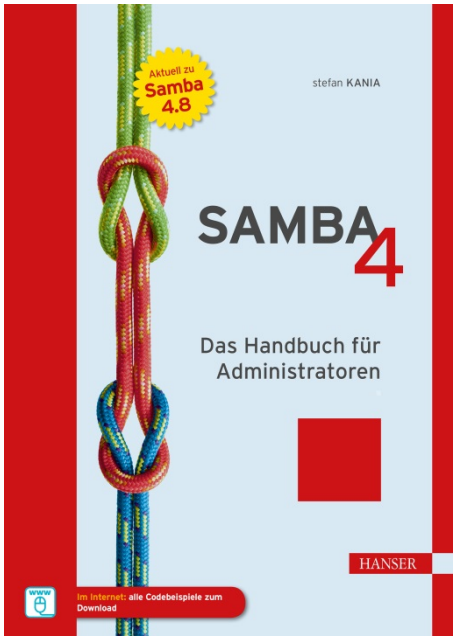
HANSER



Leseprobe

zu

„Samba 4“

von Stefan Kania

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

Weitere Informationen und Bestellungen unter
http://www.hanser-fachbuch.de/978-3-446-45735-5
sowie im Buchhandel

Vorwort

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

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

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

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

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

Danksagung

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

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

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

Inhalt

4 Einrichten des ersten Domaincontrollers

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

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

Hinweis

Zurzeit wird hier noch der Heimdal-Kerberos verwendet.

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

4.1 Allgemeines zum Einrichten des Domaincontrollers

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

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

Listing 4.1 Ein Testlisting

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

Main samba administration tool.


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

  Version Options:
    -V, --version  Display version number


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

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

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

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

- **Den NetBIOS-Domainname:**
  Der NetBIOS-Domainname ist die Adresse, über die der Server per NetBIOS-Protokoll erreichbar ist. Der NetBIOS-Name sollte immer der erste Teil des Realms sein.
- **Die Funktion des Servers:**
  Sie sollten wissen, welche Rolle der Server in der Domäne übernehmen soll. In unserem Fall übernimmt er die Rolle des Domaincontrollers.
- **Welcher DNS-Server soll verwendet werden?**
  Sie müssen wissen, ob Sie den internen DNS-Server von Samba4 verwenden wollen oder einen Bind9-Server.
- **Die IP-Adresse eines eventuell benötigten DNS-Forwarders:**
  An diese IP-Adresse werden alle DNS-Anfragen weitergeleitet, die nicht zur eigenen Zone gehören. Ohne einen Forwarder ist die Namensauflösung der Namen im Internet nicht möglich. Sie können hier auch mehr als eine IP-Adresse angeben. Die einzelnen Server werden durch Leerzeichen voneinander getrennt.

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

Hinweis

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

4.2 Konfiguration des ersten Domaincontrollers (DC Teil 1)

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

Listing 4.2 Provisioning mit internem DNS-Server

```
root@sambabuch:~# samba-tool domain provision
Realm [EXAMPLE.NET]:
 Domain [EXAMPLE]:
 Server Role (dc, member, standalone) [dc]:
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) \
             [SAMBA_INTERNAL]:
 DNS forwarder IP address (write 'none' to disable forwarding) \
             [8.8.8.8]:
Administrator password:
Retype password:
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.56.31
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Unable to determine the DomainSID, can not enforce uniqueness \
       constraint on local domainSIDs

Adding DomainDN: DC=example,DC=net
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=example,DC=net
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba AD has been \
          generated at /var/lib/samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf \
          or replace it with this one. Do not create a symlink!
Once the above files are installed, your Samba AD server \
```

