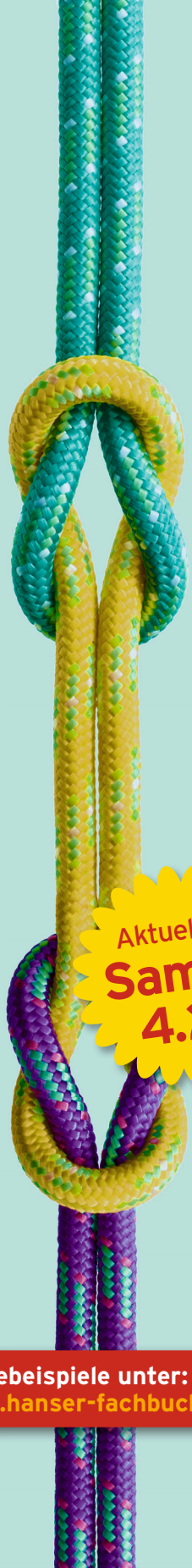
E-BOOK inklusive

Stefan KANIA

# SAMBA 4

## Das Handbuch für Administratoren

3. Auflage



Aktuell zu Samba 4.21

Codebeispiele unter:
plus.hanser-fachbuch.de

HANSER

Stefan Kania

# Samba 4

**Ihr Plus – digitale Zusatzinhalte!**
Auf unserem Download-Portal finden Sie zu diesem Titel kostenloses Zusatzmaterial. Geben Sie dazu einfach diesen Code ein:

plus-47c3U-rjRbq

**plus.hanser-fachbuch.de**

Stefan Kania

# Samba 4

3., überarbeitete Auflage

HANSER

Der Autor:
*Stefan Kania*, St. Michaelisdonn

Print-ISBN: 978-3-446-48385-9
E-Book-ISBN: 978-3-446-48449-8
E-Pub-ISBN: 978-3-446-48501-3



Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.


Kolbergerstraße 22 | 81679 München | info@hanser.de
*www.hanser-fachbuch.de*
Lektorat: Brigitte Bauer-Schiewek, Kristin Rothe
Copy editing: Jürgen Dubau, Freiburg/Elbe
Herstellung: le-tex publishing services GmbH, Leipzig
Coverkonzept: Marc Müller-Bremer, www.rebranding.de, München
Covergestaltung: Thomas West
Titelmotiv: © istockphoto.com/malerapaso
Druck: Elanders Waiblingen GmbH, Waiblingen
Printed in Germany

# Inhalt

# Vorwort

Nach über vier Jahren folgt nun die 3. Neuauflage des Samba-Buches im Hanser Verlag. Warum hat es dieses Mal so lange gedauert? In den Versionen zwischen 4.14 und 4.18 war vieles, was in den Versionen neu hinzugekommen ist, oft Dinge, die im Hintergrund relevant waren, aber nicht so sehr für die Administration. Immer wieder habe ich überlegt, eine neue Auflage zu erstellen. Aber ich denke, gerade für die Leser unter Ihnen, die schon eine vorherige Auflage gekauft haben, macht ein Neukauf nur Sinn, wenn sich auch vieles ändert. Mit der Version 4.19 war es dann so weit: Eine der größten Änderungen der letzten Jahre ist eingetreten, es gibt ein neues *Function Level*. Seit der Version 4.19 wird jetzt auch das Function Level 2016 unterstützt. Aber warum dann keine neue Version des Buches mit der Samba-Version 4.19? Mit der Version wurde zwar das neue Function Level eingeführt und eine Domäne kann auch auf das neue Function Level hochgestuft werden, aber es fehlten noch zu viele Funktionen. Erst mit der Version 4.21 ist es soweit, dass das neue Function Level auch genutzt werden kann. Auch habe ich in den letzten Jahren mein OpenLDAP-Buch aktualisiert und da viele Umstellungen bei Kunden durchgeführt. Jetzt habe ich aber die Zeit, eine neue Auflage des Samba-Buchs zu schreiben und wirklich einen Mehrwert für alle, die schon eine vorherige Auflage besitzen, zu bringen. Selbstverständlich wird der Schwerpunkt des Buches wieder bei der Administration liegen. Auch Dienste wie CTDB und Printserver sind wieder Bestandteil des Buches. Aber ich habe ein ganz neues Kapitel aufgenommen, in dem es um das Thema Sicherheit geht. Hier habe ich das BSI-Grundschutzhandbuch als Grundlage genutzt, um Domaincontroller und Fileserver abzusichern. In dem Kapitel gehe ich auf die einzelnen Module des Grundschutzhandbuchs ein, die für einen Samba-Server, egal ob Domaincontroller oder Fileserver, relevant sind. Alle Fragebögen sowie die Skripte aus dem Buch können Sie direkt per *git* mit dem Kommando `git clone https://github.com/stkania/samba4-buch-2024` herunterladen.

Aus dem Inhalt der letzten Auflage habe ich die Kapitel zum Thema *wins* und das Kapitel mit dem *Workshop* am Ende des Buches herausgenommen. Trotzdem ist diese Auflage etwas umfangreicher als die vorherige. An vielen Stellen habe ich weiter Inhalte hinzugefügt, um bestimmte Themen noch zu vertiefen. So ist zum Beispiel im Kapitel *Cluster* der Abschnitt zum GlusterFS etwas umfangreicher geworden. Zwei neue Kapitel sind dazugekommen: zum einen ein Kapitel, in dem es um die Sicherheit von Samba-Diensten geht, hier gehe ich auf die neuen Möglichkeiten mit dem neuen Function Level 2016 ein. Ein weiteres neues Kapitel beschäftigt sich noch einmal mit

dem Thema CTDB, hier geht es aber darum, einmal zu zeigen, dass CTDB auch mit NFS umgehen kann.

Einen Blick über den Tellerrand habe ich dann noch in dem Kapitel zum Thema CTDB und NFS geworfen. Ich will damit zeigen, dass CTDB weitaus mehr kann, als nur einen hochverfügbaren Samba-Server bereitzustellen. In dem Kapitel nutze ich dann CTDB, um einen NFS-Server hochverfügbar im Netzwerk einzubinden. Wenn Sie dann die Einrichtung einer Samba-Domäne und den NFS-Server kombinieren, erhalten Sie eine Umgebung für Linux-Clients, bei denen das Kerberos über das Active Directory für die Authentifizierung genutzt wird, und einen abgesicherten NFS-Server.

## Danksagung

Wie auch schon in der letzten Auflage gilt mein Dank immer Ihnen als Leser. Besonders an die Leser, die mir mit konstruktiven Feedbacks geholfen haben, bestimmte Dinge in der neuen Auflage aufzunehmen und zu verbessern. Ein Dank geht auch an den Hanser Verlag, dass Sie mir wieder die Möglichkeit gegeben haben, die Neuauflage zu schreiben.

Einer Person muss ich an dieser Stelle ganz besonders danken: Martin Schwenke, einem der Entwickler vom CTDB. Danke, Martin, für deine Hilfe bei allen Fragen rund um das Thema Cluster und die Geduld, bis dann der NFS-Server endlich fehlerfrei lief.

Jetzt bleibt mir nur noch, Ihnen viel Spaß mit der neuen Auflage zu wünschen, und wie immer freue ich mich über Anregungen und Kritik. Ihr Feedback hilft stets, eine weitere Auflage zu verbessern.

# 1 Einleitung

An dieser Stelle möchte ich Ihnen erklären, was ich mir bei der Verwendung der verschiedenen Formatierungsmöglichkeiten und Administrationsarten gedacht habe. Hier finden Sie auch die Beschreibung zu den im Buch verwendeten Icons.

## 1.1 Formales

Damit Sie den größtmöglichen Nutzen aus diesem Buch ziehen können, sollen im Folgenden einige Konventionen erläutert werden.

### 1.1.1 Kommandozeile vs. grafische Administration

An vielen Stellen im Buch verwende ich die Kommandozeile, um bestimmte Dienste zu konfigurieren oder zu testen, aber auch die Maus kommt hier zum Einsatz. In diesem Buch geht es ja um Samba 4. Samba 4 soll ein möglichst genaues Abbild einer Windows-Umgebung darstellen, und das betrifft natürlich auch die Administration.

Da die Administration unter Windows im Normalfall über die grafische Oberfläche stattfindet, wird genau das hier häufig auftauchen. An manchen Stellen macht es auch keinen Sinn, obwohl es ginge, die Administration über die Kommandozeile vorzunehmen, da Sie mit der Maus viel schneller sind. An einigen Stellen haben Sie auch mehr Möglichkeiten, wenn Sie die grafische Administration verwenden.

Für alle Leser unter Ihnen, die am liebsten alles oder wenigstens möglichst viel über die Kommandozeile erledigen möchten, habe ich das Kapitel zur Arbeit auf der Kommandozeile überarbeitet und erweitert. Mit der neuen Version 4.21 sind die Möglichkeiten der Administration mit dem `samba-tool` gegeben.

## 1.2 Schriftarten

Viele der Beispiele zu den Kommandos werden aber auch in Listings dargestellt. In den Listings werden Sie von der Befehlszeile bis zum Ergebnis alles nachvollziehen können, wie Sie hier im Beispiel sehen:

**Listing 1.1** Ein Testlisting

```
stefan@samba4~\$ ps
 PID TTY          TIME CMD
 4008 pts/2    00:00:00 bash
 4025 pts/2    00:00:00 ps
```

Die folgenden Schriftarten werden im Buch verwendet:

- Um bestimmte Begriffe hervorzuheben, wird die Schriftart *Schief* eingesetzt.
- Für die Darstellung von Tastenkombinationen und Klicks auf bestimmte Symbole oder Karteireiter in der grafischen Oberfläche wird die Schriftart KAPITÄLCHEN verwendet.
- Wenn im Text der Hinweis auf eine Datei gegeben wird, werde ich die Schriftart Sans Serif verwenden.
- Im fließenden Text werden Konsolenbefehle mit `Schreibmaschine` dargestellt.
- Parameter und Werte aus Listings durch die Verwendung von *Kursivschrift* gekennzeichnet.

