. Das neue Passwort wird nur einmal eingegeben. Achten Sie also darauf, was Sie eingeben. Sonst müssen Sie den Vorgang wiederholen.

[+] Das Ändern der Passwörter wird hier als Benutzer *root* durchgeführt. Damit sind Sie auch in der Lage, das Passwort für den *Administrator* zu setzen.

Denken Sie außerdem daran, dass das Passwort des Administrators ebenfalls ein Ablaufdatum hat.

Ändern des Passworts durch den Benutzer mit »samba-tool user password«

Natürlich kann ein Benutzer sein Passwort auch selbst über die Kommandozeile verändern. Dafür gibt es das Kommando `samba-tool user password`.

In Listing 4.21 sehen Sie diesen Vorgang:


```
EXAMPLE\stefan@sambabuch:~# samba-tool user password
Password for [EXAMPLE\stefan]:
New Password:
Retype Password:
Changed password OK
```

Listing 4.21 Änderung des Passworts durch den Benutzer

Da der Benutzer immer erst sein altes Passwort angeben muss, wird er bei der Änderung des eigenen Passworts immer zweimal aufgefordert, sein neues Passwort einzugeben. Denn sollte an der Stelle das Passwort falsch eingegeben worden sein, hat der Benutzer keine Chance mehr, sein Passwort zu ändern, da er immer zuerst nach dem alten Passwort gefragt wird.

Löschen eines Benutzers mit »samba-tool user delete <username>«

Wenn Sie einen Benutzer aus dem System entfernen wollen, nutzen Sie dafür das Kommando `user delete <username>` so, wie Sie es in Listing 4.22 sehen:

```
root@samba4-1:~# samba-tool user delete Stefan
Deleted user Stefan
```

Listing 4.22 Löschen eines Benutzers

Denken Sie daran, dass ein eventuelles Heimatverzeichnis des Benutzers nicht automatisch gelöscht wird.

4.1.3 Passwortregeln setzen

Seit der Version 4.2 können Sie Passwortregeln mit `samba-tool` für die Benutzer direkt auf dem Domaincontroller setzen. Listing 4.23 zeigt eine Liste aller möglichen Optionen:

```
root@sambabuch:~# samba-tool domain passwordsettings show
Password informations for domain 'DC=example,DC=net'
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Listing 4.23 Liste aller Passwortregeln

Mit dem Kommando `samba-tool domain passwordsettings show -help` können Sie sich alle Optionen anzeigen lassen. Wie Sie eine Option ändern, sehen Sie in Listing 4.24:

```
root@sambabuch:~# samba-tool domain passwordsettings set --max-pwd-age=50
Maximum password age changed!
All changes applied successfully!
```

Listing 4.24 Anpassen des maximalen Passwortalters

Alle Änderungen sind immer in der gesamten Domäne gültig und müssen nicht auf jedem Domaincontroller eingerichtet werden.

4.1.4 Ändern und Suchen von Benutzern mit den ldb-tools

Natürlich können Sie auch über die Kommandozeile nach Benutzern und Gruppen suchen und diese mittels Skripten verändern. Dazu gibt es verschiedene Kommandos. Wenn Sie bis jetzt vielleicht schon mit openLDAP gearbeitet haben, wird Ihnen die Syntax bekannt vorkommen.

Auflisten von Benutzern mittels »ldbsearch«

Mit dem Kommando `ldbsearch` können Sie nach Objekten suchen. Natürlich können Sie hier Filter verwenden, um die Ergebnisse einzugrenzen. In Listing 4.25 sehen Sie ein Beispiel für die Suche mit `ldbsearch`:

```
root@sambabuch:~# ldbsearch -H ldaps://localhost "cn=Stefan Kania"
search error - LDAP error 1 LDAP_OPERATIONS_ERROR -  <00002020: \
    Operation unavailable without authentication> <>

root@sambabuch:~# ldbsearch -H ldaps://localhost "cn=Stefan Kania" \
                  -U administrator
Password for [EXAMPLE\administrator]:
# record 1
dn: CN=Stefan Kania,CN=Users,DC=example,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Stefan Kania
sn: Kania
givenName: Stefan
instanceType: 4
whenCreated: 20151204093952.0Z
displayName: Stefan Kania
```



```
uSNCreated: 3729
name: Stefan Kania
objectGUID: ab3e5b95-fed5-4dec-9b4a-e135a4a8d40b
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
primaryGroupID: 513
objectSid: S-1-5-21-2641355115-960991230-4068238628-1105
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Stefan
sAMAccountType: 805306368
userPrincipalName: Stefan@example.net
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=net
userAccountControl: 512
pwdLastSet: 130936961710000000
whenChanged: 20151204094931.0Z
uSNChanged: 3737
distinguishedName: CN=Stefan Kania,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

root@sambabuch:~# kinit administrator
administrator@EXAMPLE.NET's Password:

root@sambabuch:~# ldbsearch -H ldaps://sambabuch "cn=Stefan Kania" \
                  -k yes
# record 1
dn: CN=Stefan Kania,CN=Users,DC=example,DC=net
```

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Stefan Kania
sn: Kania
givenName: Stefan
.
.
.
```

Listing 4.25 Beispiel für die Suche mit »ldbsearch«

Im ersten Teil dieses Beispiels sehen Sie, was passiert, wenn Sie ohne eine Authentifizierung versuchen, auf das AD zuzugreifen. Denken Sie daran: Wenn Sie über das Netz auf das AD zugreifen, müssen Sie sich immer authentifizieren. Im zweiten Versuch gelingt die Suche, da hier der *administrator* für die Authentifizierung verwendet wird.

Im dritten Beispiel sehen Sie, dass auch hier eine Authentifizierung über Kerberos möglich ist.

In Listing 4.26 wird nicht über das Netz auf die Benutzerdatenbank zugegriffen, sondern direkt auf die Benutzerdatenbank auf dem Domaincontroller:

```
root@sambabuch:~#  ldbsearch --url=/var/lib/samba/private/sam.ldb \
                   "cn=Stefan Kania"
# record 1
dn: CN=Stefan Kania,CN=Users,DC=example,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Stefan Kania
sn: Kania
givenName: Stefan
instanceType: 4
whenCreated: 20151204093952.0Z
displayName: Stefan Kania
uSNCreated: 3729
name: Stefan Kania
objectGUID: ab3e5b95-fed5-4dec-9b4a-e135a4a8d40b
badPwdCount: 0
codePage: 0
countryCode: 0
```



```
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
primaryGroupID: 513
objectSid: S-1-5-21-2641355115-960991230-4068238628-1105
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Stefan
sAMAccountType: 805306368
userPrincipalName: Stefan@example.net
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=net
userAccountControl: 512
pwdLastSet: 130936961710000000
whenChanged: 20151204094931.0Z
uSNChanged: 3737
distinguishedName: CN=Stefan Kania,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
```

Listing 4.26 Zugriff direkt auf die Datenbank

Wie Sie hier sehen, können Sie direkt auf dem Server auf die Datenbankdatei zugreifen. Bei diesem Zugriff wird keine Authentifizierung benötigt. Der Zugriff wird hier über die Dateisystemrechte gesteuert. Zugriff auf die Datei hat aber nur der *root*, so dass ein normaler Benutzer diese Möglichkeit nicht nutzen kann. Auch ein Zugriff über den lokalen LDAP-Socket, wie in Listing 4.27 gezeigt, ist möglich.

Auch hier kann dieser Zugriff nur vom Benutzer *root* durchgeführt werden, da auch hier nur der *root* Rechte am Socket hat.

```
root@sambabuch:~# ldbsearch -H ldapi:///var/lib/samba/private/ldap_priv/ldapi \
                  "cn=Stefan Kania"
# record 1
dn: CN=Stefan Kania,CN=Users,DC=example,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Stefan Kania
sn: Kania
givenName: Stefan
instanceType: 4
whenCreated: 20151204093952.0Z
displayName: Stefan Kania
uSNCreated: 3729
name: Stefan Kania
objectGUID: ab3e5b95-fed5-4dec-9b4a-e135a4a8d40b
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
primaryGroupID: 513
objectSid: S-1-5-21-2641355115-960991230-4068238628-1105
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Stefan
sAMAccountType: 805306368
userPrincipalName: Stefan@example.net
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=net
userAccountControl: 512
pwdLastSet: 130936961710000000
whenChanged: 20151204094931.0Z
uSNChanged: 3737
distinguishedName: CN=Stefan Kania,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
```

Listing 4.27 Zugriff auf den lokalen LDAP-Socket

Auch eine eingeschränkte Suche auf bestimmte Attribute ist möglich, wie Sie in Listing 4.28 sehen:

```
root@sambabuch:~# ldbsearch -H ldapi:///var/lib/samba/private/ldap_priv/ldapi \
                  "cn=Stefan Kania" attr sn givenName

# record 1
dn: CN=Stefan Kania,CN=Users,DC=example,DC=net
sn: Kania
givenName: Stefan

# 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
```

Listing 4.28 Eingeschränkte Suche

Ändern eines Objektes mit »ldbedit«

Mit dem Kommando `ldbedit` können Sie einzelne Objekte ändern und die Änderung wieder im AD speichern. Für die Änderung wird der bei Ihnen im System eingestellte Standardeditor verwendet. In Listing 4.29 sehen Sie den Aufruf von `ldbedit`:

```
root@sambabuch:~# ldbedit -H ldapi:///var/lib/samba/private/ldapi \
                  sAMAccountName=stefan -k yes
```

Listing 4.29 Ändern eines Objekts mittels »ldbedit«

Obwohl Sie hier wieder über den Socket zugreifen, müssen Sie sich jetzt authentifizieren, da Sie schreibend auf die Datenbank zugreifen wollen und dieses nur für authentifizierte Benutzer erlaubt ist.

Wenn Sie beim Editieren einen Fehler machen, wird die Änderung nicht gespeichert, und Sie bekommen eine Fehlermeldung, wie in Listing 4.30 zu sehen ist:

```
root@sambabuch:~# ldbedit -H ldapi:///var/lib/samba/private/ldapi \
                  sAMAccountName=stefan -k yes

failed to modify CN=Stefan Kania,CN=Users,DC=example,DC=net \
      - LDAP error 16 LDAP_NO_SUCH_ATTRIBUTE - \
      <acl_modify: attribute 'ivenName' on\
      entry 'CN=Stefan Kania,CN=Users,DC=example,DC=net'\
      was not found in the schema!> <>
```

Listing 4.30 Fehlerbehandlung beim Editieren mit »ldbedit«

Ändern eines Objektes mit »ldbmodify«

Sie können einzelne Attribute eines oder mehrerer Objekte auch mithilfe des Kommandos `ldbmodify` und einer *.ldif*-Datei ändern. Als Erstes erstellen Sie eine *.ldif*-Datei wie in Listing 4.31:

```
dn: cn=ktom,cn=users,dc=example,dc=net
changetype: modify
replace: sn
sn: Tom
-
add: description
description: Ein Benutzer
```

Listing 4.31 Änderung eines Objektes mit »ldbmodify«

Anschließend spielen Sie die Änderung wie Sie in Listing 4.32 sehen, ein:

```
root@sambabuch:~# ldbmodify -H ldapi:///var/lib/samba/private/ldapi \
                  -k yes ktom.ldif

Modified 1 records successfully
```

Listing 4.32 Einspielen der Änderung

Wollen Sie ein weiteres Objekt mit derselben *.ldif*-Datei ändern, können Sie dieses einfach durch eine Leerzeile in die Datei eintragen.

In Listing 4.33 sehen Sie ein Beispiel für eine *.ldif*-Datei mit mehreren Objekten:


```
dn: cn=ktom,cn=users,dc=example,dc=net
changetype: modify
replace: sn
sn: Tom
-
add: description
description: Ein Benutzer

dn: cn=Stefan Kania,cn=users,dc=example,dc=net
changetype: modify
replace: sn
sn: Stefan
-
add: description
description: Ein weiterer Benutzer
```

Listing 4.33 ».ldif«-Datei zur Änderung mehrerer Objekte

Sie sehen hier, dass die Objekte immer durch eine Leerzeile getrennt sind und die einzelnen Attribute durch eine Zeile, in der nur ein Minuszeichen steht.

In der Leerzeile zwischen den Objekten darf wirklich kein Zeichen stehen, auch kein Leerzeichen und kein Tabulator.

Nachdem Sie jetzt gesehen haben, wie Sie Gruppen und Benutzer auf der Kommandozeile verwalten, wird es in nächsten Abschnitt um die Verwendung der *Remote Server Administration Tools (RSAT)* gehen.

4.2 Die »Remote Server Administration Tools« (RSAT)

Microsoft hat für die Verwaltung einer AD-Domäne Werkzeuge bereitgestellt, mit denen Sie die Domäne von einer Windows-Workstation aus administrieren können. Sie benötigen mindestens eine Windows 7-Professional-Version. Die Workstation muss Mitglied der Domäne sein, die Sie von dort aus verwalten wollen. In diesem Teil der Benutzerverwaltung geht es jetzt darum, die *RSAT* zu installieren und dann Gruppen und Benutzer über die RSAT zu verwalten.

Die RSAT gibt es für alle Windows-Versionen ab Windows 7. Hier im Buch verwende ich für alle Aufgaben aber Windows 10.

4.2.1 Einrichtung der »Remote Server Administration Tools« (RSAT)

Die Installation und Einrichtung der RSAT kann ein paar Minuten dauern, in denen es so aussieht, als würde auf dem System nichts passieren. Hier müssen Sie auf jeden Fall etwas Geduld haben und auf den Abschluss des Vorgangs warten.

Passen Sie den DNS-Server am Client an

Damit Sie den Client überhaupt erfolgreich in die Domäne aufnehmen können, müssen Sie dafür sorgen, dass auf der Workstation in den Einstellungen des Netzwerks der DNS-Server der neuen Domäne eingetragen ist. Ohne diesen Eintrag klappt der Beitritt zur Domäne nicht, da der Client den Domaincontroller über DNS sucht. Abbildung 4.1 zeigt die entsprechende Einstellung:

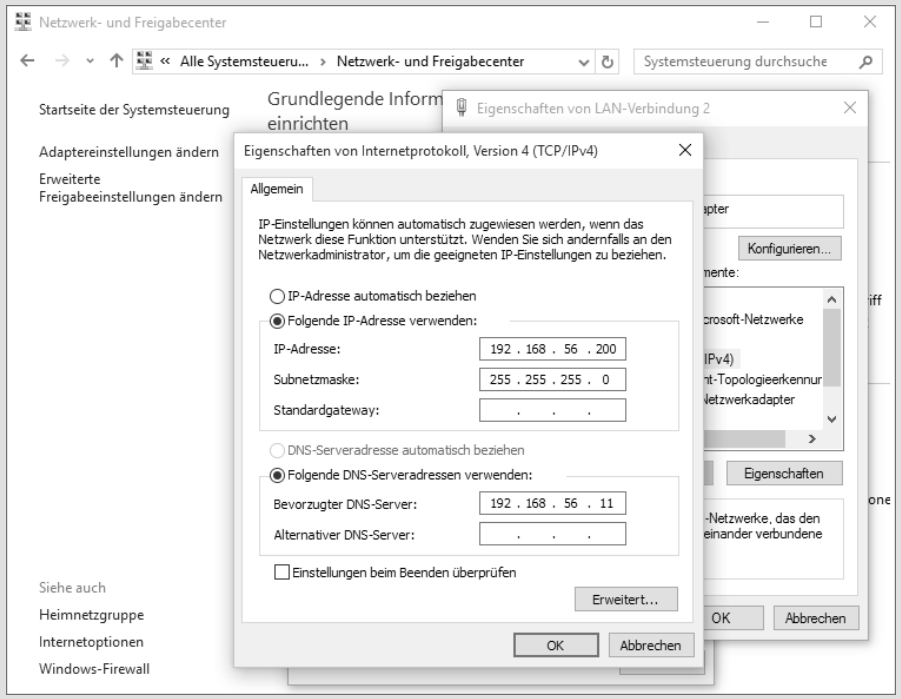


Abbildung 4.1 Client in die Domäne aufnehmen

Hierbei wird nicht nur der Name des Domaincontrollers über DNS gesucht, sondern auch die Dienste Kerberos und LDAP.