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

Hinweis

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

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

Hinweis

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

Hinweis

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

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

Listing 4.3 Die neue smb.conf

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

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

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

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

4.2.1 Erster Start des Samba4-Servers

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

Listing 4.4 System für den Domaincontroller einrichten

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

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

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

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

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

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

4.3 Konfiguration des ersten Domaincontrollers (DC Teil 2)

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

Hinweis

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

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

Listing 4.5 Provisioning mit bind9

```
root@sambabuch:~# samba-tool domain provision
Realm [EXAMPLE.NET]:
 Domain [EXAMPLE]:
 Server Role (dc, member, standalone) [dc]:
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) \
             [SAMBA_INTERNAL]: BIND9_DLZ
Administrator password:
Retype password:
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.56.31
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
```

```
Pre-loading the Samba 4 and AD schema
Unable to determine the DomainSID, can not enforce uniqueness \
          constraint on local domainSIDs

Adding DomainDN: DC=example,DC=net
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers and extended rights
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=example,DC=net
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
See /var/lib/samba/bind-dns/named.conf for an example \
        configuration include file for BIND
and /var/lib/samba/bind-dns/named.txt for further \
        documentation required for secure DNS updates
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba AD has been \
        generated at /var/lib/samba/private/krb5.conf
Merge the contents of this file with your system krb5.conf \
        or replace it with this one. Do not create a symlink!
Once the above files are installed, your Samba AD server \
        will be ready to use
Server Role:           active directory domain controller
Hostname:              sambabuch
NetBIOS Domain:        EXAMPLE
DNS Domain:            example.net
DOMAIN SID:            S-1-5-21-1129951053-411964844-750776748
```

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

Listing 4.6 Hinweis auf die DNS-Konfiguration

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

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

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

Listing 4.7 Einstellungen in der named.conf.options

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

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

Listing 4.8 Änderungen an der Datei named.conf.local

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

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

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

Listing 4.9 Prüfen der Berechtigungen

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

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

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

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

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

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

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

Hinweis

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

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

Listing 4.10 Änderungen in Apparmor

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

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

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

Listing 4.11 Erster Test des Bind9

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

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

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

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

Listing 4.12 Anpassen des Systemd

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

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

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

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

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

Wichtig

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

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

4.4 Testen des Domaincontrollers

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

4.4.1 Testen der Prozesse

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

Listing 4.13 Testen der Prozesse

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

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

4.4.2 Testen der Serverports

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

Listing 4.14 Testen der Ports

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

Hinweis

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

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

4.4.3 Testen des DNS-Servers

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

Listing 4.15 Die verschiedenen DNS-Tests

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

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

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

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

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

4.4.4 Testen des Verbindungsaufbaus

Jetzt können Sie den Verbindungsaufbau zum Samba4-Server testen.

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

Listing 4.16 Ein erster Verbindungsaufbau

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

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

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            SAMBABUCH
```

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

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

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

4.4.5 Testen des Kerberos-Servers

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

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

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

Listing 4.17 Inhalt der Datei krb5.conf

```
[libdefaults]

        default_realm = EXAMPLE.NET
        dns_lookup_realm = false
        dns_lookup_kdc = true
```

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

Listing 4.18 Testen des Kerberos-Servers

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

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

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

Listing 4.19 Verbindung mit Kerberos

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

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

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            SAMBABUCH

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

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

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

Hinweis

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

4.4.6 Testen des LDAP-Servers

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

Listing 4.20 Testen des LDAP-Servers

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

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

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

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

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

# returned 4 records
# 1 entries
# 3 referrals
```

Hinweis

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

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

4.5 Konfiguration des Zeitservers

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

Listing 4.21 Konfiguration des Zeitservers

```
server 127.127.1.0
fudge  127.127.1.0 stratum 10
server 0.pool.ntp.org  iburst prefer
server 1.pool.ntp.org  iburst prefer
driftfile /var/lib/ntp/ntp.drift
logfile /var/log/ntp
ntpsigndsocket /var/lib/samba/ntp_signd/
restrict default kod nomodify notrap nopeer mssntp
restrict 127.0.0.1
restrict 0.pool.ntp.org mask 255.255.255.255 nomodify \
         notrap nopeer noquery
restrict 1.pool.ntp.org mask 255.255.255.255 nomodify \
         notrap nopeer noquery
```

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

Listing 4.22 Rechte für den Zeitserver setzen

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

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

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

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

Stichwortverzeichnis