### 1.2.1 Eingabe langer Befehle

Es gibt noch eine weitere wichtige, eher technische Konvention: Einige der vorgestellten Kommandozeilenbefehle oder Ausgaben von Ergebnissen erstrecken sich über mehrere Buchzeilen. Im Buch kennzeichnet am Ende der entsprechenden Zeilen ein „\“, dass der Befehl oder die Ausgabe in der nächsten Zeile weitergeht.

### 1.2.2 Screenshots

Wie heißt es doch so schön: Ein Bild sagt mehr als tausend Worte. Wann immer es sinnvoll erscheint, soll ein Screenshot zur Erhellung des Sachverhalts beitragen.

Gerade wenn Windows verstärkt für die Administration eingesetzt wird, sind Screenshots einfach unerlässlich. Auch sollen die Screenshots Ihnen helfen, bestimmte Einstellungen schneller und einfacher zu finden.

### 1.2.3 Internetverweise

An einigen Stellen werde ich auf bestimmte URLs verweisen – sei es, um Ihnen Quellen für bestimmte Downloads zu geben, oder um Ihnen den Weg zu tiefergehenden und weiterführenden Erklärungen zu geben, die den Rahmen dieses Buches sprengen würden. Verweise auf Internetadressen werden immer so geschrieben: www.samba.org.

### 1.2.4 Icons

Sie werden in den einzelnen Kapiteln am Rand oft Icons finden, die Sie auf bestimmte Zusammenhänge oder Besonderheiten hinweisen sollen. Die Icons haben die folgenden Bedeutungen:

**Wichtig**

Wann immer Sie das nebenstehende Symbol sehen, ist Vorsicht angeraten: Hier weise ich auf besonders kritische Einstellungen hin oder auf Fehler, die dazu führen können, dass das System nicht mehr stabil läuft. Damit sich die Warnungen mehr vom übrigen Text abheben, habe ich diese Textbereiche dann noch mit einem grauen Kasten hinterlegt.

**Hinweis**

Alle Textstellen, die ich mit diesem Icon versehen habe, sollten Sie unbedingt lesen! Hier handelt es sich oft um wichtige Hinweise, die Sie nicht außer Acht lassen sollten.

**Tipp**

Bei diesem Symbol finden Sie nützliche Tipps und Tricks zu bestimmten Aufgaben.

## 1.3 Linux-Distributionen

Welche Distribution Sie verwenden, ist immer abhängig davon, welche Samba-Funktion Sie nutzen wollen. Da die Verwendung des MIT-Kerberos immer noch als *experimental* gekennzeichnet ist, unterstützen nur Ubuntu und Debian die Funktion des Active Directory-Domaincontrollers aus den eigenen Repositories. Nur Debian und Ubuntu stellen den Heimdal-Server noch zur Verfügung, alle anderen Distributionen verwenden nur noch den MIT-Kerberos. Um die aktuelle Version 4.21 nutzen zu können, verwende ich hier im Buch die Backports zu Debian 12, denn dort ist diese Version

schon enthalten. Viele der von mir hier im Buch angesprochenen Funktionen erfordern mindestens die Samba-Version 4.20, besser ist aber auf jeden Fall der Einsatz der Samba-Version 4.21. Nur damit können Sie alles hier im Buch nachvollziehen.

In der vorherigen Auflage habe ich die Pakete von Louis van Belle genutzt. Der hat aber bedauerlicherweise die Bereitstellung der Pakete schon vor einiger Zeit eingestellt. Das zeigt leider, dass Sie immer einen Blick darauf werfen sollten, wer und vor allen Dingen wie viele Menschen die von Ihnen genutzten Pakete bereitstellen.

Natürlich haben Sie immer noch die Möglichkeit, die Pakete der Firma SerNet einzusetzen. Gerade im produktiven Umfeld sind diese Pakete aufgrund des schnellen und guten Supports zu empfehlen. Auch bekommen Sie dort die Pakete für andere Distributionen. Die SerNet-Pakete stellen dann den Heimdal-Kerberos für die Distributionen bereit.

Da die wichtigsten Unterscheidungsmerkmale hauptsächlich in der Installation liegen, können Sie die im Buch erklärten Vorgehensweisen auch auf andere Distributionen übernehmen. Die Administration ist bei allen Distributionen identisch. Wenn Sie also Samba entweder aus den Quellen selber bauen oder die Pakete aus externen Quellen nutzen, können Sie mit jeder beliebigen Distribution den Aufbau Ihrer Systeme mit diesem Buch nachvollziehen. Sie sind nicht zwingend auf Debian oder Ubuntu angewiesen.

Ein Hinweis zu Firewalls, SELinux und Apparmor: Ich werde vor der Installation diese Systeme immer deaktivieren, da es in diesem Buch nicht um das Thema Systemsicherheit der Systeme geht. Wenn Sie eines dieser Systeme nutzen wollen, müssen Sie sich in zusätzlicher Literatur darüber informieren, da diese Systeme für sich schon ganze Bücher füllen.

Wenn Sie jetzt überlegen, welche Distribution Sie verwenden wollen, folgen hier ein paar Tipps:

- Achten Sie auf langen Support, wählen Sie deshalb auf jeden Fall eine LTS-Version Ihrer Lieblingsdistribution.
- Installieren Sie auf allen Servern die gleiche Distribution, schaffen Sie sich keinen Distributionszoo. Das gilt besonders für die Domaincontroller und die CTDB-Server. Gerade hier sollten Sie auf jeden Fall die Version 4.21 nutzen.
- Testen Sie, mit welcher Distribution Sie am besten zurechtkommen.
- Schauen Sie sich die verschiedenen Versionen von Samba 4 an und überlegen Sie, welche Version Sie mindestens installieren müssen, um alle benötigten Funktionen realisieren zu können. Denken Sie daran, nur die letzten drei Samba-Versionen werden vom Samba-Team betreut.

## 1.4 Windows-Version

Da Windows 10 nicht mehr von Microsoft mit Updates versorgt wird, verwende ich hier im Buch ausschließlich Windows 11.

Jetzt bleibt mir nur noch, Ihnen viel Spaß mit dem Buch zu wünschen und zu hoffen, dass Ihnen mein Buch bei Ihrer täglichen Arbeit eine Hilfe sein wird.

# 2
# Grundlagen

Bevor es an die Praxis geht, will ich auf ein paar Grundlagen eingehen. Hier soll nicht das gesamte OSI-Referenzmodell besprochen, sondern ein kurzer Einblick in die verwendeten Protokolle vermittelt werden. Auch werde ich an dieser Stelle darauf eingehen, welche der Protokolle und welche Versionen noch aktuell sind und welche Versionen nicht mehr benutzt werden sollten.

In diesem Kapitel werden zunächst einige Grundlagen zu den Protokollen SMB und NetBIOS angesprochen. Auch will ich hier auf die verschiedenen Versionen des SMB-Protokolls eingehen.

Für die Datenübertragung und Adressierung im Netzwerk verwendet Windows zwei unterschiedliche Protokolle: SMB für die Datenübertragung und NetBIOS für die Adressierung über die NetBIOS-Namen.

Die beiden Protokolle haben dabei verschiedene Aufgaben. Auf das SMB-Protokoll können Sie nicht verzichten, denn es wird immer für die Datenübertragung verwendet. Das Protokoll wurde auch über die Jahre immer weiterentwickelt.

Auf das NetBIOS-Protokoll können Sie heute aber ganz verzichten, denn sämtliche Adressierung kann über DNS oder das Active Directory vorgenommen werden. Früher kam das Protokoll zum Einsatz, um zum Beispiel die Netzwerkumgebung im Explorer unter Windows nutzen zu können. Aber die Netzwerkumgebung, die vom Computersuchdienst gefüllt wird, basiert auf SMBv1, und das sollte auf gar keinen Fall mehr zum Einsatz kommen. Sowohl bei Windows als auch bei Samba ist das alte SMBv1-Protokoll deaktiviert. In Zukunft wird diese Protokollversion komplett verschwinden. Dann verliert auch das NetBIOS-Protokoll jegliche Bedeutung.

Unter Samba ist es aber schon so, dass auf einem Domaincontroller das NetBIOS-Protokoll gar nicht mehr aktiv ist und auch nicht mehr benötigt wird.

Da das Protokoll immer mehr in den Hintergrund tritt, werde ich hier auch nicht weiter darauf eingehen. Allerspätestens mit der Einführung von IPv6 ist die Nutzung nicht mehr möglich, da IPv6 das Protokoll nicht mehr unterstützt.

## 2.1 Das Protokoll SMB

Bei SMB handelt es sich um ein Protokoll zur Kommunikation mit Datei- und Druckdiensten. SMB wird auch oft als Dateisystem betrachtet, was es aber eigentlich nicht ist. SMB kann wohl besser mit NFS verglichen werden, das besonders unter Linux verwendet wird und dort den Austausch von Dateien regelt.

SMB ist für die Übertragung der Daten zwischen dem Client und dem Server verantwortlich. SMB benötigt immer ein Transportprotokoll. Hier kam früher das Protokoll NetBIOS alleine zum Einsatz, später wurde dann auf NetBIOS over TCP umgeschwenkt. Ab Windows 2000 ist es aber auch möglich, TCP alleine zu verwenden. Unter Samba wird das Protokoll SMB über den Daemon smbd bereitgestellt.