Um Benutzer und Gruppen über die Windows Remote Server Administration Tools (RSAT) verwalten zu können, müssen Sie mindestens einen Client mit Windows 7 Professional in Ihrer Domäne haben. Aus diesem Grund nehmen Sie jetzt erst einen

Windows-Rechner in die Domäne auf. Suchen Sie je nach Windows-Version die Einstellungen für die Arbeitsgruppe, und treten Sie der Domäne bei. Für den Beitritt benötigen Sie den *Administrator* und dessen Passwort. In Abbildung 4.2 sehen Sie alle Fenster für den Vorgang.

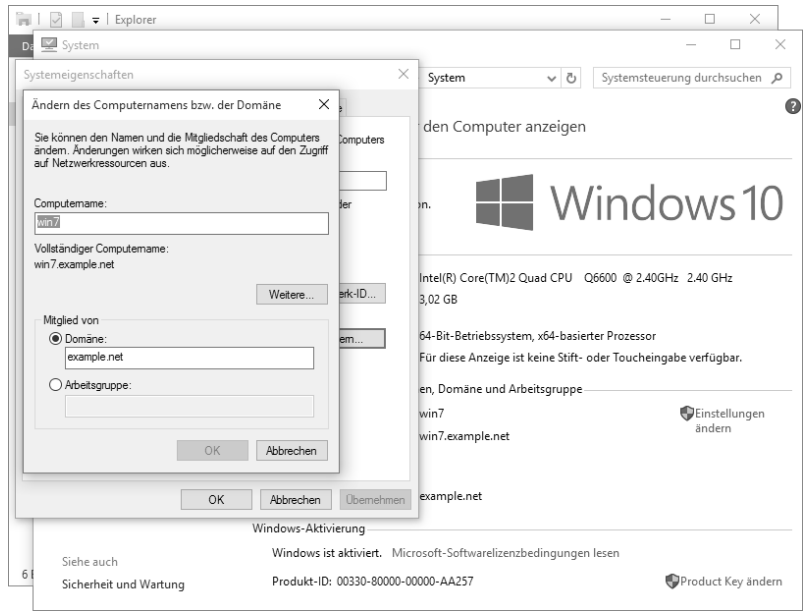


Abbildung 4.2 Client in die Domäne aufnehmen

Um die Einstellung wirksam werden zu lassen, müssen Sie Windows neu starten. Nach dem Neustart können Sie sich jetzt als *Domänenadministrator* oder mit einem anderen Domänenbenutzer anmelden.

Wenn Sie sich als *Administrator* anmelden, müssen Sie immer den Domänennamen voranstellen, da sonst eine Anmeldung als lokaler Administrator durchgeführt wird. Wenn Sie sich als Benutzer der Domäne anmelden, reicht der Benutzername.

Nachdem Sie sich als Domänenadministrator angemeldet haben, laden Sie die RSAT von der Microsoft-Webseite herunter und installieren sie. Bei den RSAT handelt es sich nicht um eine zusätzliche Software, sondern die RSAT werden wie ein Update behandelt und installiert. Die RSAT sind dabei immer abhängig von der verwendeten Windows-Version.

Unter Windows 7 können Sie die RSAT nach der Installation nicht sofort nutzen, Sie müssen sie erst aktivieren. Öffnen Sie hierfür die Systemsteuerung, und klicken Sie dann auf Programme und Funktionen. Dort klicken Sie dann auf Windows-Funktionen aktivieren oder deaktivieren. Es öffnet sich ein neues Fenster, in dem Sie

jetzt die RSAT über den Unterpunkt REMOTESERVER-VERWALTUNGSTOOLS aktivieren. Sie müssen alle Unterpunkte öffnen und dann alle gewünschten Funktionen separat aktivieren. Bei Windows 10 sind alle RSAT sofort aktiv. Abbildung 4.3 zeigt die aktivierten RSAT.

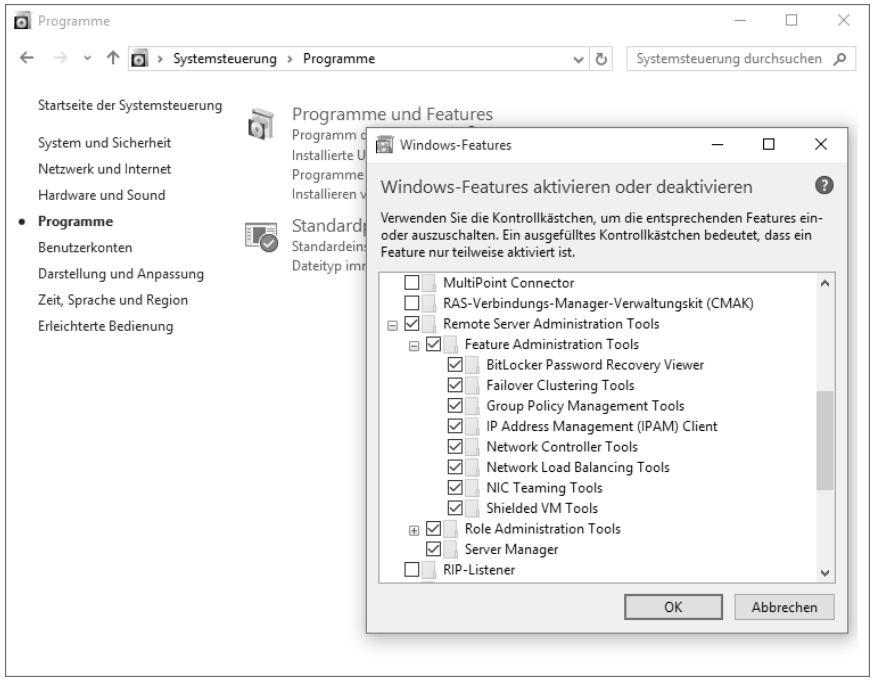


Abbildung 4.3 Konfiguration der RSAT

Anschließend klicken Sie auf OK. Jetzt werden die RSAT im System aktiviert, und Sie können über START • ALLE PROGRAMME • VERWALTUNG auf die RSAT zugreifen.

4.2.2 Benutzer- und Gruppenverwaltung mit den »RSAT«

Wenn Sie das Tool *Active Directory-Benutzer und -Computer* starten, können Sie die von Ihnen erstellte Domäne sehen und Benutzer und Gruppen verwalten. Eine Übersicht über alle Gruppen sehen Sie in Abbildung 4.4. Die vorher über die Kommandozeile erzeugten Benutzer und Gruppen sehen Sie im unteren Teil der Abbildung. Wenn Sie einen neuen Benutzer, eine neue Gruppe oder einen neuen Host anlegen wollen, führen Sie einen Rechtsklick auf die rechte Seite des Fensters aus. Dann öffnet sich ein Kontextmenü. Dort klicken Sie auf NEU, und es öffnet sich ein neues Menü, in dem Sie dann das entsprechende Objekt auswählen können.

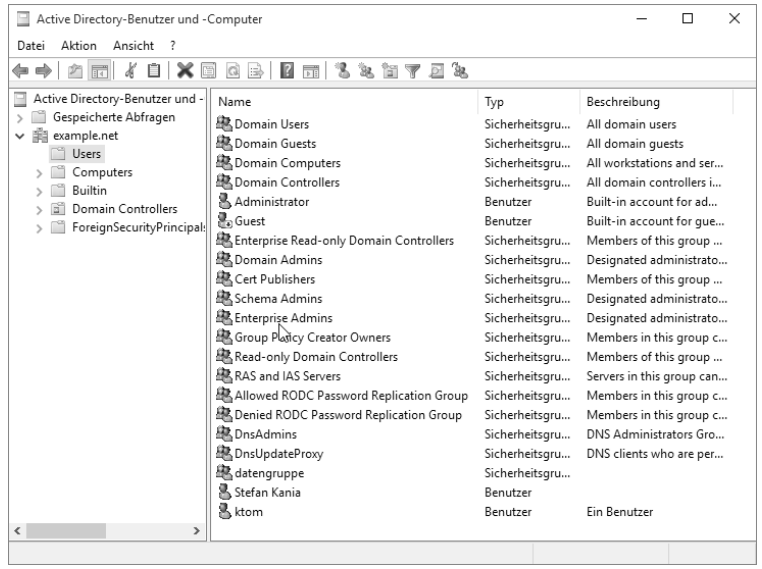


Abbildung 4.4 Übersicht über Benutzer und Gruppen in den »RSAT«

In Abbildung 4.5 sehen Sie als Beispiel das Anlegen eines neuen Benutzers.

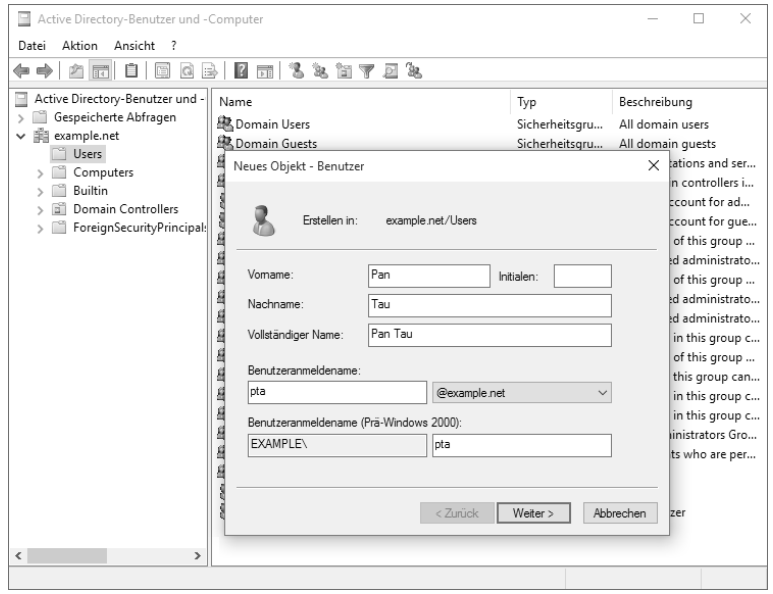


Abbildung 4.5 Anlegen eines neuen Benutzers

So können Sie jetzt Schritt für Schritt alle Benutzer und Gruppen über Ihren Windows-Client anlegen und verwalten.

4.3 Benutzer- und Gruppenverwaltung mit dem LAM

Der ein oder andere von Ihnen kennt den *LDAP Account Manager (LAM)* vielleicht schon als Werkzeug für den openLDAP. Seit der Version 4.2 ist der LAM auch in der Lage, Samba 4 zu verwalten. Da mit dem LAM eine Möglichkeit besteht, Samba 4 auch über einen Webzugriff zu verwalten, soll in diesem Abschnitt etwas genauer auf den LAM eingegangen werden.

4.3.1 Installation des LAM

Auch in dieser Auflage des Buches werde ich wieder auf den LAM eingehen, denn mit diesem Werkzeug sind Sie in der Lage, Ihre Benutzer und Gruppen über eine Webanwendung zu verwalten. Das ist oft von Vorteil, da Sie nicht immer einen Arbeitsplatz in der Nähe haben, auf dem die RSAT installiert sind. Auch bietet der LAM ein paar zusätzliche Funktionen, die die RSAT nicht bieten. So können Sie später bei der Wiederherstellung von gelöschten Objekten sehr einfach auf diese Objekte zugreifen.

Als Erstes müssen Sie den LAM installieren. Dazu laden Sie sich die aktuelle Version des LAM von der Webseite *https://www.ldap-account-manager.org/lamcms/releases* herunter.

Falls Sie die Heimatverzeichnisse der Benutzer automatisch auf einem Dateiserver anlegen wollen, wenn Sie einen Benutzer anlegen, dann müssen Sie zusätzlich das Paket *lamdaemon* mit herunterladen und installieren. Sie sollten den LAM immer auf einem eigenen Webserver installieren, um nicht in Konflikten mit anderen Diensten zu kommen. Ich werde den LAM hier im Buch auf einer eigenen Debian 8-Maschine installieren und konfigurieren, um dann die Domäne zu verwalten. Der Webserver verwendet den Domaincontroller als DNS-Server, so dass später der Name im Zertifikat des Domaincontrollers überprüft werden kann. Installieren Sie die Pakete mit dem Kommando `dpkg`. Bei der Installation kommt es zu nicht aufgelösten Abhängigkeiten. Diese können Sie mit `apt-get -f install` auflösen. In Listing 4.34 sehen Sie die Installation:

```
root@lam:~# dpkg -i ldap-account-manager_5.1-1_all.deb
Vormals nicht ausgewähltes Paket ldap-account-manager wird gewählt.
(Lese Datenbank ... 31967 Dateien und Verzeichnisse sind derzeit installiert.)
Vorbereitung zum Entpacken von ldap-account-manager_5.1-1_all.deb ...
Entpacken von ldap-account-manager (5.1-1) ...
dpkg: Abhängigkeitsprobleme verhindern Konfiguration von ldap-account-manager:
 ldap-account-manager hängt ab von php5 (>= 5.4.26); aber:
  Paket php5 ist nicht installiert.
 ldap-account-manager hängt ab von apache2 | httpd; aber:
  Paket apache2 ist nicht installiert.
  Paket httpd ist nicht installiert.
 ldap-account-manager hängt ab von php-fpdf (>= 1.7); aber:
  Paket php-fpdf ist nicht installiert.

dpkg: Fehler beim Bearbeiten des Paketes ldap-account-manager (--install):
 Abhängigkeitsprobleme - verbleibt unkonfiguriert
Fehler traten auf beim Bearbeiten von:
 ldap-account-manager

root@lam:~# apt-get -f install
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut.
Statusinformationen werden eingelesen.... Fertig
Abhängigkeiten werden korrigiert ... Fertig
Die folgenden zusätzlichen Pakete werden installiert:
  apache2 apache2-bin apache2-data apache2-utils
```

Listing 4.34 Installation des LAM

Nach der Installation können Sie den LAM jetzt über einen Browser erreichen. Geben Sie dafür in Ihrem Browser die URL *http://<ip-webserver>/lam* ein.

Daraufhin erhalten Sie das Fenster aus Abbildung 4.6.

Abbildung 4.6 Erster Zugriff auf den LAM

4.3.2 Konfiguration des LAM

Bevor Sie mit dem LAM Ihren Samba 4 administrieren können, müssen Sie den LAM erst konfigurieren. Klicken Sie dazu auf LAM CONFIGURATION in der oberen rechten Ecke des Startbildschirms. Sie erhalten daraufhin eine neue Ansicht. Dort wählen Sie den Punkt EDIT GENERAL SETTINGS. Bei der Abfrage nach dem Passwort geben Sie das Standardpasswort `lam` ein und klicken auf OK.

Auf der folgenden Seite können Sie Einstellungen für den LAM vornehmen. Alle Einstellungen zu den Passwörtern betreffen nur die Anmeldung am LAM und haben nichts mit den Einstellungen der Benutzer zu tun.

Für die Verwendung von *ldaps* anstelle von *ldap* müssen Sie hier auch das Zertifikat von Ihrem Domaincontroller importieren. Geben Sie den FQDN ihres Servers an, und klicken Sie anschließend auf IMPORT FROM SERVER. Sollte das direkte Importieren nicht funktionieren, können Sie sich die Datei */var/lib/samba/private/tls/cert.pem* von Ihrem Domaincontroller auf Ihren lokalen Rechner speichern und von dort aus als Datei einbinden. Beachten Sie, dass Sie, nachdem Sie das Zertifikat eingespielt haben, den Webserver auf jeden Fall neu starten müssen. Ändern Sie vor dem Neustart noch das Masterpasswort; dann speichern Sie die Änderungen, so wie es Abbildung 4.7 zeigt, und starten dann den Webserver neu.

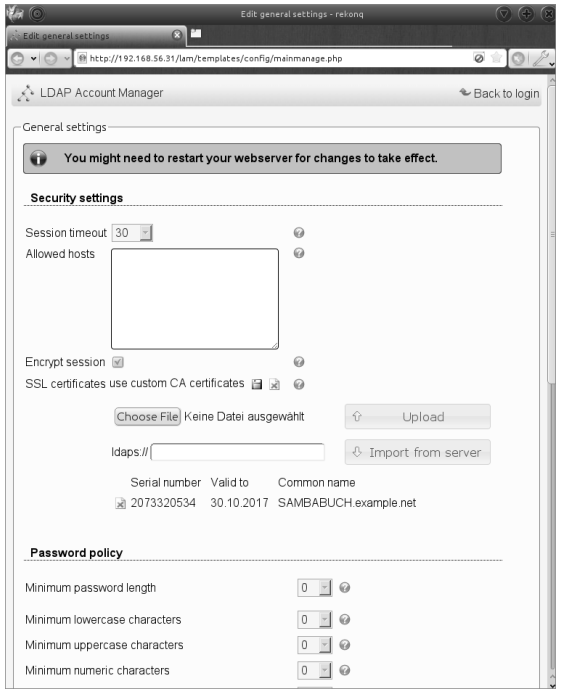


Abbildung 4.7 Setzen des Masterpassworts

Anschließend landen Sie wieder auf der Anmeldeseite des LAM. Klicken Sie hier wieder auf LAM CONFIGURATION. Jetzt geht es darum, ein Profil für Ihren Samba 4-Server zu erstellen. Sie können später über diesen Punkt weitere Profile erstellen, um andere LDAP- oder AD-Server zu verwalten.

Zwei verschiedene Accounttypen

Der LAM unterscheidet zwischen dem Hauptbenutzer, der Profile anlegen kann, und den Profilverwaltern, die nur das Profil verwalten können. Hierfür haben sie vom Hauptbenutzer das Passwort bekommen. Deshalb benötigen Sie nur eine Instanz des LAM, um alle Ihre Server zu verwalten.

Klicken Sie auf EDIT SERVER PROFILES. Um ein neues Profil für Ihren Samba 4-Dienst zu erstellen, klicken Sie auf MANAGE SERVER PROFILES. Daraufhin erhalten Sie ein neues Fenster (siehe Abbildung 4.8). Tragen Sie dort den Namen für Ihr Profil ein, und vergeben Sie ein Passwort, um später das Profil verwalten zu können. Wichtig ist hier, dass Sie als Template `windows_samba4` auswählen.

Abbildung 4.8 Erstellen eines Profils

Durch Anklicken der Schaltfläche ADD fügen Sie ein neues Profil zum LAM hinzu. Um das Profil auch anlegen zu können, werden Sie noch nach dem Masterpasswort gefragt. Danach gelangen Sie automatisch in das neu erstellte Profil. In dem Feld SERVER SETTINGS tragen Sie die Werte für Ihren Samba-Server ein. Die folgenden Werte müssen Sie hier eingeben:

- SERVER ADDRESS
  Geben Sie hier den FQDN Ihres Domaincontrollers ein – zusammen mit dem Port `386` und dem Protokoll `ldaps`. Dazu muss der Server, auf dem der LAM läuft, aber den Namen des Domaincontrollers über DNS auflösen können.
- ACTIVATE TLS
  Setzen Sie diesen Parameter unbedingt auf NO, da es sonst zu Konflikt mit `ldaps` führt, wenn Sie hier YES auswählen würden.
- TREE SUFFIX
  An dieser Stelle müssen Sie die oberste Ebene Ihres ADs angeben. Der Name ist identisch mit den DNS-Domänennamen. Im Buch ist es `dc=example,dc=net`.
- LDAP SEARCH LIMIT
  Diesen Wert müssen Sie nur ändern, wenn durch zu viele Suchergebnisse die Netzwerklast zu stark ansteigt. Ein Aussage über das »wann und wie viel« ist hier somit nicht möglich, das müssen Sie immer in Ihrer Umgebung testen. In Abbildung 4.9 sehen Sie eine Zusammenfassung der SERVER SETTINGS.

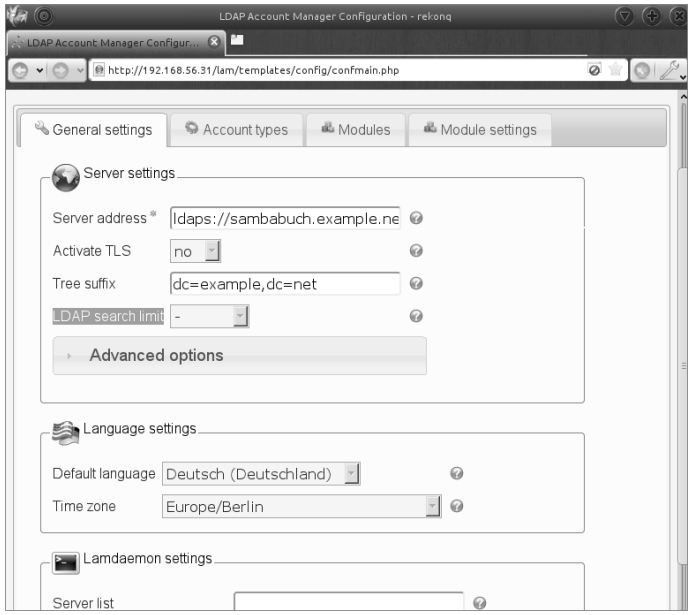


Abbildung 4.9 Zusammenfassung der »Server settings«

Bei den LANGUAGE SETTINGS können Sie die spätere Anzeigesprache für den LAM auswählen. Den Abschnitt LAMDAEMON SETTINGS können Sie im Moment überspringen; diese Parameter werden erst relevant, wenn Sie später den *lamdaemon* installieren und konfigurieren wollen.

Wichtig für die momentane Konfiguration ist nur noch der Abschnitt SECURITY SETTINGS. An dieser Stelle legen Sie fest, wer sich am LAM anmelden kann und wie die Liste der gültigen Benutzer erstellt und verwaltet wird.

Für die Verwaltung stehen Ihnen zwei Methoden zur Verfügung: zum einen über eine FIXED LIST und zum anderen LDAP-SEARCH. Bei FIXED LIST geben Sie jeden Benutzer aus dem AD einzeln an, der auf den LAM zugreifen darf.

Im Gegensatz dazu können alle Benutzer, die über eine LDAP-Suche ab einem bestimmten Punkt im AD gefunden werden, sich am LAM anmelden und administrativ tätig werden. Natürlich erhalten die Benutzer über den LAM keine zusätzlichen Rechte im AD, sodass die Benutzer nur diejenigen Objekte administrieren dürfen, auf die sie auch Rechte haben.

In Abbildung 4.10 sehen Sie die Einträge für eine FIXED LIST.

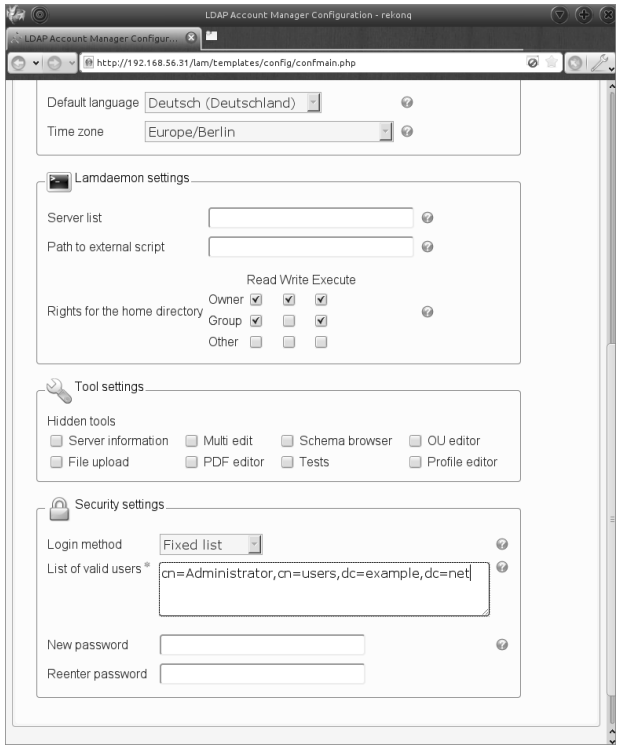


Abbildung 4.10 Login-Methode »Fixed list«

Anfangs kann nur der *Domainadministrator* zugreifen, der bei der Konfiguration des AD eingerichtet wurde.

Sie müssen also auf jeden Fall sicherstellen, dass dieser sich auch anmelden kann.

Nachdem Sie den Bereich SECURITY SETTINGS ausgefüllt haben, klicken Sie oben auf den Karteireiter ACCOUNT TYPES. Da Sie beim Anlegen des Profils bereits festgelegt haben, dass Sie eine Windows-Domäne verwalten wollen, sind an dieser Stelle schon die richtigen Accounttypen ausgewählt.

Sie müssen hier nur noch die Werte für Ihre Domäne angeben. Abbildung 4.11 zeigt die Einstellungen.

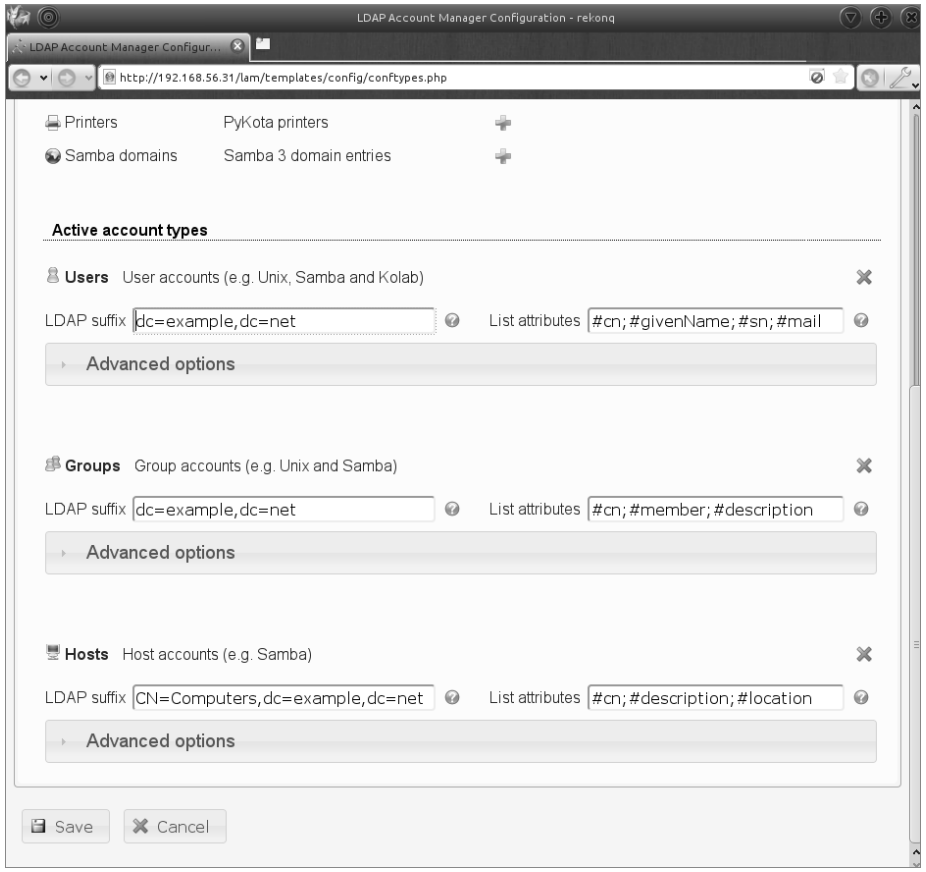


Abbildung 4.11 Auswahl der »Accounttypen«

Anschließend klicken Sie oben auf den Karteireiter MODULES. Hier müssen Sie nichts mehr ändern, wenn Sie bei der Erstellung des Profiles das Template `windows_samba4` ausgewählt haben.

Sowohl bei den Benutzern, als auch bei den Gruppen und den Hosts darf hier nur das entsprechende Windows-Modul ausgewählt werden, so wie Sie es in Abbildung 4.12 sehen.

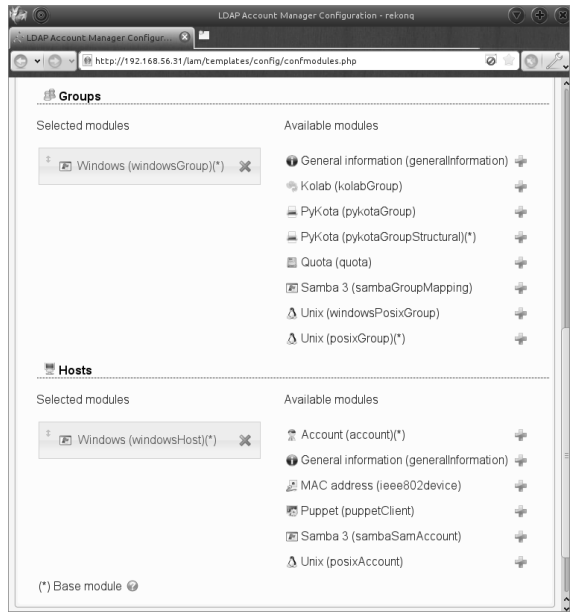


Abbildung 4.12 Module

Klicken Sie jetzt auf den Karteireiter MODULE SETTINGS und tragen Sie im Feld DOMAINS Ihre Domäne ein, so wie es Abbildung 4.13 zeigt.

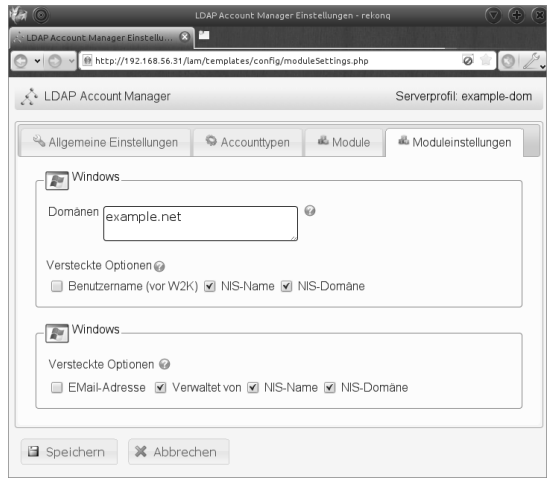


Abbildung 4.13 Modul settings

Jetzt können Sie am unteren Ende der Eingabemaske auf Speichern klicken, um das Profil zu speichern. Sie gelangen dann automatisch wieder auf die Anmeldemaske des Profils. Am oberen Rand der Maske sehen Sie die Meldung Your settings were sucessfully safed.

Damit ist der erste Schritt der Konfiguration des LAM abgeschlossen. Jetzt müssen Sie noch die Datei */etc/ldap/ldap.conf* anpassen, damit der LAM auch den LDAP Ihres ADs erreichen kann. Da Sie währen der Installation die Sprache festlegen können, werden Sie nach der Konfiguration den LAM in deutsch sehen, wenn Sie Deutsch als Sprache gewählt haben.

4.3.3 Arbeiten mit dem LAM

Nachdem Sie diese Einträge vorgenommen haben, können Sie sich jetzt das erste Mal am LAM mit Ihrem Domainadministrator anmelden. Jetzt haben Sie den LAM so weit, dass Sie die ersten Benutzer und Gruppen anlegen können. Über die Karteireiter Benutzer, Gruppen und Hosts können Sie jetzt bestehende Objekte verwalten oder neue anlegen.

Wenn Sie auf Baumansicht klicken, sehen Sie eine Übersicht über alle Objekte in Ihrem Active Directory. Abbildung 4.14 zeigt die Baumansicht.

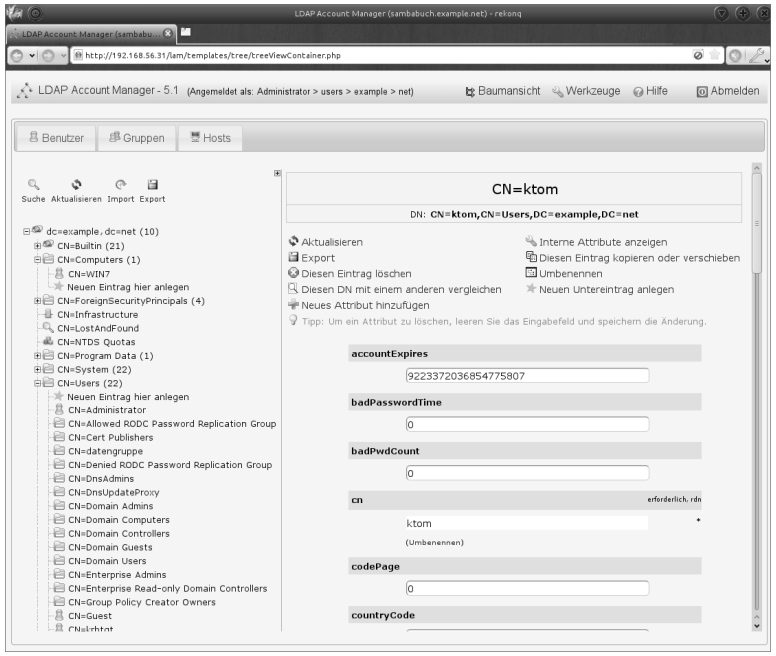


Abbildung 4.14 Die Baumansicht

Der große Vorteil der Baumansicht ist, dass Sie hier auch Attribute ergänzen können, die Sie in der Verwaltung auf der Übersichtsseite nicht sehen.