Mit Windows Vista erschien eine neue Version des SMB-Protokolls auf dem Markt: das SMB2-Protokoll. Dieses Protokoll wurde an einigen Stellen komplett überarbeitet. Eines der Hauptmerkmale der neuen Version ist, dass die Anzahl der Kommandos von über 100 auf 16 reduziert wurde.

Dadurch ist das Protokoll im Netzwerk nicht mehr so „gesprächig“. Auch wurden die Puffer für die Datenübertragung vergrößert, wodurch eine schnellere Übertragung von großen Dateien möglich ist.

Mit Samba 4 kam dann die Unterstützung des SMB3-Protokolls. Damit ist die Entwicklung aber nicht abgeschlossen, es wird weiter an dem Protokoll gearbeitet, und das sowohl auf Seiten von Microsoft als auch auf Seiten des Samba-Teams.

Das SMB-Protokoll gibt es in verschiedenen Versionen, die von den unterschiedlichen Windows-Versionen unterstützt werden:

- Version 1.0
  Diese Version kommt bei Windows 2000, Windows XP, Windows Server 2003 und Windows Server 2003 R2 zum Einsatz. Mittlerweile wird diese Version nur noch unterstützt, wenn Sie es explizit aktivieren. Die Version 1 hat einfach zu viele Sicherheitslücken, dass ein Einsatz heute nicht mehr empfohlen wird.
- Version 2.0
  Ab Windows Vista Service Pack 1 und Windows Server 2008 ist das Protokoll SMB in der Version 2.0 das Standardprotokoll für die Datenübertragung. Diese Version wurde auch bei Samba ab der Version 3.6 unterstützt.
- Version 2.1
  Mit Windows 7 und Windows Server 2008 R2 wurde die verbesserte Version 2.1 eingeführt. Samba unterstützte diese Version seit 3.6.

- **Version 3.0**
  Seit Windows 8 und Windows Server 2012 wird die aktuelle Version 3.0 des Protokolls implementiert. Ältere Windows-Versionen unterstützen die Version 3.0 nicht mehr. Aktuelle Samba-Versionen unterstützen die Version 3.1.1.

## 2.2 Das Protokoll NetBIOS

Obwohl es nur noch historische Bedeutung hat, möchte ich das Protokoll hier noch einmal kurz erläutern. NetBIOS ist (oder war) für die Namensdienste im Netzwerk verantwortlich. Es wird unter Samba über den Daemon nmbd bereitgestellt. Im Verlauf des Buchs werden Sie sehen, dass bei Samba 4 NetBIOS auf den Domaincontrollern nicht mehr für den Computersuchdienst bereitgestellt wird. Dadurch werden die Domaincontroller nicht mehr in der Netzwerkumgebung angezeigt. Verbindungen lassen sich dort nur noch direkt über die Freigabe einrichten.

Das Protokoll NetBIOS ist eine Entwicklung der Firmen IBM und Sytek Inc. Es wurde bereits im Jahre 1983 entwickelt. Ursprünglich war es dazu gedacht, die Kommunikation in kleinen Netzen bis maximal 80 Hosts zu gewährleisten. Später wurde NetBIOS als Protokoll definiert, das direkt auf der OSI-Ebene 2 aufsetzt. Daraus wurde das Protokoll NetBEUI, ein sehr einfach aufgebautes Protokoll ohne Routing-Funktion, das aber den Anforderungen an kleine Netze genügte.

Alle Microsoft-Betriebssysteme vor der Version Windows 2000 waren zwingend auf das Protokoll NetBIOS angewiesen, da mit diesem Protokoll die gesamte Adressierung der Systeme und der Dienste im Netz durchgeführt wurde. NetBIOS ist ein Protokoll der Ebene 5 des OSI-Referenzmodells. Dadurch können die verschiedensten Netzwerkprotokollfamilien auf den Ebenen 3 und 4 verwendet werden. Am Anfang stand hier NetBEUI im Vordergrund, da das Protokoll NetBIOS mehr für kleine lokale Netze gedacht war. Heute verwendet NetBIOS die Protokolle TCP/IP zum Transport der Daten und kann somit auch in modernen Netzen zum Einsatz kommen.

Seit Windows 2000 kann aber auch ganz auf NetBIOS verzichtet und die gesamte Kommunikation komplett über TCP/IP realisiert werden. Aus Kompatibilitätsgründen ist NetBIOS aber immer noch in den Microsoft-Betriebssystemen vorhanden und auch standardmäßig immer aktiv. Der Grund, weshalb NetBIOS noch vorhanden und aktiv ist, ist der, dass die Netzwerkumgebung auf einem Windows-Client stark von NetBIOS abhängig ist. Zwar füllt NetBIOS die Netzwerkumgebung nicht direkt (dafür ist der Computersuchdienst verantwortlich), aber der Computersuchdienst ist sehr stark von NetBIOS abhängig. NetBIOS ist nicht mehr relevant und wird von mir hier im Buch auch nicht mehr eingesetzt.

## 2.3 Was hat sich bei Samba getan?

In diesem Abschnitt möchte ich erst einmal aufzeigen, was sich seit der letzten Auflage des Samba-Buchs alles getan hat. Die letzte Auflage des Samba-Buchs basiert auf der Version 4.14, also vom März 2021. Seitdem ist eine Menge passiert. Sehr viele Änderungen sind für die Administration, die ja Schwerpunkt diese Buches ist, nicht sofort ersichtlich. Ein Großteil der Veränderungen beziehen sich auf interne Neuerungen, die für die Sicherheit und die Performance relevant sind. Aus diesem Grund möchte ich an dieser Stelle einmal alle wichtigen Änderungen auflisten. Die Änderungen, die die Administration und Sie als Administrator direkt betreffen, werden natürlich in den einzelnen Kapiteln des Buches genau angesprochen und erklärt.

### Version 4.15 (September 2021)

- Bis zur Version 4.14 war es möglich, einige Entwicklerversionen des SMB-Protokolls zu nutzen, doch das ist jetzt nicht mehr möglich. Wenn Sie also bei den Parametern *client max protocol* und/oder *server max protocol* diese Versionen nutzen, sollten Sie das auf jeden Fall wie folgt umstellen:
  - SMB2_22 => SMB3_00
  - SMB2_24 => SMB3_00
  - SMB3_10 => SMB3_11
- Das VFS-Interface wurde so überarbeitet, dass Samba jetzt auch komplett ohne SMBv1 betrieben werden kann.
- Bislang konnte jeder Client eine DNS-Zonentransferanfrage an den bind-Server stellen und eine Antwort von Samba erhalten. Jetzt ist das Standardverhalten, diese Anfragen abzulehnen. Es wurden zwei neue Optionen hinzugefügt, um die Liste der autorisierten/verweigerten Clients für Zonentransferanfragen zu verwalten. Um akzeptiert zu werden, muss die Anfrage von einem Client gestellt werden, der in der Zulassen-Liste und NICHT in der Ablehnen-Liste steht.
- Bis zu dieser Version war der *server multi channel support* noch *experimental*. Ab der Version 4.15 ist der Standard, dass der *server multi channel support* automatisch aktiviert ist. So kann jetzt ein Server seine Daten über mehrere Netzwerkkarten parallel bereitstellen, und somit ist einen höherer Datendurchsatz möglich.
- Die Samba-Dienstprogramme haben ihre Optionen nicht konsistent implementiert. Eine Reihe von Optionen erforderte die Angabe von Werten, aber bei anderen Programmen ist das nicht notwendig. Einige Optionen hatten in verschiedenen Tools unterschiedliche Bedeutungen. Das ist ab dieser Version konsistenter geworden. Ich werde bei den entsprechenden Kommandos darauf eingehen.

- Als Überbleibsel aus der Zeit der NT-Domänen ist das Verhalten von *winbind*, immer nach vertrauten Domänen zu suchen. Da das Ergebnis beim Einsatz von Active Directory nicht korrekt ist, wurde dieses Verhalten deaktiviert.
- Offline Domain join. Bei Windows ist es seit der Version 7 möglich, einen Client auch offline zur Domäne hinzuzufügen. Das ist vor allen Dingen dann sinnvoll, wenn mehrere Clients gleichzeitig zur Domäne hinzugefügt werden sollen. Mittels des Kommandos `net offlinejoin` ist das jetzt auch bei Samba möglich. Ich werde auf diese Möglichkeit in Kapitel 12, »Verwaltung von Clients in der Domäne«, genauer eingehen.
- Um veraltete dynamische Zoneneinträge automatisch zu entfernen, kann jetzt das *aging* für die Einträge aktiviert werden. Im ersten Schritt setzen Sie das *aging* auf einen sehr hohen Wert (im Beispiel 5 Jahre). Dazu nutzen Sie das Kommando `samba-tool dns zoneoptions --aging=1 --refreshinterval=306600`. Nachdem die Zone einige Zeit mit der Einstellung gelaufen ist, kann der Wert für das *aging* reduziert werden. Der Standardwert dafür sind 7 Tage. Das geschieht mit dem Kommando `samba-tool dns zoneoptions --refreshinterval=168`.
- Wenn ein DNS-Eintrag gelöscht wird, wird dieser in einen *tombstone*-Status versetzt. Erst wenn der Zeitraum für das *tombstoning* abgelaufen ist, wird der Eintrag vollständig gelöscht. Das bedeutet aber, wenn das *aging* nicht aktiv ist, wird der Eintrag niemals gelöscht. Mit der Version 4.15 werden die Einträge auch ohne die Aktivierung des *agings* gelöscht. Müssen die alten DNS-Einträge von Hand gelöscht werden, weil das *aging* nicht aktiv war, kann das Löschen der Einträge sehr lange dauern, immer abhängig von der Anzahl der gelöschten DNS-Einträge. Beim Einsatz von DDNS kann die Anzahl der Einträge sehr schnell sehr groß werden.
- Beim Kommando `Samba-tool domain backup offline` konnte es passieren, dass beim Einsatz von LMDB als Backend die Locks der Datenbanken nicht ordnungsgemäß entfernt wurden. Dieser Bug wurde in der Version 4.15 behoben.

### Version 4.16 (März 2022)

- Die verwendete Heimdal Kerberos-Version wurde aktualisiert und unterstützt jetzt auch *FAST*, ein Protokoll, das versucht, die Bandbreite eines Netzwerks besser auszunutzen. Windows-Clients unterstützen FAST aber erst, wenn die Domäne mindestens im Function Level 2012 betrieben wird. Erst mit Samba 4.19 werden höhere Function Level als 2008_R2 unterstützt.
- Es wird das automatische Ausrollen von Zertifikaten für Geräte unterstützt, aber nur zusammen mit dem dafür entwickelten Daemon *certmonger*. Die Zertifikate werden dabei über eine Gruppenrichtlinie bereitgestellt. Dafür muss der Linux-Client aber für die Verwendung von Gruppenrichtlinien über die smb.conf-Option *apply group policies = Yes* aktiviert sein.

- Beim internen DNS-Server können die Weiterleitungen an einen anderen DNS-Server auch auf andere Ports eingerichtet werden. Bis zu dieser Version war eine Weiterleitung nur an den Port 53 möglich. Beim Eintrag in der der smb.conf für den Forwarder wird dann der Port, durch einen Doppelpunkt getrennt, direkt hinter die IP-Adresse des Forwarders geschrieben.
- In dieser Version gibt es eine Menge Änderungen beim CTDB: Die Rolle *Recovery Master* wurde in *Leader* umbenannt. Dokumentation und Protokolle beziehen sich jetzt auf *Leader*. Hier geht es nicht unbedingt um political correctness, sondern auch darum zu zeigen, dass sich die Funktion grundsätzlich geändert hat. Wichtig ist bei der Umstellung auf diese oder eine der nachfolgenden Versionen, dass die Konfiguration des CTDB-Clusters dementsprechend angepasst wird. Die alten Namen der Optionen funktionieren zwar im Moment noch, werden aber in Zukunft nicht mehr nutzbar sein und zu Fehlern führen.

  Die folgenden ctdb-Befehlsnamen haben sich geändert:

  – recmaster -> leader
  – setrecmasterrole -> setleaderrole

  Die Befehlsausgabe hat sich für die folgenden Befehle geändert:

  – status
  – getcapabilities

  Die Konfigurationsoption *[legacy] -> recmaster capability* wurde umbenannt und in den Cluster-Abschnitt verschoben, sodass sie jetzt *[cluster] -> leader capability* lautet. Die Option *recovery lock* wurde in *cluster lock* umbenannt. Dokumentation und Protokolle beziehen sich jetzt nur noch auf *cluster lock*. Wenn *cluster lock* aktiviert ist, werden keine traditionellen Wahlen für den Leader mehr durchgeführt, es wird ein Wettlauf um die Cluster-locks zwischen den Knoten durchgeführt. Dadurch werden Situationen vermieden, in denen ein Knoten zum Anführer gewählt wird, dieser aber nicht die Cluster-locks übernehmen kann. Dies kann passieren, wenn beim Start ein Knoten sich selbst zum Anführer seines eigenen Clusters ernennt, bevor er Verbindung zu anderen Knoten hergestellt hat.

  CTDB verwendet nun Leader-Broadcasts, um eine damit verbundene Zeitüberschreitung festzustellen. So wird geprüft, ob eine Wahl erforderlich ist. Die Zeitüberschreitung für Leader-Broadcasts kann über eine neue Konfiguration mit der Option aus Listing 2.1 festgelegt werden.

**Listing 2.1** timeout für das Leader-Broadcast

```
[cluster]
leader timeout <wert>
```

Der Wert gibt die Anzahl der Sekunden ohne Leader-Broadcasts an, bevor ein Knoten eine Wahl durchführt. Der Standardwert ist 5.

- In der Version wird so langsam auch ein Abschied von SMBv1 eingeläutet. Das alte Kommando `smbcopy` wurde entfernt. Soll Server-site copy verwendet werden, kann hierfür das Kommando `scopy` genutzt werden.
- SMBv1 hat jetzt den Status *deprecated*. Das Protokoll ist jetzt in der Standardkonfiguration immer deaktiviert. Die Protokolle *NT LANMAN 1.0* und *NT1* sind somit nicht mehr nutzbar.

### Version 4.17 (September 2022)

- In dieser Version wurde die Performance beim Zugriff auf Dateien in Freigaben erheblich verbessert. Der Pfad einer Datei in einer Freigabe wird jetzt in *dirname* und *basename* zerlegt und dann für jeden Teil nur ein Syscall aufgerufen.
- Diese Version ist die erste, die Sie komplett ohne SMBv1 verwenden können. Wenn Sie Samba selbst kompilieren, kann durch die Option *–without-smb1-server* komplett auf SMBv1 verzichtet werden, dann kann SMBv1 auch nicht mehr durch Optionen in der smb.conf aktiviert werden.
- Jetzt kann auch der Port des internen DNS-Servers angepasst werden, sodass auf dem Domaincontroller ein zweiter DNS-Server laufen kann, der den Port 53 nutzt.
- CTDB wird jetzt direkt über den Systemd gestartet und nicht mehr über den ctdbd_wrapper. Der Wrapper wurde aus dem Grund auch entfernt.
- Es gibt jetzt eine Python-API, um die smb.conf zu verwalten.
- Das Ergebnis von `smbstatus` kann jetzt auch im JSON-Format ausgegeben werden.
- Die *protected users*-Gruppe kann genutzt werden. Mitglieder dieser Gruppe erhalten verschärft Regeln für die Kerberos-Authentifizierung. Mehr dazu in Kapitel 5, »Die Benutzerverwaltung«.

### Version 4.18 (März 2023)

- Die Fehlermeldungen im `samba-tool` waren immer nur in der Form von Python-Meldungen vorhanden. Viele dieser Meldungen wurden jetzt so übersetzt, dass sie verständlich sind. Die alten Python-Meldungen können über die Option *-d3* weiterhin ausgegeben werden. Einige der Meldungen können jetzt mit der Option *--color* auch farbig dargestellt werden. Die Hilfe zu `samba-tool` zeigt, welche Kommandos die farbige Anzeige unterstützen.
- Jetzt können die *dsacl* nicht nur gesetzt werden, sondern bestehende *dsacl* können jetzt mit dem `samba-tool` auch gelöscht werden.
- Mit der neuen Option *–change-secret-at* kann mit `wbinfo` das Passwort des *trust accounts* einer Vertrauensstellung geändert werden.
- Die Verwendung des *Azure AD Connect cloud sync tool*, um Passwörter aus Samba in die Cloud zu synchronisieren, wird jetzt unterstützt.

### Version 4.19 (September 2023)

- Wenn in der smb.conf *winbind debug traceid* = *yes* gesetzt ist, wird in den Winbindlogs ein neuer Trace-Header-Felder *traceid* und die *depth* gespeichert. Das Feld *traceid* erlaubt die Verfolgung der Aufzeichnungen, die zur selben Anfrage gehören. Das Feld *depth* ermöglicht die Verfolgung der Verschachtelungsebene der Anfrage. Ein neues Tool `samba-log-parser` wurde für das Log Parsing hinzugefügt.
- In dieser Version wird die Datenbank für ein neues *Function Level* vorbereitet. Ab dieser Version ist es möglich, das *Function Level 2016* zu nutzen, zusammen mit den AD-Schema 2019. Bei einer Umstellung auf das neue Function Level werden in der Datenbank verschiedene Änderungen vorgenommen:
  - Container für die authentication policies werden hinzugefügt.
  - Container für die authentication silos werden hinzugefügt.
  - Claims werden jetzt unterstützt.

  Bei der Umstellung wird die Datenbank komplett umgestellt, ein Weg zurück ist dann nur noch schwer möglich. Sie sollten auf jeden Fall ein Backup der Datenbank erstellen, bevor Sie das Function Level erhöhen. Da hier noch nicht alle Funktionen vorhanden sind, würde ich mit der Umstellung bis zur Version 4.21 warten. Diese Neuerung ist bei dieser Version der erste Schritt hin zu einem neuen Function Level.
- Kerberos Armoring (FAST) Unterstützung für Windows-Clients-Domänen mit einem Function Level ab 2012 können jetzt via einer GPO so konfiguriert werden, dass die Übermittlung der Passwörter zwischen den Clients und dem Domaincontroller über *FAST* abgesichert wird. Da hier die Verwendung von *AS-REQ* nicht mehr unterstützt wird, ist die Übertragung von Passwörtern erheblich sicherer geworden. Durch den Verzicht auf *AS-REQ* sind offline-Angriffe auf Passwörter nicht mehr möglich. Eine sehr gute, aber englische Beschreibung, wie die Absicherung mit *FAST* funktioniert, finden Sie unter https://medium.com/@business1sg00d/as-req-roasting-from-a-router-2a216c801a2c
- Neuer samba-tool-Support für silos, claims, sites und subnets.
  Diese neuen Funktionen lassen sich über das samba-tool einrichten und verwalten.
- Samba verlangt jetzt GnuTLS 3.6.13, noch besser wäre GnuTLS 3.6.14 oder höher.
- Wenn die Active Directory TLS-Zertifikate erneuert werden, muss der Samba-Dienst nicht mehr neu gestartet werden. Bei allen vorherigen Versionen musste der Dienst beim Austausch der Zertifikate neu gestartet werden. Die Aktualisierung der Zertifikate erfolgt mittels des Kommandos `smbcontrol ldap_server reload-certs`.