Denken Sie daran, dass der *LAM* noch nicht in der Lage ist, die Heimatverzeichnisse der neuen Benutzer anzulegen. Um die Heimatverzeichnisse auch gleich mit anzulegen, muss unbedingt der *lamdaemon* installiert und konfiguriert werden. Die Installation und Konfiguration ist aber nicht Bestandteil dieses Buches.

Mit dem LDAP Account Manager haben Sie ein Werkzeug, mit dem Sie, im Gegensatz zu den RSAT, Ihre Domäne auch browserbasiert verwalten können. Eine sehr gute Anleitung zur Einrichtung des LDAP Account Managers finden Sie auch unter *https://www.ldap-account-manager.org/static/doc/manual/ch03s02.html*.

Jetzt können Sie die Benutzer und Gruppen in Ihrer Domäne auf unterschiedliche Art und Weise verwalten. Wählen Sie den Weg, der für Sie am einfachsten ist. In den meisten Fällen werden Sie Benutzer und Gruppen sowohl über die Kommandozeile als auch über ein grafisches Werkzeug verwalten.

Kapitel 6

Verwaltung von Domaincontrollern

Jetzt wird es Zeit, über die Ausfallsicherheit Ihres Anmeldedienstes nachzudenken. Im Moment gibt es nur einen Domaincontroller, fällt dieser aus, steht Ihren Benutzern kein Anmeldedienst mehr zur Verfügung. Deshalb sollten Sie immer einen zweiten Domaincontroller in Ihrer Domain einrichten, um eine Ausfallsicherheit des Anmeldedienstes zu gewährleisten. Es kommt bestimmt irgendwann der Punkt, an dem Sie einen Ihrer Domaincontroller aus der Domäne entfernen wollen, auch diesen Vorgang werde ich in diesem Kapitel erklären.

Um Ihren Benutzern die Anmeldung an der Domäne immer zu ermöglichen, sollten Sie mindestens zwei Domaincontroller in der Domäne installieren. Selbst wenn einer der beiden Domaincontroller ausfallen sollte, können sich Ihre Benutzer immer noch in der Domäne anmelden.

Ein zweiter Domaincontroller ermöglicht es Ihnen auch, die Wartung der Systeme zu normalen Arbeitszeiten durchzuführen und nicht nachts oder am Wochenende.

Im ersten Teil dieses Kapitels geht es um die Installation eines zweiten Domaincontrollers in Ihrer Domäne, um die Ausfallsicherheit zu erhöhen. Auch ist eine Wartung der Systeme mit mindestens zwei Domaincontrollern in der Domäne einfacher, da Sie die Domaincontroller einzeln herunterfahren können und trotzdem der Anmeldedienst noch zur Verfügung steht.

Im zweiten Abschnitt werde ich Ihnen dann erklären, wie Sie einen Domaincontroller aus der Domäne entfernen können. Ich werde dabei auf zwei verschiedene Szenarien eingehen. Einmal auf den Fall, dass Sie einen Domaincontroller geplant aus der Domäne entfernen wollen, und anschließend auf den Fall, dass der Domaincontroller unwiderruflich ausgefallen ist.

6.1 Installation des neuen DCs

Als Erstes installieren Sie ein Linux-System Ihrer Wahl und installieren die benötigten Pakete für die Funktion eines Domaincontrollers. Führen Sie nach der Installation auf

gar keinen Fall ein Provisioning durch. Dadurch würden Sie eine neue Domäne einrichten und keinen zweiten Domaincontroller in die bestehende Domäne einbinden.

6.1.1 Konfiguration des DNS-Servers

Damit die Kommunikation zwischen den DCs über die Namen möglich ist, sollten Sie an dieser Stelle erst den DNS um den neuen Server erweitern.

Sollte bis zu diesem Zeitpunkt auch noch keine *Reverse-Zone* in Ihrem DNS eingerichtet worden sein, können Sie diesen Schritt jetzt auch noch vornehmen.

Sie haben die Möglichkeit, die gesamte Verwaltung des DNS-Servers entweder über die grafischen Windows-Werkzeuge für das DNS-Management durchzuführen oder alles über die Kommandozeile direkt auf dem Samba 4-Server zu realisieren. Ich möchte Ihnen in diesem Abschnitt beide Möglichkeiten vorstellen.

Einrichten des DNS-Servers über die Windows-Werkzeuge

Starten Sie unter Windows den *DNS-Manager*. Beim ersten Aufruf müssen Sie die IP-Adresse des Servers angeben, mit dem Sie sich verbinden wollen. Anschließend startet der DNS-Manager, und Sie sehen Ihren Server.

Ein Doppelklick auf den Server öffnet die untergeordnete Struktur. Dort sehen Sie die beiden Einträge Forward-Lookupzonen und Reverse-Lookupzonen. Wenn Sie die Ordner öffnen, sehen Sie, dass bis zu diesem Zeitpunkt nur eine Forward-Lookupzone verwaltet wird.

Sehen Sie sich dazu auch Abbildung 6.1 an.

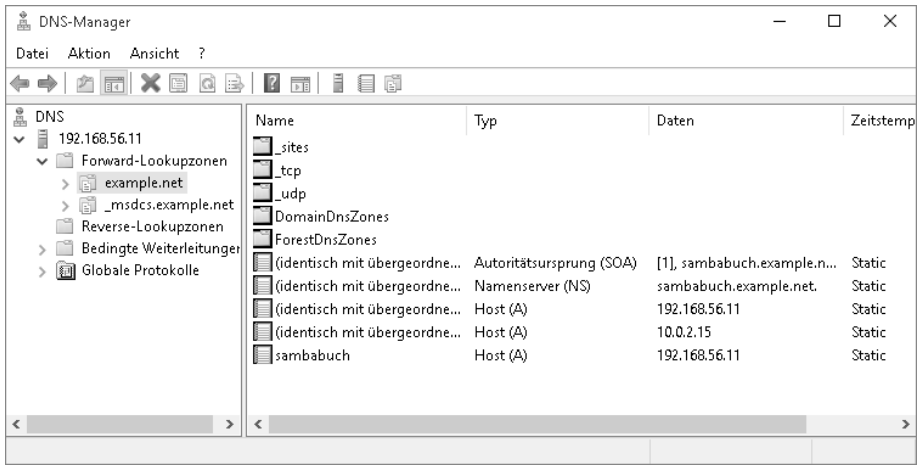


Abbildung 6.1 Zonenverwaltung über Windows

Mit einem Rechtsklick auf den Ordner Reverse-Lookupzonen öffnet sich ein Kontextmenü. Dort klicken Sie auf Neue Zone... Dadurch starten Sie einen Assistenten für die Erstellung einer neuen Zone. Klicken Sie hier auf Weiter.

Es öffnet sich ein neues Fenster. Dort wählen Sie den Punkt Primäre Zone aus und klicken anschließend auf Weiter. Anschließend legen Sie fest, wie die Zonen repliziert werden sollen.

Wählen Sie hier den Punkt Auf alle DNS-Server, die auf Domänencontrollern dieser Domäne ausgeführt werden aus, und klicken Sie anschließend auf Weiter.

Im nächsten Fenster legen Sie fest, ob Sie eine IPv4- oder eine IPv6-Zone anlegen wollen. Treffen Sie die für Ihr Netz passende Auswahl, und klicken Sie auf Weiter.

Wollen Sie sowohl eine IPv4- als auch eine IPv6-Zone anlegen, müssen Sie den Vorgang anschließend wiederholen.

Im nächsten Fenster geben Sie die Netzadresse Ihres Netzwerkes als Netzwerk-ID an. Daraus wird die neue Zone erstellt. In Abbildung 6.2 sehen Sie die entsprechenden Einstellungen.

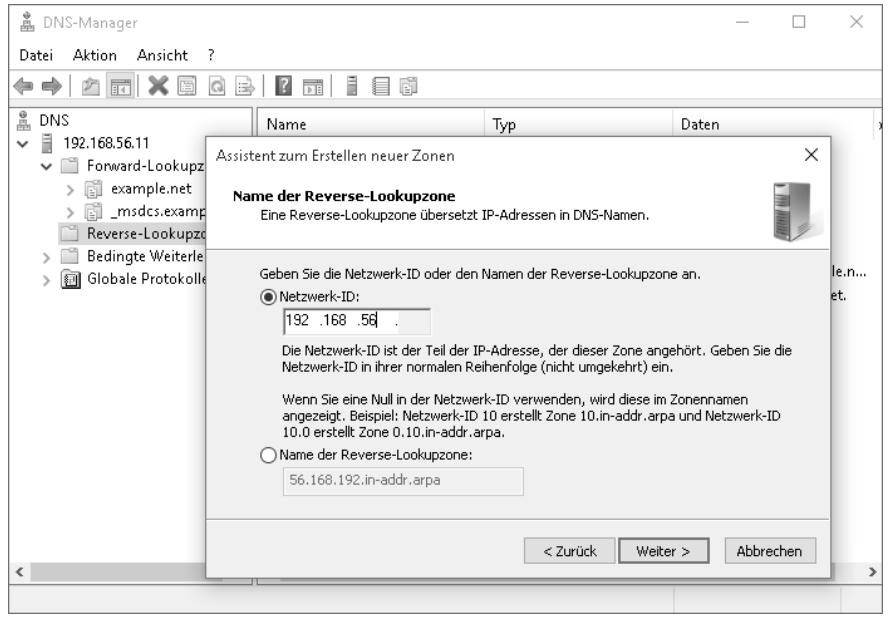


Abbildung 6.2 Die Einstellungen für die neue Reverse-Lookupzone

Klicken Sie anschließend auf Weiter. Wählen Sie im nächsten Schritt den Punkt Nur sichere dynamische Updates zulassen aus, und klicken Sie auf Weiter. Im Anschluss bekommen Sie eine Zusammenfassung der neuen Zone angezeigt.

In Abbildung 6.3 sehen Sie die Zusammenfassung.

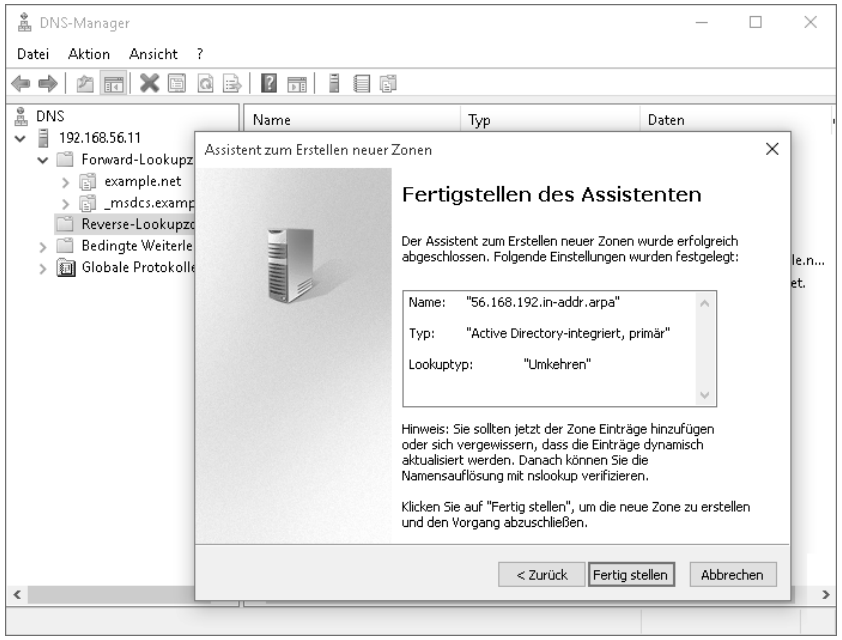


Abbildung 6.3 Zusammenfassung für die neue Reverse-Lookupzone

Jetzt klicken Sie auf FERTIG STELLEN, und die Zone wird angelegt. Anschließend sehen Sie die neue Zone wie in Abbildung 6.4.

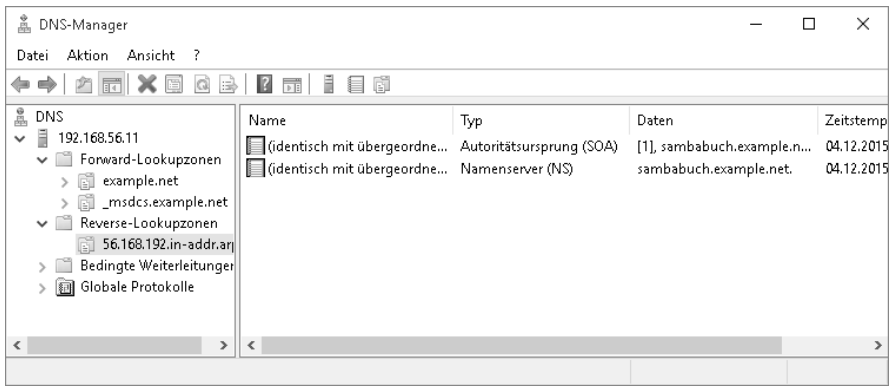


Abbildung 6.4 Die neue reverse-Lookupzone

Durch einen Rechtsklick in der rechten Seite des DNS-Managers können Sie jetzt einen neuen PTR-Record für alle bestehenden Systeme erstellen. In Abbildung 6.5 sehen Sie ein Beispiel für einen neuen *PTR-Record*.

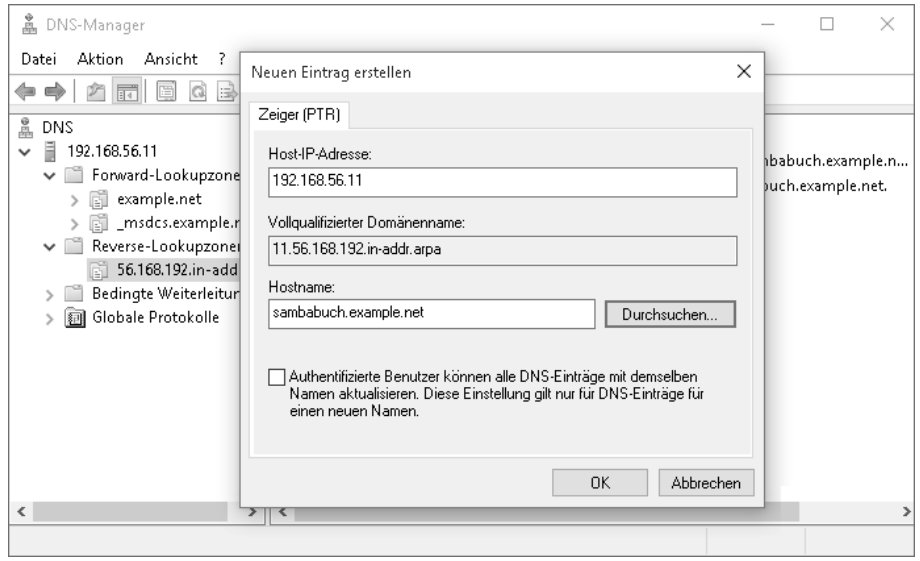


Abbildung 6.5 Ein neuer PTR-Record

Samba-Dienst neu starten

Der DNS-Server kann die Zonen nur beim Starten des Dienstes einlesen, deshalb müssen Sie nach dem Erstellen einer neuen Zone immer den Samba-Dienst neu starten, sonst können die Einträge nicht aufgelöst werden.

Es spielt dabei keine Rolle, ob Sie die Zone unter Windows oder über die Kommandozeile auf dem Domaincontroller erstellt haben.

Erzeugen Sie jetzt in der Forward-Lookupzone einen neuen Eintrag für den zweiten DC. Prüfen Sie anschließend, ob der Name auch richtig aufgelöst wird. Am einfachsten geht das auf dem ersten DC über die Kommandozeile mit dem Kommando `host`.