### Version 4.20 (März 2024)

- Eine der wichtigsten Sicherheitsfunktionen hat mit der Version 4.20 Einzug gehalten – und zwar die *group managed service accounts*. Wer kennt das nicht: Da wird

ein Benutzer für einen Dienst eingerichtet, der Benutzer bekommt bei der Einrichtung ein Passwort. Dieses Passwort bleibt bestehen, solange der Dienst genutzt wird. Die Passwörter der *group managed service accounts* werden in regelmäßigen Abständen automatisch geändert.

- Das Suchprotokoll „Windows Search Protocol (WSP)“ steht jetzt zur Verfügung, ist aber zur Zeit als *experimental* gekennzeichnet.
- Weiter Verbesserung beim Einsatz von *authentication policies* und *authentication silos*. Der volle Funktionsumfang steht aber erst mit der Samba-Version 4.21 zur Verfügung.
- Jetzt ist das Function Level 2016 soweit implementiert, dass eine Umstellung sinnvoll sein kann. Wie die Function Level eingerichtet werden und wie eine neue Domäne gleich mit dem aktuellen Function Level eingerichtet werden kann, finden Sie in Kapitel 7, »Verwaltung von Domaincontrollern«.
- Unterstützung von bedingten ACEs und Resource Attribute ACEs
  Gewöhnliche Zugriffskontrolleinträge (ACEs) erlauben oder verweigern bedingungslos den Zugang durch einen bestimmten Benutzer oder eine Gruppe. Bedingte ACEs haben einen zusätzlichen Abschnitt, der die Bedingungen beschreibt, unter denen der ACE gilt. Wenn der Bedingungsausdruck wahr ist, funktioniert der ACE wie ein gewöhnlicher ACE, andernfalls wird er ignoriert. Die Bedingungsausdrücke können sich auf Ansprüche, Gruppenmitgliedschaften und Attribute des Objekts selbst beziehen. Diese Attribute werden in Ressourcenattribut-ACEs beschrieben, die in der System Access Control List (SACL) des Objekts vorkommen. Bedingte ACEs sind in der Microsoft-Dokumentation beschrieben (https://learn.microsoft.com/de-de/entra/identity/conditional-access/overview).

  Die bedingte ACE-Auswertung wird durch die Option *acl claims evaluation* in der smb.conf gesteuert. Der Standardwert ist *only AD DC*, was die AD DC-Einstellungen aktiviert. Die andere Option ist *never*, die deaktiviert sie gänzlich. Derzeit gibt es keine Option, um sie auf einem Samba-Fileserver zu aktivieren (das wird erst in zukünftigen Versionen möglich sein).
- Die *Security Descriptor Definition Language* hat Erweiterungen für bedingte ACEs und Ressourcen-Attribut-ACEs; diese werden jetzt von Samba unterstützt.

### Version 4.21 (September 2021)

- In allen vorherigen Samba-Versionen war es so, dass wenn die Einträge *valid users*, *invalid users*, *read list* und *write list* Namen enthielten, die keinen gültigen SID hatten, der Benutzer oder die Gruppe einfach ignoriert wurden. Ab dieser Version kommt es zu einem Fehler, wenn ein Benutzername nicht gegen einen Domaincontroller aufgelöst werden kann. Jeder *TREE_CONNECT* wird dabei zu einem Fehler führen.

- LDAP TLS/SASL channel binding support
  Der LDAP-Server von Samba unterstützt jetzt *SASL binds* mit TLS oder NTLMSSP. Verbindungen können sowohl über ldaps als auch über starttls hergestellt werden. Die Option *ldap server require strong auth = allow_sasl_over_tls* ist nicht mehr notwendig.
- Für die Einbindung eines Ceph-Clusters steht ein neu überarbeitetes VFS-Module *cephfs* zur Verfügung. Die Unterstützung für *Group Managed Service Accounts* ist in dieser Version erstmals vollständig implementiert. Die Passwörter für die *Group Managed Service Accounts* werden über *root-keys* generiert. Die Keys können Sie über das Kommando `samba-tool domain kds root_key create` erzeugen und mit dem Kommando `samba-tool domain kds root_key list` auflisten. Samba wird beim Erstellen der Domäne immer einen neuen root-key erzeugen. Der root-key muss nur dann von Hand erzeugt werden, wenn die Domäne auf das neue Function Level angehoben wird.
- Die Struktur der Kommandos für die *authentication policies* und *Authentication Silo* im `samba-tool` wurde komplett überarbeitet und erlaubt es jetzt, policies und silos vollständig zu erstellen.
- Veto Files sind jetzt auch für einzelne Benutzer oder Gruppen möglich. Die beiden Parameter *hide files* und *veto files* können jetzt bestimmten Benutzern oder Gruppen zugeordnet werden. Der Parameter kann in der smb.conf mehrfach eingetragen werden, so wie es Listing 2.2 zeigt:

  **Listing 2.2** Gruppen und Benutzer für veto files

  ```
  hide files : USERNAME = /somefile.txt/
  veto files : GROUPNAME = /otherfile.txt/
  ```

Neben den hier aufgeführten Änderungen hat sich in den letzten Versionen auch viel hinsichtlich der Performance, der Sicherheit und der Stabilität von Samba getan. Wenn Sie alle Neuerungen nachlesen möchten, finden Sie diese in den Release Nodes auf https://www.samba.org.

Viele der Änderungen betreffen die Sicherheit von Samba. Ich habe in dieser Auflage des Buches ein extra Kapitel zum Thema Sicherheit geschrieben, in dem ich auf einige dieser neuen Funktionen und Möglichkeiten näher eingehe. Ich habe die Möglichkeiten bewusst aus den ersten Kapiteln der Konfiguration der Domäne herausgenommen, da ich Ihnen so zeigen kann, wie Sie eine neue oder eine bestehende Domäne auch nachträglich noch absichern können. Sollten bestimmte Techniken schon bei der Einrichtung der Domäne benötigt werden, spreche ich diese Themen dann auch an der Stelle schon an.

Sie sehen, es hat sich viel getan in den letzten vier Jahren.

# 3
# Installation von Samba

In diesem Kapitel geht es um die verschiedenen Möglichkeiten, Samba 4 zu installieren. Im Gegensatz zur letzten Auflage werde ich hier nicht mehr auf das Compilieren von Samba eingehen. Das Vorgehen ist nicht mehr so trivial wie bei den älteren Versionen und würde hier im Buch zu viel Platz benötigen, den ich lieber für andere Themen nutzen möchte.

Ich werde für die Funktion des Domaincontrollers, der Fileserver und der CTDB-Server auf die Pakete aus den Debian 12 Backports zurückgreifen, um dort möglichst die aktuellen Funktionen erklären zu können. Auf den Clients werde ich immer die Pakete der Distributionen nutzen. Wenn Sie aber den vollen Funktionsumfang der Gruppenrichtlinien für Linux-Clients im Active Directory nutzen wollen, geht das nur, wenn Sie auch auf den Clients die Samba-Version 4.21 nutzen.

Auch möchte ich hier wieder die Installation der SerNet-Pakete mit aufnehmen. Der eine oder andere, der gerne Support für Software nutzen möchte, ist mit den SerNet-Paketen sehr gut beraten. Auch sind die Pakete sehr stabil und aktuell. Ein weiterer Grund, der für die SerNet-Pakete spricht, ist die Unterstützung für Red-Hat- und Suse-Distributionen. Denn mithilfe der SerNet-Pakete können Sie auch auf diesen Distributionen Domaincontroller installieren.

Nachdem Sie sich Gedanken darüber gemacht haben, welche Distribution und Samba-Version Sie einsetzen möchten, bleibt für Sie die Entscheidung, welchen Weg der Installation Sie gehen wollen und welche Distribution Sie nutzen möchten. Bei der Installation des Active Directory-Domaincontrollers wird immer auch ein Kerberos-Server benötigt. Samba verwendet hierfür im Moment noch den Heimdal-Kerberos. Seit der Version 4.7 wird zwar auch der MIT-Kerberos unterstützt, aber der Einsatz ist immer noch als *experimental* gekennzeichnet. Damit fallen die Pakete der Distributionen aus der Auswahl, die nur den MIT-Kerberos bereitstellen. Dazu gehören *Fedora*, *Red Hat*, *Suse* und *Alma Linux*. Wollen Sie eine dieser Distributionen verwenden, kön-

nen Sie hierfür nicht die von der Distribution bereitgestellten Pakete benutzen. Für diese Distributionen bleiben Ihnen nur zwei Wege: die Installation aus den Quellen, wobei Sie dann auch den Kerberos-Server mit bauen müssen, oder die Installation der SerNet-Pakete. Suse stellt zwar die Funktion des Domaincontrollers zur Verfügung, nutzt aber dafür die experimentelle Unterstützung des MIT-Kerberos-Servers.

Die Funktion des Fileservers kann aber mit allen Paketen aus den Distributionen realisiert werden. Wenn Sie die Pakete der Distributionen einsetzen, dann achten Sie darauf, dass die Samba-Version die von Ihnen benötigten Funktionen unterstützt.

In den folgenden Abschnitten werde ich Ihnen die Installation auf verschiedenen Wegen an Beispielen erklären und die Vor- und Nachteile ansprechen. Die Art und Weise, die Sie letztendlich auswählen, ist abhängig von den Funktionen, die Sie benötigen.

## 3.1 Die verschiedenen Installationsarten

Damit Sie eine Übersicht über die verschiedenen Installationsarten bekommen, habe ich hier die unterschiedlichen Arten mit ihren Vor- und Nachteilen aufgeführt.

### 3.1.1 Installation eines Domaincontrollers aus den Distributionspaketen

Bei Debian 12 wird (Stand beim Schreiben des Buches) in den offiziellen Repositories die Version 4.17 bereitgestellt. Diese Version ist aber schon zu alt, denn es gibt keine offiziellen Updates mehr. In den Backports zu Debian 12 befindet sich aber die Version 4.21, also die momentan aktuellste Version. Das wird auch die Version sein, die ich hier im Buch verwenden werde.

#### Vor- und Nachteile der Paketinstallation eines ADDC

Wenn Sie die Domaincontroller-Funktion direkt aus den Paketen der Distribution installieren, haben Sie den Vorteil, dass Sie alle Sicherheitsupdates automatisch erhalten und keine zusätzlichen fremden Quellen benötigen. Das betrifft auch die Installation aus den Debian Backports. Der Nachteil ist aber, dass Sie nie die aktuellste Version von Samba 4 erhalten und neue Funktionen daher nicht nutzen können. Wenn der Funktionsumfang der hier vorgestellten Distributionspakete für Sie ausreichend ist, sind Sie mit dieser Art der Installation gut beraten. Die Debian Backports werden außerhalb der regulären Repositories bereitgestellt. Da diese Pakete oft noch nicht durch alle Tests gelaufen sind, ist es in vielen Firmen nicht erlaubt, die Pakete aus den Backports zu nutzen.

### 3.1.2 Installation eines Fileservers aus den Distributionspaketen

Für die Funktion des Fileservers können Sie jede der großen Distributionen einsetzen. Da für den Fileserver kein Kerberos-Server benötigt wird, haben Sie bei allen Distributionen die Möglichkeit, einen Fileserver oder Client als Mitglied einer Active-Directory-Domäne zu installieren. Hier besteht nur ein Unterschied zwischen den bereitgestellten Versionen von Samba 4. Nach der Installation ist die Konfiguration bei allen Distributionen identisch.

#### Vor- und Nachteile der Paketinstallation eines Fileservers

Hier gilt das Gleiche wie schon vorher beim Domaincontroller. Wenn die Funktionen reichen, die Ihnen die Pakete aus der Distribution bieten, dann nehmen Sie diese Pakete. Aber auch hier gilt, dass Sie mit diesen Paketen nie den aktuellen Stand von Samba 4 erhalten. Wenn Sie einen CTDB-Cluster mit Samba realisieren wollen, dann ist es angebracht, wie auch schon beim Domaincontroller, eine möglichst aktuelle Samba-Version zu nutzen, da gerade hier immer sehr viele Änderungen stattfinden.

### 3.1.3 Installation aus den Quellen

Bei dieser Art der Installation können Sie auf allen Distributionen sowohl den Active-Directory-Domaincontroller als auch den Fileserver installieren. Für jede Distribution müssen Sie dann die passende *Build-Umgebung* installieren. Auch GnuTLS und Python verlangt hier mittlerweile mehr Vorbereitung und ist nicht mehr so einfach wie bei älteren Versionen. Aus diesem Grund werde ich in dieser Auflage nicht mehr auf das Selberbauen von Samba eingehen.

#### Vor- und Nachteile der Installation aus den Quellen

Sie sind mit einer Installation aus den Quellen immer auf dem neuesten Stand der Entwicklung und können so auch immer alle Funktionen von Samba nutzen. Auch Distributionen, die über die Pakete die Funktion des Domaincontrollers nicht unterstützen, können Sie so als Domaincontroller einrichten. Aber: Sie haben immer eine Build-Umgebung mit Compiler und allen Libraries auf dem System und müssen für jedes Update Samba neu bauen. Ein einfaches Update ist nicht möglich. Gerade im produktiven Einsatz sollten Sie sich überlegen, ob das der richtige Weg ist. Sie müssen sich neben den Updates auch um alle anderen Abhängigkeiten selbst kümmern. Wenn Sie für sich die Entscheidung treffen, Samba aus den Quellen zu installieren, dann bauen Sie unbedingt ein Testsystem auf, auf dem Sie jedes neue Update erst testen.

### 3.1.4 Installation der SerNet-Pakete

Mit der Version 4.3 hat die Firma SerNet die kostenfreie Bereitstellung der Samba-Pakete eingestellt. Die aktuellen Pakete können Sie nur noch über eine Subscription nutzen. Trotzdem sind die SerNet-Pakete immer noch eine sehr gute Alternative für den produktiven Einsatz. Die Stabilität und die Versorgung mit Updates ist sehr gut. Auch die Migration auf eine höhere Samba-Version ist gut getestet und unproblematisch.

Die Pakete stellen für alle unterstützten Distributionen (dazu zählen auch Red-Hat- und Suse-Systeme) immer auch die Funktion des Domaincontrollers zur Verfügung, sind immer auf dem aktuellen Stand und lassen sich über Repositories in das System einbinden und somit auch einfach aktualisieren. Wenn Sie also im Unternehmen eine andere Distribution als Debian oder Ubuntu nutzen, können die SerNet-Pakete eine sehr gute Wahl sein.

#### Vor- und Nachteile der Installation aus den SerNet-Paketen

Mit den SerNet-Paketen erhalten Sie aktuelle Pakete, die sich einfach verwalten und aktualisieren lassen. Durch den Support wird sichergestellt, dass die Pakete auch ohne Probleme auf eine neue Version aktualisiert werden können. Der Nachteil ist, dass die Pakete nicht mehr kostenlos bereitgestellt werden.

**Hinweis**

In der letzten Auflage habe ich hier noch die Pakete von Louis van Belle aufgeführt, aber auch gleich erläutert, welche Nachteile es hat, Pakete zu nutzen, die nur von einer Person gepflegt werden. Seit ein paar Jahren gibt es diese Pakete nicht mehr, da Louis von einem auf den anderen Tag keine neuen Pakete mehr bereitgestellt hat. Überlegen Sie sich daher genau, welche Paketquelle Sie nutzen wollen.

## 3.2 Installation

In diesem Abschnitt zeige ich Ihnen, welche Pakete Sie für Domaincontroller oder Fileserver installieren müssen. Die Installation auf dem Debian-System bezieht sich dabei auf die Pakete in den Backports.

Um die Backports von Debian nutzen zu können, ist es notwendig, dass Sie die Datei /etc/apt/sources.list um die Zeile aus Listing 3.1 erweitern:

**Listing 3.1** Einbinden der Backports

```
deb http://deb.debian.org/debian bookworm-backports main
```

Anschließend aktualisieren Sie Ihre Repository-Liste mit dem Kommando `apt-get update`.

### Installation über die Pakete

Wie bei Debian üblich, werden die Pakete hier über die Kommandozeile mittels `apt-get` installiert. Listing 3.2 zeigt die Installation für einen ADDC:

**Listing 3.2** Installation unter Debian 12

```
root@dc01:~# apt-get -t bookworm-backports install  samba-ad-dc \
        samba-ad-provision bind9 bind9utils dnsutils lmdb-utils ldb-tools
```

Allen, die schon mal früher Samba als Domaincontroller unter Debian installiert haben, fällt hier auf, dass es jetzt eigene Pakete für die Einrichtung eines Domaincontrollers gibt. Die Pakete bind9, bin9utils und dnsutils benötigen Sie nur, wenn Sie den `Bind9` als DNS-Backend einsetzen wollen. Bei der Konfiguration des ersten Domaincontrollers in Kapitel 5 werde ich näher auf die Unterschiede und die verschiedenen Einrichtungen eingehen. Das Paket lmdb-utils benötigen Sie nur, wenn Sie anstelle der TDB-Datenbanken die LMDB-Datenbanken für Ihre Objekte verwenden wollen. Mehr dazu finden Sie in Kapitel 4, »Einrichten des ersten Domaincontrollers«.

Die Konfigurationsdatei smb.conf befindet sich später im Verzeichnis /etc/samba. Diese Datei ist bei Debian und Ubuntu nach der Installation der Pakete bereits vorhanden. Löschen Sie diese Datei vor dem Einrichten der Domäne auf jeden Fall, da es sonst zu Fehlern während der Einrichtung der Domäne kommt. Alle Dateien, die Datenbanken und die sysvol-Freigabe befinden sich im Verzeichnis /var/lib/samba.

Wenn Sie einen Domaincontroller unter Debian einrichten wollen und aus dem Grund die Pakete aus den Backports installiert haben, ist es nicht mehr notwendig, den Systemd anzupassen. Da die Pakete für den Domaincontroller extra installierbar sind, wird bei der Installation der Pakete auch gleich der Systemd korrekt eingerichtet.

Für den Fileserver oder einen Linux-Client installieren Sie die Pakete aus Listing 3.3:

**Listing 3.3** Pakete für den Linux-Fileserver und -Clients

```
apt-get install -t bookworm-backports samba winbind samba-vfs-modules \
               libpam-winbind libnss-winbind smbclient libpam-heimdal
```

## 3.2.1 Installation der SerNet-Pakete

Für alle großen Distributionen können Sie auf die Pakete der Firma SerNet zurückgreifen. Wie anfangs schon beschrieben, haben Sie mit diesen Paketen den großen Vorteil, dass Sie einfach die Repositories in Ihr System einbinden und dann über die Paketverwaltung Ihrer Wahl die Pakete installieren und aktuell halten können. Die Pakete sind immer auf dem aktuellsten Stand der Samba-Entwicklung, und Sie können somit auch alle neuen Funktionen wie den Aufbau eines CTDB-Clusters oder der Domain-Trusts verwenden.