Einrichten des DNS über die Kommandozeile

Sie können den gesamten DNS-Server auch über die Kommandozeile realisieren – vom Einrichten einer neuen Zone bis zum Eintragen der Hosts in die Zonen. Im ersten Schritt müssen Sie eine neue Reverse-Lookupzone anlegen. In Listing 6.1 sehen Sie, wie die Zone erstellt wird:

```
root@sambabuch:~# samba-tool dns zonecreate sambabuch 56.168.192.in-addr.arpa \
                -k yes
Zone 56.168.192.in-addr.arpa created successfully
```

Listing 6.1 Anlegen einer neuen Reverse-Lookupzone

Jetzt können Sie als Erstes Ihren ersten DC in der Reverse-Lookupzone anlegen, so wie Sie es in Listing 6.2 sehen:

```
root@sambabuch:~# samba-tool dns add sambabuch 56.168.192.in-addr.arpa 11 PTR \
                sambabuch.example.net -k yes
Record added successfully
```

Listing 6.2 Einrichten des PTR-Eintrags für den ersten DC

In Listing 6.3 sehen Sie, wie Sie den Forward-Eintrag für den zweiten DNS-Server anlegen können:

```
root@sambabuch:~# samba-tool dns add sambabuch example.net sambabuch-dc2 \
                A 192.168.56.21 -k yes

Record added successfully
```

Listing 6.3 Anlegen des Forward-Eintrags für den zweiten DC

Jetzt fehlt nur noch der Reverse-Eintrag für den zweiten DC. In Listing 6.4 sehen Sie, wie Sie diesen Eintrag erstellen können:

```
root@sambabuch:~# samba-tool dns add sambabuch 56.168.192.in-addr.arpa 21 PTR \
                sambabuch-dc2.example.net -k yes

Record added successfully
```

Listing 6.4 Der Reverse-Eintrag für den zweiten DC

Jetzt können Sie die Namensauflösung mit dem Kommando `host` so wie in Listing 6.5 testen:

```
root@sambabuch:~# host 192.168.56.11
11.56.168.192.in-addr.arpa domain name pointer sambabuch.example.net.

root@sambabuch:~# host sambabuch
sambabuch.example.net has address 192.168.56.11

root@sambabuch:~# host sambabuch-dc2
sambabuch-dc2.example.net has address 192.168.56.21

root@sambabuch:~# host 192.168.56.11
11.56.168.192.in-addr.arpa domain name pointer sambabuch.example.net.

root@sambabuch:~# host 192.168.56.21
21.56.168.192.in-addr.arpa domain name pointer sambabuch-dc2.example.net.
```

Listing 6.5 Testen der Namensauflösung

Damit ist die Konfiguration des DNS-Servers abgeschlossen, und Sie können mit der Konfiguration des zweiten DCs beginnen.

6.2 Konfiguration des zweiten DCs

Auch für den zweiten DC ist Kerberos zur Authentifizierung der Benutzer notwendig. Darum müssen Sie als Erstes die Datei */etc/krb5.conf* vom ersten DC auf den neuen DC kopieren. Der Inhalt der Datei */etc/krb5.conf* muss wie in Listing 6.6 aussehen:

```
[libdefaults]
 dns_lookup_realm = true
 dns_lookup_kdc = true
 default_realm = EXAMPLE.NET
```

Listing 6.6 Die Datei »krb5.conf«

Installieren Sie, falls es noch nicht vorhanden ist, das Paket *heimdal-clients* auf dem neuen DC, um die Kerberos-Authentifizierung testen zu können. Jetzt können Sie so, wie Sie es in Listing 6.7 sehen, die Kerberos-Authentifizierung testen:

```
root@sambabuch-dc2:~# kinit administrator
administrator@EXAMPLE.NET's Password:

root@sambabuch-dc2:~# klist
Credentials cache: FILE:/tmp/krb5cc_0
        Principal: administrator@EXAMPLE.NET

  Issued                Expires               Principal
Dec  4 21:53:50 2015  Dec  5 07:53:50 2015  krbtgt/EXAMPLE.NET@EXAMPLE.NET
```

Listing 6.7 Testen von Kerberos

Fahren Sie mit der Konfiguration des neuen DCs erst fort, wenn die Authentifizierung funktioniert. Damit stellen Sie auch sicher, dass alle benötigten Dienste über DNS aufgelöst werden können.

Jetzt können Sie den neuen DC zur Domäne hinzufügen. Dazu verwenden Sie wieder das Kommando `samba-tool`, wie Sie in Listing 6.8 sehen:

```
root@sambabuch-dc2:~# samba-tool domain join example.net DC \
                     --realm=example.net -Uadministrator

Finding a writeable DC for domain 'example.net'
Found DC sambabuch.example.net
Password for [WORKGROUP\administrator]:
```

```
workgroup is EXAMPLE
realm is example.net
checking sAMAccountName
Adding CN=SAMBABUCH-DC2,OU=Domain Controllers,DC=example,DC=net
Adding CN=SAMBABUCH-DC2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,\
       CN=Configuration,DC=example,DC=net
Adding CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
       CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
Adding SPNs to CN=SAMBABUCH-DC2,OU=Domain Controllers,DC=example,DC=net
Setting account password for SAMBABUCH-DC2$
Enabling account
Calling bare provision
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.56.21
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
A Kerberos configuration suitable for Samba 4 has been generated \
          at /var/lib/samba/private/krb5.conf
Provision OK for domain DN DC=example,DC=net

Starting replication
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net]\
          objects[402/1550] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net]\
          objects[804/1550] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net]\
          objects[1206/1550] linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net]\
          objects[1550/1550] linked_values[0/0]
Analyze and apply schema objects
Partition[CN=Configuration,DC=example,DC=net]\
          objects[402/1614] linked_values[0/0]
Partition[CN=Configuration,DC=example,DC=net]\
          objects[804/1614] linked_values[0/0]
```



```
Partition[CN=Configuration,DC=example,DC=net]\
          objects[1206/1614] linked_values[0/0]
Partition[CN=Configuration,DC=example,DC=net]\
          objects[1608/1614] linked_values[0/0]
Partition[CN=Configuration,DC=example,DC=net]\
          objects[1614/1614] linked_values[28/0]
Replicating critical objects from the base DN of\
          the domain
Partition[DC=example,DC=net] objects[97/97]\
          linked_values[23/0]
Partition[DC=example,DC=net] objects[311/214]\
          linked_values[24/0]
Done with always replicated NC (base, config, schema)
Replicating DC=DomainDnsZones,DC=example,DC=net
Partition[DC=DomainDnsZones,DC=example,DC=net]\
          objects[45/45] 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
Sending DsReplicaUpdateRefs for all the replicated partitions
Setting isSynchronized and dsServiceName
Setting up secrets database

Joined domain EXAMPLE (SID S-1-5-21-2641355115-960991230-4068238628) as a DC
```

Listing 6.8 Konfiguration des zweiten DCs

Hier sehen Sie genau, was alles beim Eintritt in die Domäne passiert. In der letzten Zeile erscheint die Meldung, dass der Rechner der Domäne beigetreten ist, und zwar als neuer DC.

Den Forwarder nicht vergessen

Während dieses Vorgangs wird eine Datei */etc/samba/smb.conf* generiert, aber leider wird der `dns forwarder` nicht vom ersten Domaincontroller übernommen.

Diesen Eintrag müssen Sie von Hand zur Konfiguration hinzufügen.

Jetzt müssen Sie noch dafür sorgen, dass der neue Samba 4-DC auch startet. Die Schritte für den Start des Domaincontrollers sind wieder abhängig von der Art und Weise, wie Sie Samba installiert haben und der Distribution, die Sie nutzen.

6.2.1 Testen des neuen Domaincontrollers

Um die Funktion des neuen DCs zu testen, fragen Sie als Erstes die Domäneninformationen so wie in Listing 6.9 ab:

```
root@sambabuch-dc2:~# samba-tool domain info 192.168.56.21
Forest           : example.net
Domain           : example.net
Netbios domain   : EXAMPLE
DC name          : sambabuch-dc2.example.net
DC netbios name  : SAMBABUCH-DC2
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

Listing 6.9 Anzeige der Domäneninformationen

Als IP-Adresse geben Sie hier die IP-Adresse des neuen DCs an.

Im nächsten Schritt prüfen Sie, ob die *objectGUID* des neuen DCs auch auflösbar ist. Wie das geht, sehen Sie in Listing 6.10:

```
root@sambabuch-dc2:~# ldbsearch -H /var/lib/samba/private/sam.ldb \
                      '(invocationid=*)' --cross-ncs objectguid

# record 1
dn: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,CN=Default-First-Site-Name,\
    CN=Sites,CN=Configuration,DC=example,DC=net

objectGUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477

# record 2
dn: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,CN=Default-First-Site-Name,\
    CN=Sites,CN=Configuration,DC=example,DC=net

objectGUID: f63cbf74-fc55-4839-87b1-f6ef96c155c1

# returned 2 records
# 2 entries
# 0 referrals
```

Listing 6.10 Test der »objectGUIDs«

Hier sehen Sie die *objectGUID*s der beiden DCs Ihrer Domäne. Diese *objectGUID*s benötigen Sie für den folgenden Test. Denn im nächsten Test prüfen Sie, ob die Funktion des DCs auch über den DNS erreichbar ist.

In Listing 6.11 sehen Sie, wie Sie die Prüfung durchführen:


```
root@sambabuch-dc2:~# host -t CNAME f63cbf74-fc55-4839-87b1-f6ef96c155c1.\
                      _msdcs.example.net
f63cbf74-fc55-4839-87b1-f6ef96c155c1._msdcs.example.net is an alias \
                      for sambabuch.example.net.

root@sambabuch-dc2:~# host -t CNAME 672d0a4f-cf92-4383-ad5b-da88ab12d477.\
                      _msdcs.example.net
672d0a4f-cf92-4383-ad5b-da88ab12d477._msdcs.example.net is an alias \
                       for sambabuch-dc2.example.net.
```

Listing 6.11 Auflösen der »opjectGUID«

Sie sehen: Beide DCs werden über den DNS aufgelöst, und der Dienst steht somit allen Clients in der Domäne zur Verfügung. Bevor Sie die Replikation prüfen, führen Sie noch einen Konsistenztest durch. Dieser Test prüft, ob die Datenbanken der DCs konsistent sind. Die Befehle dazu sehen Sie in Listing 6.12:

```
root@sambabuch-dc2:~# samba-tool drs kcc -U administrator \
                      sambabuch.example.net
Password for [EXAMPLE\administrator]:
Consistency check on sambabuch.example.net successful.

root@sambabuch-dc2:~# samba-tool drs kcc -U administrator \
                      sambabuch-dc2.example.net
Password for [EXAMPLE\administrator]:
Consistency check on sambabuch-dc2.example.net successful.
```

Listing 6.12 Durchführung des Konsistenztests

Sind beide DCs konsistent, kommt der letzte Test: die Prüfung, ob die Replikation der SAM-Datenbank funktioniert. In Listing 6.13 sehen Sie die Prüfung der Replikation:

```
root@sambabuch:~# samba-tool drs showrepl

Default-First-Site-Name\SAMBABUCH
DSA Options: 0x00000001
DSA object GUID: f63cbf74-fc55-4839-87b1-f6ef96c155c1
DSA invocationId: e8bfd7e8-5822-494b-91dc-d60bb5e56032

==== INBOUND NEIGHBORS ====

DC=ForestDnsZones,DC=example,DC=net
        Default-First-Site-Name\SAMBABUCH-DC2 via RPC
                DSA object GUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477
                Last attempt @ Mon Dec 14 18:36:34 2015 CET was successful
```

```
                0 consecutive failure(s).
                Last success @ Mon Dec 14 18:36:34 2015 CET

DC=DomainDnsZones,DC=example,DC=net
        Default-First-Site-Name\SAMBABUCH-DC2 via RPC
                DSA object GUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477
                Last attempt @ Mon Dec 14 18:36:34 2015 CET was successful
                0 consecutive failure(s).
                Last success @ Mon Dec 14 18:36:34 2015 CET

DC=example,DC=net
        Default-First-Site-Name\SAMBABUCH-DC2 via RPC
                DSA object GUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477
                Last attempt @ Mon Dec 14 18:36:50 2015 CET was successful
                0 consecutive failure(s).
                Last success @ Mon Dec 14 18:36:50 2015 CET

CN=Schema,CN=Configuration,DC=example,DC=net
        Default-First-Site-Name\SAMBABUCH-DC2 via RPC
                DSA object GUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477
                Last attempt @ Mon Dec 14 18:36:34 2015 CET was successful
                0 consecutive failure(s).
                Last success @ Mon Dec 14 18:36:34 2015 CET

CN=Configuration,DC=example,DC=net
        Default-First-Site-Name\SAMBABUCH-DC2 via RPC
                DSA object GUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477
                Last attempt @ Mon Dec 14 18:36:34 2015 CET was successful
                0 consecutive failure(s).
                Last success @ Mon Dec 14 18:36:34 2015 CET

==== OUTBOUND NEIGHBORS ====

DC=ForestDnsZones,DC=example,DC=net
        Default-First-Site-Name\SAMBABUCH-DC2 via RPC
                DSA object GUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

DC=DomainDnsZones,DC=example,DC=net
        Default-First-Site-Name\SAMBABUCH-DC2 via RPC
                DSA object GUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477
```



```
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

DC=example,DC=net
        Default-First-Site-Name\SAMBABUCH-DC2 via RPC
                DSA object GUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

CN=Schema,CN=Configuration,DC=example,DC=net
        Default-First-Site-Name\SAMBABUCH-DC2 via RPC
                DSA object GUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

CN=Configuration,DC=example,DC=net
        Default-First-Site-Name\SAMBABUCH-DC2 via RPC
                DSA object GUID: 672d0a4f-cf92-4383-ad5b-da88ab12d477
                Last attempt @ NTTIME(0) was successful
                0 consecutive failure(s).
                Last success @ NTTIME(0)

==== KCC CONNECTION OBJECTS ====

Connection --
        Connection name: c9f2a41a-732f-4407-9e55-7ee4e62dc074
        Enabled        : TRUE
        Server DNS name : sambabuch-dc2.example.net
        Server DN name  : CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
               CN=Default-First-Site-Name,CN=Sites,CN=Configuration,\
               DC=example,DC=net
                TransportType: RPC
                options: 0x00000001
Warning: No NC replicated for Connection!
```

Listing 6.13 Prüfung der Replikation

Auf beiden DCs sollte bei allen Tests ein `was successful` erscheinen. Sollte das nicht der Fall sein, prüfen Sie erneut, ob die Namensauflösung funktioniert und ob Sie eventuell eine IPv6-Adresse ansprechen, die im DNS eingetragen ist, die der DC aber nicht mehr besitzt.

Jetzt können Sie – am einfachsten über die RSAT – eine Änderung an einem Objekt vornehmen und dann in den RSAT auf den zweiten DC umschalten und prüfen, ob die Veränderung auch an dem zweiten DC angekommen ist. Führen Sie diesen Test an beiden DCs aus, und testen Sie jeweils das Ergebnis.

Um in den RSAT auf den jeweils anderen DC umschalten zu können, öffnen Sie das RSAT *Active Directory-Benutzer und -Computer*, klicken mit der rechten Maustaste auf die oberste Ebene und wählen dann den Punkt Domänencontroller ändern... Es erscheint dann ein Fenster, so wie in Abbildung 6.6, in dem Sie den jeweiligen DC auswählen können.

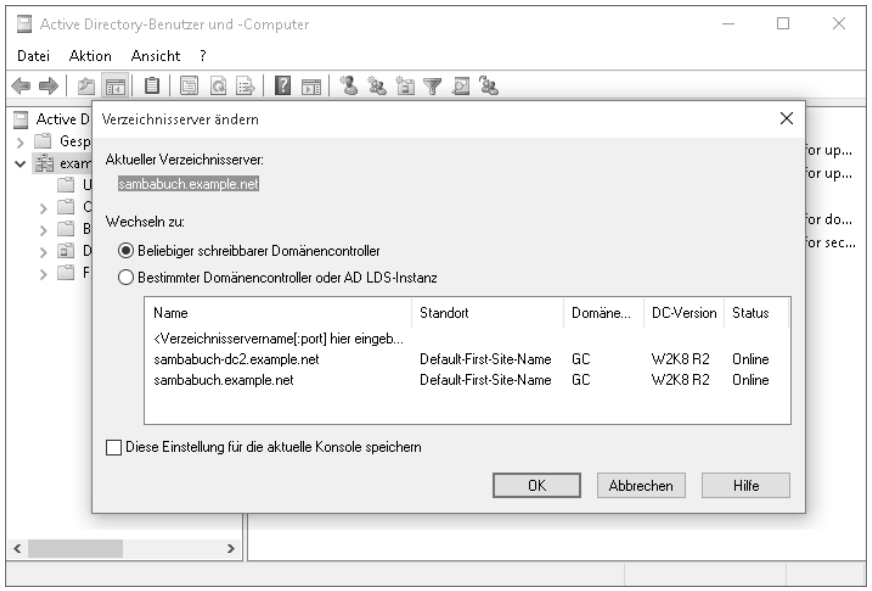


Abbildung 6.6 Auswahl eines Domaincontrollers

Damit Ihre Clients bei der Anmeldung am zweiten Domaincontroller auch die Uhrzeit setzen können, müssen Sie jetzt noch – wie schon beim ersten Domaincontroller – einen Zeitserver einrichten.

Nach der Installation des `ntp` erstellen Sie wieder die Konfigurationsdatei */etc/ntp.conf* wie in Listing 6.14:

```
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
```

Listing 6.14 Die Datei »ntpd.conf«

Jetzt müssen Sie auch wieder dafür sorgen, dass der *ntp* auch auf den Socket von Samba zugreifen kann. Dazu müssen Sie die Rechte wie in Listing 6.15 setzen:

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

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

Listing 6.15 Rechte für den Socket setzen

Damit ist die Konfiguration des zusätzlichen DCs für die Benutzerdatenbank abgeschlossen. Jetzt haben Sie zwei DCs und zwei DNS-Server in Ihrer Domäne, denn der DNS-Server wird gleich mit repliziert.

So können Sie jederzeit weitere DCs in Ihre Domäne einbinden. Nach dem Anlegen eines DCs können Sie diesen auch an einen anderen Standort verschieben.

6.3 Replikation der Freigabe »sysvol«

Bei mehreren DCs können sich ja alle Benutzer an jedem beliebigen DC anmelden. Damit dann auch die Logon-Skripte und die Gruppenrichtlinien wirksam werden, müssen diese bei allen DCs in der Freigabe *sysvol* liegen.

Da Samba 4 im Moment noch keine Dateisystemreplikation durchführen kann, müssen Sie einen anderen Weg finden, um die Replikation durchführen zu können. Am einfachsten ist die Verwendung von rsync. In diesem Abschnitt sehen Sie, wie Sie die Replikation einrichten und prüfen.

Das Problem bei rsync ist, dass Sie nur in eine Richtung replizieren können. Würden Änderungen an beiden Seiten vorgenommen, so würden Änderungen überschrieben. Daher müssen Sie die Replikation genau planen. Sie benötigen immer einen DC, auf dem Sie die Änderungen durchführen, und alle anderen DCs erhalten dann die Replikation.

Wählen Sie den DC als Master, auf dem die FSMO-Rolle *PDC-Master* läuft. Bei der Verwaltung der Gruppenrichtlinien und der Logon-Skripte dürfen Sie Änderungen nur noch dort vornehmen. Mit den RSAT zur Verwaltung der Gruppenrichtlinien können Sie den Server, auf dem die Gruppenrichtlinien bearbeitet werden sollen, aber vorein-

stellen. Dadurch erstellen und ändern Sie Gruppenrichtlinien automatisch auf dem richtigen Server.

In den folgenden Schritten wird erst die Replikation eingerichtet und getestet, und anschließend werden die RSAT eingestellt.

6.3.1 Testen der FSMO-Rolle

Im ersten Schritt müssen Sie den *PDC-Master* ermitteln. Ihn können Sie am einfachsten über die Kommandozeile an einem der DCs ermitteln. In Listing 6.16 sehen Sie, wie Sie vorgehen müssen, um den *PDC-Master* herauszufinden:

```
root@sambabuch:~# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
InfrastructureMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
RidAllocationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
DomainNamingMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
```

Listing 6.16 Ermittlung des »PDC-Masters«

Erst mit Version 4.3 werden alle Rollen angezeigt

Erst mit Samba-Version 4.3 werden die beiden Rollen `DomainDnsZonesMasterRole` und `ForestDnsZonesMasterRole` angezeigt. Auch können diese Rollen erst ab Version 4.3 mit dem Kommando `samba-tool` verschoben werden. In Abschnitt 6.4, »Die FSMO-Rollen«, gehe ich näher auf diese Problematik ein und zeige Ihnen eine Lösung für ältere Versionen.

Wie Sie sehen können, werden hier alle Rollen aufgeführt. Im Beispiel sehen Sie auch, dass der DC `sambabuch` der *PDC-Master* ist. Nur auf diesem DC dürfen Sie Gruppenrichtlinien und Logon-Skripte ändern und erstellen. Alle anderen DCs erhalten später die Informationen über rsync.

6.3.2 Einrichten von rsync auf dem »PDC-Master«

Auf dem PDC-Master brauchen Sie neben dem Programm rsync auch noch den *xinetd*, um den *rsync-Server* starten zu können. Installieren Sie die Pakete *rsync* und *xinetd* auf dem entsprechenden DC.

Anschließend müssen Sie für den *xinetd* eine Konfigurationsdatei *rsync* im Verzeichnis */etc/xinetd.d* erstellen.

In Listing 6.17 sehen Sie den Inhalt dieser Datei:

```
service rsync
{
   disable         = no
   only_from       = 192.168.56.21
   socket_type     = stream
   wait            = no
   user            = root
   server          = /usr/bin/rsync
   server_args     = --daemon
   log_on_failure += USERID
}
```

Listing 6.17 Konfigurationsdatei für »rsync«

Grenzen Sie den Zugriff ein

Durch die Zeile `only_from = 192.168.56.21` legen Sie fest, dass nur der zusätzliche Domaincontroller die Daten replizieren kann. Weitere Domaincontroller können Sie, durch Leerzeichen getrennt, in der Zeile eintragen.

Im nächsten Schritt müssen Sie den rsync-Server konfigurieren. Diese Konfiguration führen Sie über die Datei */etc/rsyncd.conf* durch. Wenn diese Datei nicht vorhanden ist, erstellen Sie sie. Die Datei muss den Inhalt aus Listing 6.18 haben:

```
[sysvol]
path = /var/lib/samba/sysvol/
comment = Samba sysvol
uid = root
gid = root
read only = yes
auth users = sysvol-repl
secrets file = /etc/samba/rsync.secret
```

Listing 6.18 Inhalt der Konfigurationsdatei des rsyncd

In die Datei */etc/samba/rsync.secret* tragen Sie den Benutzer ein, den Sie in dieser Datei als `auth user` eingetragen haben, und das Passwort, das dieser Benutzer verwenden soll. Ein Beispiel dafür sehen Sie in Listing 6.19:

```
sysvol-repl:geheim
```

Listing 6.19 Daten für die Authentifizierung

Der Benutzername und das Passwort werden durch einen Doppelpunkt getrennt. Sorgen Sie dafür, dass *other* keinen Zugriff auf die Datei hat.

Starten Sie anschließend den *xinetd* neu. In der Datei */var/log/syslog* finden Sie die Meldungen wie in Listing 6.20:

```
root@sambabuch:~# tail  -20 /var/log/syslog
Dec 22 09:53:15 sambabuch xinetd[18282]: Stopping internet\
                superserver: xinetd.
Dec 22 09:53:15 sambabuch xinetd[18287]: Starting internet\
                superserver: xinetd.
Dec 22 09:53:15 sambabuch xinetd[18295]: Reading included\
                configuration file: /etc/xinetd.d/chargen\
                [file=/etc/xinetd.conf] [line=14]
Dec 22 09:53:15 sambabuch xinetd[18295]: Reading included\
                configuration file: /etc/xinetd.d/daytime\
                [file=/etc/xinetd.d/daytime] [line=28]
Dec 22 09:53:15 sambabuch xinetd[18295]: Reading included\
                configuration file: /etc/xinetd.d/discard\
                [file=/etc/xinetd.d/discard] [line=26]
Dec 22 09:53:15 sambabuch xinetd[18295]: Reading included\
                configuration file: /etc/xinetd.d/echo\
                [file=/etc/xinetd.d/echo] [line=25]
Dec 22 09:53:15 sambabuch xinetd[18295]: Reading included\
                configuration file: /etc/xinetd.d/rsync\
                [file=/etc/xinetd.d/rsync] [line=26]
Dec 22 09:53:15 sambabuch xinetd[18295]: Reading included\
                configuration file: /etc/xinetd.d/time\
                [file=/etc/xinetd.d/time] [line=11]
Dec 22 09:53:15 sambabuch xinetd[18295]: removing chargen
Dec 22 09:53:15 sambabuch xinetd[18295]: removing chargen
Dec 22 09:53:15 sambabuch xinetd[18295]: removing daytime
Dec 22 09:53:15 sambabuch xinetd[18295]: removing daytime
Dec 22 09:53:15 sambabuch xinetd[18295]: removing discard
Dec 22 09:53:15 sambabuch xinetd[18295]: removing discard
Dec 22 09:53:15 sambabuch xinetd[18295]: removing echo
Dec 22 09:53:15 sambabuch xinetd[18295]: removing echo
```



```
Dec 22 09:53:15 sambabuch xinetd[18295]: removing time
Dec 22 09:53:15 sambabuch xinetd[18295]: removing time
Dec 22 09:53:15 sambabuch xinetd[18295]: xinetd Version 2.3.15\
                started with libwrap loadavg options compiled in.
Dec 22 09:53:15 sambabuch xinetd[18295]: Started working: 1 available service
```

Listing 6.20 Auszug aus der Datei »/var/log/syslog«

Hier sehen Sie, dass die Datei zur Konfiguration des *rsyncd* abgearbeitet wurde. Mit dem Kommando `netstat` können Sie dann noch testen, ob der Port auch erreichbar ist. In Listing 6.21 sehen Sie diesen Test:

```
root@sambabuch:~# netstat -tlp | grep xinetd
tcp    0      0 *:rsync    *:*     LISTEN      18295/xinetd
```

Listing 6.21 Prüfung des Ports für »rsyncd«

Das zeigt, dass der rsync über den *xinetd* erreichbar ist.

6.3.3 Konfiguration aller anderen DCs

Auf allen weiteren DCs müssen Sie ebenfalls rsync installieren. Den *xinetd* benötigen Sie dort nicht, da es sich hierbei immer nur um einen rsync-Client handelt. Nach der Installation von *rsync* erstellen Sie eine Datei, in der nur das Passwort für den Zugriff auf den rsync-Server abgelegt wird. Hier im Beispiel soll es die Datei */etc/samba/rsync.pass* sein. Achten Sie hier auch wieder darauf, dass `other` keinen Zugriff auf die Datei hat.

Jetzt können Sie die Replikation testen. Verwenden Sie beim Testen auf jeden Fall den Parameter `--dry-run`. Damit verhindern Sie, dass die Replikation wirklich durchgeführt wird. Erst wenn das Ergebnis des Tests stimmt, sollten Sie die Replikation starten. In Listing 6.22 sehen Sie den Test der Replikation:

```
root@sambabuch-dc2:~# rsync --dry-run -XAavz --delete-after\
              --password-file=/etc/samba/rsync.pass\
              rsync://sysvol-repl@sambabuch/sysvol/ /var/lib/samba/sysvol/

receiving file list ... done
./
example.net/
example.net/Policies/
example.net/Policies/31B2F340-016D-11D2-945F-00C04FB984F9/
example.net/Policies/31B2F340-016D-11D2-945F-00C04FB984F9/GPT.INI
example.net/Policies/31B2F340-016D-11D2-945F-00C04FB984F9/MACHINE/
example.net/Policies/31B2F340-016D-11D2-945F-00C04FB984F9/USER/
```

```
example.net/Policies/6AC1786C-016F-11D2-945F-00C04FB984F9/
example.net/Policies/6AC1786C-016F-11D2-945F-00C04FB984F9/GPT.INI
example.net/Policies/6AC1786C-016F-11D2-945F-00C04FB984F9/MACHINE/
example.net/Policies/6AC1786C-016F-11D2-945F-00C04FB984F9/USER/
example.net/scripts/
example.net/scripts/WindowsTH-KB2693643-x64.msu

sent 62 bytes  received 1,459 bytes  3,042.00 bytes/sec
total size is 96,656,138  speedup is 63,547.76 (DRY RUN)
```

Listing 6.22 Test der Replikation

Hier sehen Sie, dass alle Gruppenrichtlinien und das Logon-Skript erfolgreich übertragen wurden.

[+]

Achten Sie auf die Pfade

Achten Sie darauf, dass die Pfade alle korrekt sind. Bei der Replikation werden später alle alten Einträge gelöscht und die neuen geschrieben. Stimmen hier die Pfade nicht, können Sie Ihr System unbrauchbar machen.

Jetzt können Sie den Parameter `--dry-run` aus der Befehlszeile entfernen und die erste Replikation durchführen. In Listing 6.23 sehen Sie die erfolgreiche Replikation:

```
root@sambabuch-dc2:~# rsync -XAavz --delete-after \
          --password-file=/etc/samba/rsync.pass \
          rsync://sysvol-repl@sambabuch/sysvol/ /var/lib/samba/sysvol/

receiving file list ... done
./
example.net/
example.net/Policies/
example.net/Policies/31B2F340-016D-11D2-945F-00C04FB984F9/
example.net/Policies/31B2F340-016D-11D2-945F-00C04FB984F9/GPT.INI
example.net/Policies/31B2F340-016D-11D2-945F-00C04FB984F9/MACHINE/
example.net/Policies/31B2F340-016D-11D2-945F-00C04FB984F9/USER/
example.net/Policies/6AC1786C-016F-11D2-945F-00C04FB984F9/
example.net/Policies/6AC1786C-016F-11D2-945F-00C04FB984F9/GPT.INI
example.net/Policies/6AC1786C-016F-11D2-945F-00C04FB984F9/MACHINE/
example.net/Policies/6AC1786C-016F-11D2-945F-00C04FB984F9/USER/
example.net/scripts/
example.net/scripts/WindowsTH-KB2693643-x64.msu
```

Listing 6.23 Erfolgreiche Replikation

Prüfen Sie, ob alle Verzeichnisse und Dateien übertragen wurden. Wenn alle Dateien übertragen wurden, können Sie mit dem nächsten Schritt fortfahren.

6.3.4 Einrichtung eines Cron-Jobs

Damit Sie die Replikation nicht immer von Hand durchführen müssen, sollten Sie an dieser Stelle einen *Cron-Job* als Benutzer *root* einrichten, der regelmäßig die Replikation durchführt.

Im Beispiel soll die Replikation alle fünf Minuten durchgeführt werden. In Listing 6.24 sehen Sie die Zeile für den Cron:

```
*/5 * * * * rsync  -XAavz --delete-after\
           --password-file=/etc/samba/rsync.pass\
           rsync://sysvol-repl@samba4-1/sysvol/ /var/lib/samba/sysvol/
```

Listing 6.24 Eintrag in der »crontab«

[+]

Sie können das Kommando auch erst in ein Shellskript schreiben und dann das Shellskript über den Cron starten. Das hat den Vorteil, dass Sie das Skript einfach auf weitere Domaincontroller kopieren und einbinden können. Vergessen Sie nicht, das Skript ausführbar zu machen.

Die Zeit für die Replikation ist immer davon abhängig, wie viele Änderungen Sie an den Gruppenrichtlinien und den Logon-Skripten vornehmen. Damit ist die Replikation des zweiten DCs abgeschlossen. Wenn Sie noch weitere DCs in Ihrer Domäne haben, müssen Sie diesen Schritt auf allen weiteren DCs durchführen.

6.3.5 Anpassen der »smb.conf« auf den Client-DCs

Auf den Client-DCs der Replikation sollten Sie die Freigabe *sysvol* auf `read-only` setzen, damit hier niemand über das Netzwerk Änderungen vornehmen kann. Passen Sie hierfür die Datei */etc/samba/smb.conf* so wie in Listing 6.25 zu sehen an:

```
[sysvol]
        path = /var/lib/samba/sysvol
        read only = Yes
```

Listing 6.25 Anpassen der Freigabe »sysvol«

Einstellung für die Gruppenrichtlinen

Jetzt müssen Sie noch dafür sorgen, dass das RSAT für die Verwaltung der Gruppenrichtlinien nur noch auf dem entsprechenden Server mit der FSMO-Rolle *PDC-Master* ausgeführt wird.

Starten Sie hierfür das RSAT Gruppenrichtlinienverwaltung. Suchen Sie auf der linken Seite Ihre Domäne, klicken Sie mit der rechten Maustaste auf die Domäne, und wählen Sie dann den Punkt Domänencontroller ändern... aus. Es öffnet sich ein neues Fenster. In diesem Fenster markieren Sie den Punkt Domänencontroller mit dem Betriebsmastertoken für die PDC-Emulation. Der entsprechende DC aus der Liste wird daraufhin im unteren Teil des Fensters markiert. In Abbildung 6.7 sehen Sie die Einstellung.

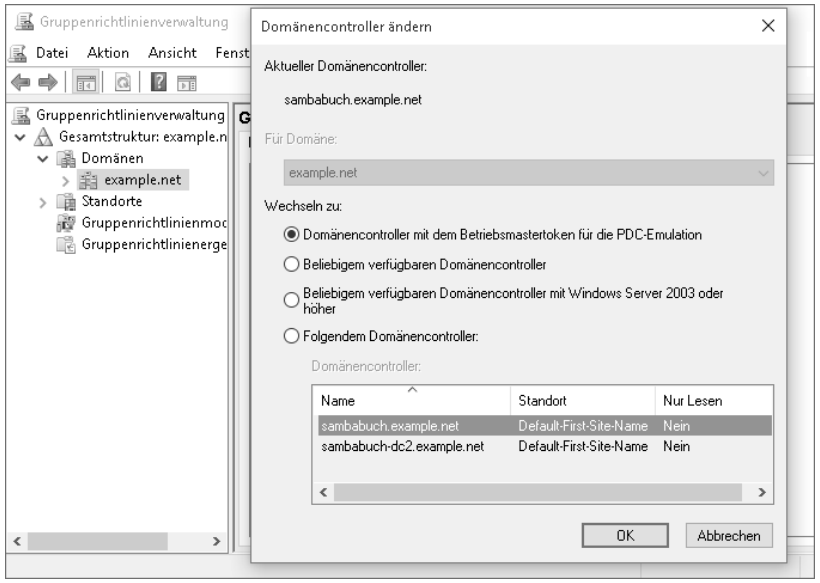


Abbildung 6.7 Auswahl des PDC-Masters

Bestätigen Sie die Einstellung mit einem Klick auf OK. Ab sofort werden alle Änderungen an den Gruppenrichtlinien nur noch auf dem entsprechenden DC durchgeführt.

Weitere Domaincontroller können Sie auf demselben Weg zu Ihrer Domäne hinzufügen, wie es hier beschrieben wurde.

6.4 Die FSMO-Rollen

Seit der Einführung von Active Directory mit Windows Server 2000 werden auf den Domaincontrollern verschiedene *Flexible Single Master Operations-(FSMO-)Rollen* verwendet, um bestimmte Aufgaben in der Domäne zu steuern. Jede dieser Rollen muss genau einmal in der Domäne durch einen der Domaincontroller bereitgestellt werden, wobei es, von der Funktion her, keine Rolle spielt, ob Sie alle Rollen auf einem Domaincontroller halten oder die Rollen auf alle Domaincontroller Ihrer Domäne

verteilen. Wichtig ist nur, dass Sie genau dokumentieren, wo die einzelnen Rollen liegen, denn im Falle eines Ausfalls eines Domaincontrollers ist es wichtig, dass Sie die Rollen, die dieser Domaincontroller innehatte, auf einen anderen Domaincontroller verschieben. In der folgenden Aufzählung sehen Sie alle FSMO-Rollen und ihre Funktion. Auch gehe ich darauf ein, welche der Rollen unbedingt auf demselben Domaincontroller eingerichtet werden sollten.

- Schemamaster
  Die Rolle des Schemamasters existiert nur einmal in der Gesamtstruktur und sollte immer zusammen mit dem *Domainnamemaster* auf demselben Domaincontroller liegen. Dieser Domaincontroller sollte auch immer einen *Global Catalog* besitzen. Der Schemamaster ist verantwortlich für den Aufbau des LDAP-Schemas innerhalb des Active Directories. Änderungen am Schema können Sie nur auf dem Domaincontroller mit dieser Rolle durchführen. Eine Änderung am Schema wird dann automatisch an die anderen Domaincontroller übertragen.
- Domainnamemaster
  Die Rolle des Domainnamemasters existiert auch nur einmal in der Gesamtstruktur und sollte immer mit dem Schemamaster zusammen auf demselben Domaincontroller eingerichtet sein. Der Domainnamemaster ist verantwortlich für die Vergabe von Namen für neue Domänen. Steht der Domainnamemaster nicht zur Verfügung, können Sie keine weiteren Domänen in der Gesamtstruktur erstellen.
- RID-Master
  Auch der *RID-Master* darf nur einmal pro Domäne existieren. Er sollte immer zusammen mit dem *PDC-Emulator* auf demselben Domaincontroller bereitgestellt werden. Der RID-Master stellt für jeden Ihrer Domaincontroller immer wieder neue Pools von IDs bereit, damit Sie auch auf verschiedenen Domaincontrollern Objekte anlegen können.

  Die IDs werden beim Anlegen eines neuen Objekts zur RID des Objekts. Dadurch ist das Objekt eindeutig in der Domäne. Die ID eines Objekts besteht immer aus der Domain-SID und dem RID.

  Der RID ist der hintere Teil der Objekt-SID, darüber lässt sich ein Objekt eindeutig in einer Domäne identifizieren. Die Objekt-SID setzt sich aus der Domain-SID, der die Domäne eindeutig identifiziert, und dem RID zusammen, der das Objekt in der Domäne eindeutig identifiziert.

  Durch dieses Verfahren lässt sich ein Objekt auch in Vertrauensstellungen eindeutig einer Domäne zuordnen.
- PDC-Emulator
  Der *PDC-Emulator* existiert auch nur einmal pro Domäne. Diese Rolle sollte immer zusammen mit dem *RID-Master* auf demselben Domaincontroller liegen. Sei-

ne Aufgabe ist es, Passwortänderungen der Benutzer möglichst schnell bekannt zu machen. Die Replikation einer Änderung im Active Directory kann bis zu 20 Minuten dauern.

Ändert jetzt ein Benutzer sein Kennwort auf einem anderen Domaincontroller, der nicht gleichzeitig auch PDC-Emulator ist, wird die Änderung des Passworts aber direkt an den PDC-Emulator weitergeleitet. Wenn sich der Benutzer jetzt ab- und wieder anmeldet, kann es passieren, dass er sich an einem Domaincontroller authentifiziert, der die Änderung des Passworts noch nicht mitbekommen hat, da die Replikation noch nicht abgeschlossen ist.

Natürlich verwendet der Benutzer sein neues Passwort, das der Domaincontroller nicht kennt. Jetzt leitet der Domaincontroller die Authentifizierung an den PDC-Emulator weiter. Dieser kennt das neue Passwort bereits, und die Anmeldung des Benutzer wird durch den PDC-Emulator durchgeführt.

- Infrastrukturmaster
  Auch der Infrastrukturmaster existiert nur einmal pro Domäne. Der Infrastrukturmaster sorgt für die referentielle Integrität zwischen Active Directory-Objekten, die untereinander verlinkt sind. Verlinkte Objekte stehen in einer Verbindung zueinander. Ein Beispiel wäre die Verwaltung von Gruppenmitgliedschaften von Benutzern. In der Gruppe finden Sie ein Attribut `Members`, in dem alle Mitglieder der Gruppe aufgelistet sind. Bei den Benutzern finden Sie eine Liste mit allen Gruppenmitgliedschaften. Die Gruppenmitgliedschaften werden dabei in dem Attribut `MembersOf` verwaltet.

  Die Aufgabe des Infrastrukturmasters ist es, sicherzustellen, dass bei einer Änderung eines Objekts auch das andere Objekt geändert wird, und zwar in allen Domänen des Baums oder Forests. Wenn nicht alle Domaincontroller mit einem Global Catalog ausgestattet sein sollen, ist es wichtig, dass der Infrastrukturmaster auf gar keinen Fall einen Global Catalog hält. Der Dienst würde dann deaktiviert, und es würde zu schweren Replikationsfehlern kommen. Bei Samba 4 werden alle Domaincontroller automatisch auch Global Catalog. Achten Sie also darauf, dass, wenn Ihr Infrastructuremaster ein Global Catalog hält, auch alle anderen Domaincontroller Ihrer Domäne Global Catalog-Server sind.

  Der Replikationsfehler, der in diesem Fall auftritt, hat die Event-ID 1419. Mehr dazu finden Sie unter *https://support.microsoft.com/en-us/kb/251095*.

- Infrastrukturmasterrolle Forest
  Die Rolle *ForestDNSZones* wurde erst mit Windows Server 2003 eingeführt und ist verantwortlich für die DNS-Struktur in der gesamten Forest-Struktur. Diese Rolle darf es in der gesamten Struktur, die aus mehreren Domänen bestehen kann, nur einmal geben. Jede neue Domäne in der Struktur wird hier verwaltet.

- Infrastrukturmasterrolle Domain
  Die Rolle der *DomainDNSZones* existiert in jeder Domäne der Struktur genau einmal. Diese Rolle verwaltet die DNS-Struktur der Domäne.

Was ist der Global Catalog?

Im *Global Catalog* werden alle Objekte einer Active Directory-Gesamtstruktur gespeichert. Ein Global Catalog-Server ist ein Domaincontroller, auf dem eine komplette Kopie aller Objekte des Verzeichnisdienstes für die eigene Domäne liegen. Zusätzlich liegt dort eine schreibgeschützte Teilkopie aller Objekte für alle anderen Domänen der Gesamtstruktur. Alle Suchen nach Objekten werden vom Global Catalog beantwortet. Jeder Domaincontroller wird bei Samba 4 als Global Catalog eingerichtet.

Mehr zum Thema Global Catalog finden Sie hier: *https://technet.microsoft.com/de-de/library/cc730749.aspx*

6.4.1 Verwaltung der FSMO-Rollen mit »samba-tool«

Die FSMO-Rollen lassen sich sowohl über die RSAT als auch über das Kommando `samba-tool` verwalten. Bei der Verwaltung über die RSAT haben Sie das Problem, dass die Rollen über verschiedene Tools verteilt sind. Es gibt also keine zentrale Stelle für die Verwaltung der Rollen.

Anders beim Kommando `samba-tool`: Dort finden Sie ein Tool zur Durchführung aller Änderungen der FSMO-Rollen. Aus diesem Grund werde ich hier im Buch nur die Verwaltung über das Kommando `samba-tool` beschreiben.

An dieser Stelle werde ich nur noch auf Samba-Versionen ab 4.3 eingehen, da nur dort alle Rollen angesprochen werden können. Am Ende des Abschnitts werde ich Ihnen noch eine Möglichkeit zeigen, wie Sie auch bei älteren Versionen die beiden Infrastrukturmasterrollen `ForestDNSZones` und `DomainDNSZones` verschieben können.

6.4.2 Auflisten aller Rollen

Wie Sie schon bei der Einrichtung der »sysvol«-Replikation gesehen haben, ist es oftmals sehr wichtig zu wissen, auf welchem der Domaincontroller sich welche der FSMO-Rollen befindet.

Dafür steht Ihnen das Kommando `samba-tool fsmo show` zur Verfügung. In Listing 6.26 sehen Sie ein Beispiel:

```
root@sambabuch:~# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
InfrastructureMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
RidAllocationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
DomainNamingMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
```

Listing 6.26 Auflisten aller Rollen

Hier sehen Sie, dass sich alle FSMO-Rollen momentan auf dem ersten Domaincontroller befinden. Es spielt dabei keine Rolle, auf welchem Ihrer Domaincontroller Sie diese Anfrage stellen, die Antwort ist immer die gleiche. Da es sich bei dem Beispiel um einen Samba 4.3-Domaincontroller handelt, sehen Sie alle sieben FSMO-Rollen.

6.4.3 Transferieren der FSMO-Rollen

Wollen Sie eine oder alle FSMO-Rollen auf einen anderen Domaincontroller verschieben, können Sie diese Aufgabe wieder mit dem Kommando `samba-tool` realisieren. Eine Rolle wird immer auf einen anderen Domaincontroller gezogen und nie verschoben. Sie müssen daher das Kommando immer auf dem Ziel-Domaincontroller ausführen. Sie können einzelnen Rollen transferieren oder aber gleich alle Rollen auf einmal transferieren.

Um die richtige Syntax für die Namen der einzelnen Rollen herauszufinden, können Sie über das Kommando `samba-tool fsmo transfer -help` die Hilfe nutzen.

In Listing 6.27 sehen Sie, wie eine Rolle auf den zweiten Domaincontroller transferiert wird:


```
root@sambabuch-dc2:~# samba-tool fsmo transfer --role=naming
FSMO transfer of 'naming' role successful

root@sambabuch-dc2:~# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
InfrastructureMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
RidAllocationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
DomainNamingMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
```

Listing 6.27 Transferieren einer Rolle

Nach dem erfolgreichen Transferieren der Rolle sehen Sie, dass die Rolle des *Domainnamemasters* jetzt auf den zweiten Domaincontroller verschoben wurde.

Jetzt sollen alle anderen Rollen ebenfalls auf den zweiten Domaincontroller transferiert werden. Listing 6.28 zeigt diesen Vorgang:

```
root@sambabuch-dc2:~# samba-tool fsmo transfer --role=all
This DC already has the 'rid' FSMO role
This DC already has the 'pdc' FSMO role
This DC already has the 'naming' FSMO role
This DC already has the 'infrastructure' FSMO role
This DC already has the 'schema' FSMO role
ERROR: Failed to delete role 'domaindns': LDAP error 50\
       LDAP_INSUFFICIENT_ACCESS_RIGHTS -  <00002098: Object\
       CN=Infrastructure,DC=DomainDnsZones,DC=example,DC=net\
       has no write property access
```

```
root@sambabuch-dc2:~# samba-tool fsmo transfer --role=all -k yes
FSMO transfer of 'rid' role successful
FSMO transfer of 'pdc' role successful
This DC already has the 'naming' FSMO role
FSMO transfer of 'infrastructure' role successful
FSMO transfer of 'schema' role successful
FSMO transfer of 'domaindns' role successful
FSMO transfer of 'forestdns' role successful
```

Listing 6.28 Transferieren aller Rollen

Im ersten Beispiel sehen Sie, dass die Rolle des *Domainnamemasters* bereits transferiert wurde. Dann sehen Sie eine Fehlermeldung, die auf fehlende Zugriffsrechte hinweist. Diese Fehlermeldung bezieht sich auf die beiden Infrastrukturmasterrollen. Diese können nur transferiert werden, wenn beim Transferieren eine Authentifizierung durchgeführt wird. Im zweiten Beispiel klappt es dann mit dem Transfer der beiden Rollen. Die Authentifizierung wird hier wieder über Kerberos durchgeführt. Jetzt sind alle Rollen erfolgreich auf den zweiten Domaincontroller transferiert, wie Listing 6.29 zeigt:

```
root@sambabuch-dc2:~# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
InfrastructureMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
RidAllocationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
DomainNamingMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
                        CN=Default-First-Site-Name,\
                        CN=Sites,CN=Configuration,DC=example,DC=net
```

Listing 6.29 Auflisten der Rollen nach »transfer«

Jetzt sind Sie in der Lage, alle FSMO-Rollen von einem laufenden Domaincontroller auf einen anderen zu übertragen. Was aber, wenn der Domaincontroller, auf dem die FSMO-Rollen eingetragen sind, nicht mehr zur Verfügung steht? Dann haben Sie noch die Möglichkeit, die Rollen neu zu generieren. Dazu gibt es zu dem Kommando `samba-tool fsmo` das Subkommando `seize`. Das Wort »seize« kann man in diesem Zusammenhang mit dem Begriff »konfisziert« übersetzen. Dabei werden alle Rollen neu generiert.

Nie mehr den alten Domaincontroller einschalten

Wenn Sie die Rollen mittels `seize` auf einen anderen Domaincontroller übertragen, müssen Sie unbedingt dafür sorgen, dass der alte Domaincontroller mit den Rollen nicht mehr hochgefahren wird. Dieser Domaincontroller muss aus der Domäne entfernt werden. Wenn Sie das nicht berücksichtigen, dann kann es zu Konflikten und zu Fehlern in der Replikation kommen. In Abschnitt 6.6, »Entfernen eines ausgefallenen Domaincontrollers«, gehe ich noch näher auf diesen Fall ein.

FSMO-Transfer bei älteren Samba-Versionen

Erst mit der Version 4.3 können Sie die beiden Infrastrukturmasterrollen *ForestDNSZones* und *DomainDNSZones* mit dem `samba-tool` transferieren. Bei den Versionen von 4.0 bis 4.2 geht das nur mithilfe einer .ldif-Datei und des Kommandos `ldpmodify`. Alle anderen Rollen können Sie genau wie im vorherigen Abschnitt transferieren. In Listing 6.30 sehen Sie die .ldif-Datei für die Modifikation:

```
dn: CN=Infrastructure,DC=DomainDnsZones,dc=example,dc=net
changetype: modify
replace: fSMORoleOwner
fSMORoleOwner: CN=NTDS Settings,CN=sambabuch-dc2,CN=Servers,\
               CN=Default-First-Site-Name,CN=Sites,CN=Configuration,\
               DC=example,DC=net

dn: CN=Infrastructure,DC=ForestDnsZones,dc=example,dc=net
changetype: modify
replace: fSMORoleOwner
fSMORoleOwner: CN=NTDS Settings,CN=sambabuch-dc2,CN=Servers,\
               CN=Default-First-Site-Name,CN=Sites,CN=Configuration,\
               DC=example,DC=net
```

Listing 6.30 .ldif-Datei für den Transfer

Achten Sie darauf, dass Sie den richtigen Namen des Domaincontrollers eintragen, auf den Sie die Rolle verschieben wollen.

Jetzt können Sie die Änderung so wie in Listing 6.31 einspielen:

```
root@sambabuch:~# ldbmodify -H /var/lib/samba/private/sam.ldb --cross-ncs \
                  dns.ldif

Modified 2 records successfully
```

Listing 6.31 Einspielen der Änderung

Da Sie die Änderung der beiden Rollen nicht mit dem Kommando `samba-tool fsmo show` sehen können, bleibt Ihnen nur der Umweg über das Kommando `ldbsearch`. Wie Sie sich die Rollen anzeigen lassen, sehen Sie in Listing 6.32:

```
root@sambabuch:~# ldbsearch -H /var/lib/samba/private/sam.ldb --cross-ncs\
                  --show-binary -b dc=example,dc=net fSMORoleOwner |\
                  grep 'fSMORoleOwner'

fSMORoleOwner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,CN=Default-First-Site-Name,\
               CN=Sites,CN=Configuration,DC=example,DC=net
fSMORoleOwner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
       CN=Default-First-Site-Name,\
               CN=Sites,CN=Configuration,DC=example,DC=net
fSMORoleOwner: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
               CN=Default-First-Site-Name,\
               CN=Sites,CN=Configuration,DC=example,DC=net
fSMORoleOwner: CN=NTDS Settings,CN=SAMBABUCH-DC2,CN=Servers,\
               CN=Default-First-Site-Name,\
               CN=Sites,CN=Configuration,DC=example,DC=net
fSMORoleOwner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
               CN=Default-First-Site-Name,\
               CN=Sites,CN=Configuration,DC=example,DC=net
fSMORoleOwner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
               CN=Default-First-Site-Name,\
               CN=Sites,CN=Configuration,DC=example,DC=net
fSMORoleOwner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
               CN=Default-First-Site-Name,\
               CN=Sites,CN=Configuration,DC=example,DC=net
```

Listing 6.32 Auflisten der Rollen mit »ldpsearch«

Wie Sie sehen, wurden die Besitzer der beiden Rollen auf den zweiten Domaincontroller geändert. So sind Sie auch mit älteren Samba-Versionen in der Lage, die beiden zusätzlichen FSMO-Rollen zu transferieren.

6.5 Entfernen eines aktiven Domaincontrollers

Irgendwann kommt der Zeitpunkt, an dem Sie einen bestehenden Domaincontroller aus der Domäne entfernen wollen. In diesem Abschnitt soll nun einer der Domaincontroller aus der Domäne genommen werden. Um Ihnen das an einem praktischen Beispiel zeigen zu können, habe ich einen dritten Domaincontroller in die Domäne aufgenommen. Dieser soll jetzt wieder aus der Domäne entfernt werden.

Als Erstes müssen Sie kontrollieren, ob der Domaincontroller, den Sie aus der Domäne entfernen wollen, eine oder mehrere FSMO-Rollen besitzt. Wenn das der Fall ist, müssen Sie diese Rollen zuerst auf einen der anderen Domaincontroller transferieren, bevor Sie ihn aus der Domäne entfernen.

Entfernen nur mit Authentifizierung

Es ist ganz wichtig, dass Sie sich beim Entfernen des Domaincontrollers aus der Domäne authentifizieren, denn sonst schlägt das Entfernen fehl, und der Domaincontroller wird nicht sauber aus der Domäne genommen.

Erst jetzt können Sie den Domaincontroller aus der Domäne entfernen. Der Samba-Dienst muss dafür laufen, da sich der Server sonst nicht aus der Domäne abmelden kann. In Listing 6.33 sehen Sie den Vorgang, wie der Domaincontroller aus der Domäne genommen wird:

```
root@sambabuch-dc3:~# samba-tool domain demote -Uadministrator
Using sambabuch-dc2.example.net as partner server for the demotion
Password for [EXAMPLE\administrator]:
Deactivating inbound replication
Asking partner server sambabuch-dc2.example.net to synchronize from us
Changing userControl and container
Demote successful
```

Listing 6.33 Entfernen des Domaincontrollers

Jetzt ist der Domaincontroller aus der Domäne entfernt. Die Replikation der Datenbank wurde entfernt, genau wie alle Einträge aus dem Active Directory. Sollte der Vorgang bei Ihnen nicht sauber durchlaufen worden sein, gibt es eine sehr gute Hilfe unter der URL *http://tinyurl.com/k63aqmf*. Es handelt sich dabei um einen Verweis auf ein Skript aus dem Microsoft Technet. Dort finden Sie ein VBS-Skript, mit dem Sie die letzten Metadaten des Domaincontrollers aus dem Active Directory entfernen können. Kopieren Sie sich das Skript in eine Datei auf dem Desktop mit der Dateiendung *.vbs*. Anschließend können Sie das Skript durch einen Doppelklick starten und den

zu entfernenden Domaincontroller auswählen. Dann werden alle Metadaten des Domaincontrollers aus dem Active Directory entfernt.

Prüfen Sie Ihren DNS

Prüfen Sie, nachdem Sie den Domaincontroller aus der Domäne entfernt haben, ob alle Einträge aus dem DNS gelöscht wurden. Es kann passieren, dass einige Einträge bestehen bleiben. Am einfachsten geht das mithilfe des DNS-Managers aus den RSAT. Gehen Sie durch den gesamten DNS-Baum mit allen Untereinträgen.

Stoppen Sie jetzt alle Samba-Dienste auf dem Server. Sorgen Sie unbedingt dafür, dass der Domaincontroller nicht einfach wieder in die Domäne aufgenommen werden kann. Entfernen Sie alle Samba-Pakete und alle Verzeichnisse, in denen Samba-Daten gespeichert werden.

6.6 Entfernen eines ausgefallenen Domaincontrollers

Solange ein Domaincontroller, der aus der Domäne entfernt werden soll, noch läuft, ist das Entfernen eines Domaincontrollers einfach und schnell zu realisieren. Was aber, wenn der Domaincontroller zum Beispiel wegen eines Hardwarefehlers ausgefallen ist? Noch schlimmer, wenn der Domaincontroller auch noch FSMO-Rollen besitzt. Was dann? Auch das ist kein großes Hexenwerk. Um diesen Vorgang zu zeigen, habe ich wieder einen dritten Domaincontroller in die Domäne aufgenommen und alle FSMO-Rollen auf diesen Domaincontroller übertragen. Listing 6.34 zeigt die Liste mit allen FSMO-Rollen:

```
root@sambabuch-dc3:~# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC3,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
InfrastructureMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC3,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
RidAllocationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC3,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC3,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
DomainNamingMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC3,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
```



```
                        CN=Configuration,DC=example,DC=net
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC3,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH-DC3,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
```

Listing 6.34 Liste aller Rollen

Wie Sie sehen, sind alle FSMO-Rollen jetzt auf dem dritten Domaincontroller eingetragen. Die Replikation zwischen allen drei Domaincontrollern funktioniert einwandfrei. Jetzt wird der Domaincontroller `sambabuch-dc3` einfach ausgeschaltet. Dabei soll der Fehler eines Totalausfalls simuliert werden, deshalb wird der Server nicht heruntergefahren, sondern direkt ausgeschaltet.

Nach dem Ausfall sollen jetzt die FSMO-Rollen auf den ersten Domaincontroller transferiert werden. Listing 6.35 zeigt diesen Versuch:

```
root@sambabuch:~# samba-tool fsmo transfer --role=all -k yes
ERROR: Transfer of 'rid' role failed: Failed FSMO transfer:\
       WERR_HOST_UNREACHABLE
```

Listing 6.35 Versuch die Rollen zu transferieren

Wie Sie sehen, wird der Vorgang bereits nach der ersten Rolle mit der Fehlermeldung abgebrochen, dass der Domaincontroller, der die Rolle hält, nicht erreichbar ist. Ein Transferieren der Rollen ist so nicht mehr möglich. Jetzt müssen Sie die Rollen mittels `seize` übernehmen. Listing 6.36 zeigt diesen Vorgang:

```
root@sambabuch:~# samba-tool fsmo seize --role=all -k yes
Attempting transfer...
ERROR: Transfer of 'rid' role failed: Failed FSMO transfer:\
       WERR_HOST_UNREACHABLE

root@sambabuch:~# samba-tool fsmo seize --role=all --force -k yes
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
```

```
Seizing domaindns FSMO role...
FSMO seize of 'domaindns' role successful
Seizing forestdns FSMO role...
FSMO seize of 'forestdns' role successful
```

Listing 6.36 Übernehmen aller Rollen

Zunächst schlägt der Versuch, die Rollen zu übernehmen, fehl, denn es wird immer versucht, die Rollen zu transferieren. Erst im zweiten Versuch mit dem Parameter `--force` funktioniert der Vorgang. Ein anschließendes Auflisten der Rollen zeigt die geglückte Übernahme der Rollen, so wie in Listing 6.37:

```
root@sambabuch:~# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                        CN=Default-First-Site-Name,CN=Sites,\
                        CN=Configuration,DC=example,DC=net
InfrastructureMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                                CN=Default-First-Site-Name,CN=Sites,\
                                CN=Configuration,DC=example,DC=net
RidAllocationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                               CN=Default-First-Site-Name,CN=Sites,\
                               CN=Configuration,DC=example,DC=net
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                              CN=Default-First-Site-Name,CN=Sites,\
                              CN=Configuration,DC=example,DC=net
DomainNamingMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                              CN=Default-First-Site-Name,CN=Sites,\
                              CN=Configuration,DC=example,DC=net
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                                CN=Default-First-Site-Name,CN=Sites,\
                                CN=Configuration,DC=example,DC=net
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=SAMBABUCH,CN=Servers,\
                                CN=Default-First-Site-Name,CN=Sites,\
                                CN=Configuration,DC=example,DC=net
```

Listing 6.37 Anzeigen der Rollen nach Übernahme

Nachdem die FSMO-Rollen jetzt wieder alle in der Domäne vorhanden sind, geht es noch ans Aufräumen. Sie müssen die Metadaten des alten Domaincontrollers entfernen und den DNS-Server aufräumen. Am einfachsten können Sie die Metadaten mit dem Technet-Skript entfernen.

Wenn Sie dieses Skript nicht nutzen wollen, müssen Sie alle Einträge des alten Domaincontrollers aus dem Active Directory manuell entfernen. Das Skript ist da auf jeden Fall die einfachere Variante. Starten Sie es, wählen Sie den alten Domaincontroller aus und klicken Sie dann auf OK und bestätigen Sie den Hinweis. Im Anschluss erhalten Sie die Meldung, dass die Metadaten des Domaincontrollers erfolgreich entfernt wurden. Jetzt ist das Active Directory schon frei von den Einträgen des alten Domaincontrollers.

Jetzt bleibt nur noch das Aufräumen des DNS. Diesen Vorgang führen Sie am einfachsten unter Windows mit dem DNS-Manager durch.

Alten Domaincontroller nie wieder einschalten

Unter keinen Umständen dürfen Sie den alten, gerade entfernten Domaincontroller wieder einschalten. Da der Domaincontroller immer noch die FSMO-Rollen eingetragen hat und auch eine Active Directory-Datenbank besitzt, kann es zu fehlerhaften Replikationen bis hin zum Totalausfall der Domäne führen.

Da Sie so alle Daten des Domaincontrollers entfernt haben, können Sie jetzt einen neuen Domaincontroller mit derselben IP und demselben Namen wie beim alten Domaincontroller wieder neu in die Domäne aufnehmen, um den alten Zustand der Domäne wiederherzustellen.

Mithilfe dieses Kapitels sind Sie jetzt in der Lage, auf alle Eventualitäten hinsichtlich Domaincontrollern zu reagieren. Die Domaincontroller sind das Rückgrat Ihres Systems, prüfen Sie regelmäßig ihre Funktion. Ein besonderes Augenmerk sollten Sie auf die Replikation der Datenbank legen.

Auf einen Blick

Inhalt

TEIL III Erweiterte Administration

Index

G

H

I

J

K

L

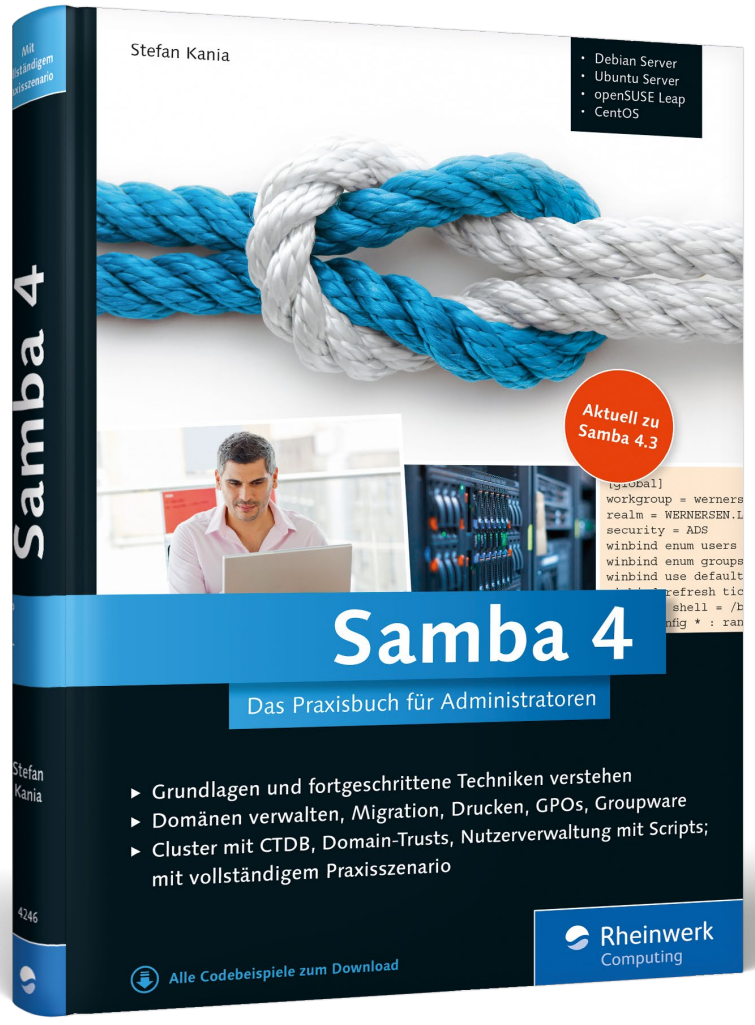
M

N

O

P

Q



Stefan Kania, Jahrgang 1961, ist ausgebildeter Informatiker und seit 1997 freiberuflich als Consultant und Trainer tätig. Seine Schwerpunkte liegen in der Implementierung von Samba und LDAP sowie in Schulungen zu beiden Themen. In seiner übrigen Zeit ist er als Tauchlehrer tätig, läuft Marathon und seit einiger Zeit versucht er sich am Square Dance. Mit dem Motorrad und seiner großen Liebe erkundet er im Sommer seine neue Wahlheimat Schleswig-Holstein.

Stefan Kania

Samba 4 – Das Praxisbuch für Administratoren

469 Seiten, gebunden, 2. Auflage 2016
49,90 Euro, ISBN 978-3-8362-4246-2

www.rheinwerk-verlag.de/4186