Da die Installation der SerNet-Pakete für alle Distributionen nahezu identisch ist, werde ich an dieser Stelle nur die Installation der Pakete unter Debian genau beschreiben. Wenn Sie eine andere Distribution verwenden, können Sie einfach den Anleitungen auf der SerNet-Website folgen.

Um überhaupt auf die aktuellen Pakete zugreifen zu können, benötigen Sie als Erstes eine Subscription, die Sie über die Website https://shop.samba.plus/samba erwerben können. Eins spezielles Passwort, um die Repositories nutzen zu können, benötigen Sie nicht mehr. Der Subscription Key und ein Standardpasswort sind ausreichend.

Erweitern Sie Ihre Datei /etc/apt/sources.list um die Zeilen aus Listing 3.4:

**Listing 3.4** Erweiterung der Datei /etc/apt/sources.list

```
deb https://KEY:PASSWORD@download.sernet.de/subscriptions/samba/\
          4.14/debian bookworm main
deb-src https://KEY:PASSWORD@download.sernet.de/subscriptions/samba/\
          4.14/debian bookworm main
```

Dabei müssen Sie den *KEY* durch Ihren Subscription Key ersetzen und das *PASSWORD* durch das Standardpasswort.

Bevor Sie jetzt ein `apt-get upgrade` durchführen können, installieren Sie erst noch die GPG-Schlüssel. Dieser Vorgang ist nur für Debian-basierte Distributionen nötig, bei allen anderen Distributionen wird der GPG-Key beim Update der Repository-Listen automatisch installiert. Zusätzlich müssen Sie bei Debian das Paket für HTTPS-Verbindung über `apt-get` installieren. Listing 3.5 zeigt diesen Vorgang:

**Listing 3.5** Installieren der GPG-Schlüssel

```
root@sambabuch:~# apt-get install apt-transport-http

root@sambabuch:~# wget \
   https://download.sernet.de/pub/sernet-samba-keyring_latest_all.deb

root@sambabuch:~# dpkg -i sernet-samba-keyring_latest_all.deb
```

Nach einer Aktualisierung der Repositories können Sie sich die Liste der Pakete, die SerNet bereitstellt, auflisten lassen.

Wollen Sie jetzt einen Domaincontroller installieren, benötigen Sie die Pakete wie in Listing 3.6:

**Listing 3.6** Installation der ADDC-Pakete

```
root@dc01:~# apt-get install sernet-samba-ad libpam-heimdal lmdb-utils
```

Wollen Sie einen Domainmember installieren, benötigen Sie die Pakete aus Listing 3.7:

**Listing 3.7** Installation der Member-Pakete

```
root@dc01:~# apt-get install sernet-samba sernet-samba-winbind \
                                    libpam-heimdal
```

**Hinweis**

Wenn Sie den Domaincontroller zusammen mit Bind9 einrichten wollen, benötigen Sie noch die Pakete bind9, bind9utils und dnsutils.

In der Konfigurationsdatei /etc/default/sernet-samba legen Sie die Startart des Samba-Dienstes fest. Über die Variable *SAMBA_START_MODE=none* können Sie entscheiden, ob Samba als Domaincontroller *SAMBA_START_MODE=dc* oder als Memberserver/Client *SAMBA_START_MODE=classic* gestartet wird.

**Hinweis**

Diese Datei finden Sie für die SerNet-Pakete auf allen Distributionen. Daher ist es sehr einfach, Samba auf verschiedenen Distributionen einzusetzen, da die Installation und Aktivierung der Dienste immer identisch sind.

Wie immer bei den SerNet-Paketen wird keine smb.conf bei der Installation der Pakete bereitgestellt.

Wenn Sie einen neuen Domaincontroller oder Memberserver oder einen Client installieren wollen, können Sie in diesem Kapitel alle Schritte nachvollziehen. Im weiteren Verlauf werde ich daher die Installation der Samba-Software nicht mehr erklären, da von diesem Zeitpunkt die weitere Administration immer identisch ist, egal welchen Weg der Installation und welche Distribution Sie gewählt haben.

# 4

# Einrichten des ersten Domaincontrollers

Nach der ausführlichen Beschreibung der Installation im letzten Kapitel geht es jetzt darum, den ersten Samba-Active-Directory-Domaincontroller einzurichten. Dabei geht es nicht nur um die reine Konfiguration, sondern auch um einige Tests, mit denen Sie die Funktion des Domaincontrollers überprüfen können.

Für Samba 4 wird, wie auch bei einem Windows-Domaincontroller, auf jeden Fall ein *Kerberos-Server* für die Authentifizierung der Benutzer benötigt. Dieser wird von Samba 4 bereitgestellt.

**Hinweis**

Zurzeit wird hier noch der Heimdal-Kerberos verwendet. Der MIT-Kerberos-Server hat immer noch den Status *experimental*.

Zusätzlich benötigt Samba 4 auf jeden Fall einen DNS-Server, der nicht nur zur Auflösung der Hostnamen dient, sondern auch zur Auflösung der benötigten Dienste in der Domäne – den SRV-Records. Der DNS-Server kann entweder von Samba 4 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 verschiedener Reihenfolge an die Clients zu geben. Diese Funktion ist unerlässlich, wenn Sie planen, einen CTDB-Cluster in Ihren Domänen einzurichten. Sobald Sie Samba als Active Directory in einer größeren Umgebung mit vielen Clients und Servern einsetzen, ist es auf jeden Fall sinnvoll, den Bind9 zu nutzen. Ich werde Ihnen hier auf jeden Fall beide Varianten erklären.

## 4.1 Allgemeines zum Einrichten des Domaincontrollers

Für die Konfiguration und Administration eines Samba-4-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 vom verwendeten DNS-Server ist. Es spielt keine Rolle, ob Sie den internen DNS-Server oder Bind9-DNS-Server verwenden.

Aufgrund der vielen neuen Möglichkeiten, die Ihnen das Kommando `samba-tool` bietet, werde ich in den verschiedensten Kapiteln immer wieder die gerade benötigten Punkte des Menüs besprechen. In Kapitel 17, »Samba 4 über die Kommandozeile verwalten«, werde ich dann alle bis dahin noch nicht angesprochenen Punkte aufgreifen.

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

```
Available subcommands:
  computer         - Computer management.
  contact          - Contact management.
  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.
  forest           - Forest management.
  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.
  ou               - Organizational Units (OU) management.
  processes        - List processes (to aid debugging on systems without
      setproctitle).
  rodc             - Read-Only Domain Controller (RODC) management.
  schema           - Schema querying and management.
  service-account  - Service Account and Group Managed Service Account
      management.
  shell            - Open a SAMBA Python shell.
  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.
```

Wenn Sie diese Ausgabe mit einer älteren Samba-Version vergleichen, werden Sie hier schon feststellen, dass einige Punkte neu hinzugekommen sind. Auch in den einzelnen Untermenüs gibt es weitere Neuerungen.

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.

### 4.1.1 Datenbankformat

Seit Samba 4.11 ist das LMBD-Format das bevorzugte Datenbankformat. Das Datenbankformat hat erhebliche Vorteile gegenüber dem alten TDB-Format. Die Datenbankgröße kann größer sein, und die Zugriffe sind schneller. Die Standardgröße der Datenbank ist jetzt 8 GB.

LMDB verwendet *memory mapped files*. Bei einer Standardgröße von 8 GB zeigen Werkzeuge wie `htop` eine Nutzung des virtuellen Speichers zwischen 40 GB und 80 GB an. Das ist aber kein Fehler, sondern hängt mit der Eigenart der LMBD zusammen. Mehr zu dem Thema finden Sie unter https://symas.com/understanding-lmdb-database-file-sizes-and-memory-utilization/.

Halten Sie den Datenbanktyp des Backends auf allen Domaincontrollern möglichst identisch. Das TDB-Format kann nicht dieselbe Anzahl an Objekten halten wie das LMDB-Format. Wenn Sie also einen Domaincontroller mit LMDB einrichten, stellen Sie auch alle bestehenden Domaincontroller um.

Um das LMDB-Backend zu verwenden, geben Sie beim Provisioning oder beim Join eines neuen Domaincontrollers den Parameter *--backend-store=mdb* mit an. Sie benötigen dann auf jeden Fall das Paket lmdb-utils.

Ob auf einem Domaincontroller das LMDB-Backend verwendet wird, können Sie einfach testen, indem Sie sich den Inhalt des Datenbankverzeichnisses /var/lib/samba/private/sam.ldb.d/ anzeigen lassen. Dort sehen Sie dann die Dateien aus Listing 4.2:

**Listing 4.2** Erkennen ob LMDB genutzt wird

```
CN=CONFIGURATION,DC=EXAMPLE,DC=NET.ldb
CN=CONFIGURATION,DC=EXAMPLE,DC=NET.ldb-lock
CN=SCHEMA,CN=CONFIGURATION,DC=EXAMPLE,DC=NET.ldb
CN=SCHEMA,CN=CONFIGURATION,DC=EXAMPLE,DC=NET.ldb-lock
DC=DOMAINDNSZONES,DC=EXAMPLE,DC=NET.ldb
DC=DOMAINDNSZONES,DC=EXAMPLE,DC=NET.ldb-lock
```

```
DC=EXAMPLE,DC=NET.ldb
DC=EXAMPLE,DC=NET.ldb-lock
DC=FORESTDNSZONES,DC=EXAMPLE,DC=NET.ldb
DC=FORESTDNSZONES,DC=EXAMPLE,DC=NET.ldb-lock
```

Zu jeder Datenbank mit der Endung .ldb gehört immer auch eine Datei mit der Endung .ldb-lock. Wollen Sie eine bestehenden Domäne mit allen Domaincontrollern auf das LMDB-Backend umstellen, joinen Sie einen neuen Domaincontroller mit dem LMDB-Backend in die Domäne, nehmen dann nach und nach alle Domaincontroller einzeln aus der Domäne und joinen sie erneut mit dem LMDB-Backend.

### 4.1.2 Vorbereitungen für den ersten Domaincontroller

Bevor Sie die Konfiguration des Domaincontrollers mit dem Kommando `samba-tool domain provision` durchführen, sorgen Sie dafür, dass Sie die benötigten Informationen besitzen. Bei der Konfiguration des Domaincontrollers werden sie abgefragt. Die folgenden Informationen sind relevant für die Konfiguration einer neuen Domäne:

- Der Realm:
  Der `Realm` wird für den Kerberos-Server benötigt. Der Realm wird bei der Einrichtung des DNS-Servers auch als DNS-Domainname verwendet.
- Der 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. Der NetBIOS-Name dient auch im Zeitalter ohne NetBIOS für die Adressierung der Domäne und muss im Netzwerk eindeutig sein.
- Die Funktion des Servers:
  Welche Rolle soll der Server in der Domäne übernehmen? In unserem Fall übernimmt er die Rolle des Domaincontrollers.
- Welchen DNS-Server wollen Sie verwenden?
  Überlegen Sie, ob Sie den internen DNS-Server von Samba 4 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.

  Wenn Sie Bind9 nutzen, wird der Forwarder dort eingetragen, nur beim Einsatz des internen DNS-Servers benötigen Sie die IP des Forwarders für das Provisioning.

Bevor Sie das Provisioning starten, werfen Sie einen Blick auf alle möglichen Optionen, 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, wird beim Provisioning das spezielle Schema für Unix-Attribute eingerichtet. Die Attribute aus dem Schema können Sie beim Anlegen von Benutzern und Gruppen mit Werten füllen. Es handelt sich unter anderem um die Attribute *UID* und *GID*. Diese Attribute können Sie dann bei den Benutzern mit angeben, wenn Sie einen neuen Benutzer oder eine neue Gruppe anlegen. Die Nummerierung der Benutzer und Gruppen müssen Sie aber immer 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. Nur wenn Sie eventuell aus einer alten Samba-3-Umgebung migrieren und die Dateisystemrechte auf den Server der Domäne nicht ändern wollen, kann es Sinn machen, das Schema für die rfc2307-Attribute mit einzubinden. Denn dann können Sie den Benutzern und Gruppen die alten UIDs und GIDs zusätzlich vergeben und so die Rechtestruktur auf den Fileservern beibehalten. Wenn Sie aber einen überschaubaren Datenbestand haben oder mit der Migration der Domäne auch gleich neue Fileserver einrichten wollen, dann ist es besser, Sie verzichten auf die Unix-Attribute und arbeiten nur noch mit der SID der Benutzer und Gruppen. Das hat den Vorteil, dass Sie sich später keine Gedanken mehr über die Vergabe der UIDNumber und GIDNumber machen müssen, denn der SID eines Objekts wird automatisch beim Anlegen vergeben und bleibt immer identisch.

**Hinweis**

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

Außer bei der Migration von Samba 3 werde ich hier im Buch immer ohne das rfc2307-Schema arbeiten.

## 4.2 Konfiguration des ersten Domaincontrollers

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 die Lastverteilung bei Diensten über DNS Round Robin realisieren wollen, geht das nur, wenn Sie den Bind9 nutzen.

**Wichtig**

Wenn Sie den internen DNS-Server von Samba nutzen wollen, installieren Sie unter gar keinen Umständen die bind9-Pakete. Denn wenn Sie den Bind9 installieren, wird er bei Debian und Ubuntu auch sofort gestartet und belegt die entsprechenden Ports, sodass der interne DNS von Samba sie nicht nutzen kann. Bei aktuellen Samba-Versionen können Sie zwar den Port des internen DNS-Servers ändern, aber dann hätten Sie zwei DNS-Server, von denen einer nicht genutzt wird.

Beim Provisioning haben Sie die Möglichkeit, interaktiv die Einrichtung durchzuführen, oder Sie können alle benötigten Parameter gleich auf der Kommandozeile angeben. Die Einrichtung unter Verwendung der Kommandozeilenoptionen hat den Vorteil, dass Sie später die Einrichtung der Domaincontroller automatisieren können. In Teil 1 der Einrichtung werde ich Ihnen beide Möglichkeiten zeigen. Im zweiten Teil, bei der Verwendung von Bind9, werde ich die Domäne nur über die Kommandozeile einrichten und dort auch das neue Datenbankformat LMDB nutzen.

Selbstverständlich können Sie das neue Datenbankformat auch mit dem internen DNS-Server nutzen, indem Sie zusätzlich den Parameter *--backend-store=mdb* angeben. Wollen Sie das LMDB-Format für Ihre Datenbank nutzen, dann installieren Sie zusätzlich das Paket lmdb-utils, ohne dieses Paket bricht die Provisionierung mit einer Fehlermeldung ab.

Bevor Sie jetzt mit der Einrichtung des ersten Domaincontrollers beginnen, prüfen Sie zuvor die folgenden Punkte:

- Haben Sie in der Datei /etc/hostname lediglich den Hostnamen eingetragen und nicht den vollständigen FQDN des Servers?
- Stimmt der DNS-Server in der Datei /etc/resolv.conf? Die dort eingetragene IP wird als Forwarder übernommen.
- Steht in der Datei /etc/host ein Eintrag für die IP-Adresse des Servers mit vollständigem FQDN?
- Handelt es sich bei der IP-Adresse des Servers um eine statische IP?
- Zeigt das Kommando `hostname -f` den FQDN des Servers an?
- Haben Sie die Datei /etc/samba/smb.conf vor der Installation der Pakete gelöscht?

Alle diese Informationen werden für das Provisioning benötigt. Eine bestehende smb.conf führt zum Abbruch des Provisioning.

### 4.2.1 Teil 1 mit dem internen DNS-Server (interaktiv)

Im ersten Beispiel sehen Sie in Listing 4.3 den Ablauf der Konfiguration des ersten Domaincontrollers mit interaktiver Abfrage der benötigten Parameter:

**Listing 4.3** Provisioning mit internem DNS-Server

```
root@dc01:~# samba-tool domain provision
```

Die Warnung hinsichtlich *Unable to determine the DomainSID* können Sie ignorieren. Diese Warnung werden Sie immer bei der Einrichtung des ersten Domaincontrollers sehen. Wenn Sie die erste Domäne einrichten, versucht der Prozess des Provisionings, weitere Domänen im Netz zu finden, um die Eindeutigkeit des Domain-SID zu prüfen. Es gibt aber noch keine, daher die Meldung.

Eine weitere Meldung möchte ich hier noch ansprechen, und zwar *More than one IPv4 address found*. Diese Meldung zeigt an, dass der Server mehr als eine IP-Adresse besitzt und sich das Provisioning eine IP-Adresse ausgesucht hat, über die die Dienste bereitgestellt werden. Wenn Sie von vornherein eine IP-Adresse festlegen wollen, können Sie das über den Parameter *--host-ip=<IP>* festlegen. Tragen Sie dann, nach dem Provisioning, zusätzlich im globalen Teil der smb.conf die beiden Zeilen aus Listing 4.4 ein:

**Listing 4.4** Interfaces-Eintrag in der smb.conf

```
interfaces = 192.168.56.101
bind interfaces only = yes
```

Anstelle der IP-Adresse können Sie auch den Gerätenamen der Netzwerkkarte eintragen, die Samba nutzen soll. Damit wäre das Provisioning abgeschlossen. Sorgen Sie jetzt noch dafür, dass der Dienst *samba-ad-dc* anstelle der einzelnen Daemons *smbd*, *nmbd* und *winbind* gestartet wird.

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.

### 4.2.2 Teil 1 mit dem internen DNS-Server (über Parameter)

Wollen Sie das Provisioning interaktiv durchführen, benötigen Parameter beim Aufruf des Kommandos `samba-tool` keine weiteren Parameter. Alle benötigten Angaben werden abgefragt, Sie sehen die Einrichtung in Listing 4.5:

**Listing 4.5** Provisioning mit Parametern

```
root@addc-01:~# samba-tool domain provision --domain=example
root@dc01:~# 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) [1.1.1.1]:
Administrator password:
Retype password:
...
2417: gkdi/gmsa root key added with guid 497c4bed-10e3-b3e9-9e74-49
    f66f0d12ec
2428: A Kerberos configuration suitable for Samba AD has been generated \
      at /var/lib/samba/private/krb5.conf
2430: Merge the contents of this file with your system krb5.conf or \
      replace with this one. Do not create a symlink!
492: Once the above files are installed, your Samba AD server will be
    ready to use
497: Server Role:           active directory domain controller
#498: Hostname:             dc01
499: NetBIOS Domain:        EXAMPLE
500: DNS Domain:            example.net
501: DOMAIN SID:            S-1-5-21-599396760-1979693784-3947908371
```

Bei der reinen interaktiven Einrichtung der Domäne wird das TDB-Format für die Datenbank genutzt und auch noch das alte Function Level 2008_R2. Wollen Sie das Function Level 2016 nutzen und das LMDB-Format der Datenbank, übergeben Sie zusätzlich die dafür benötigten Parameter. Listing 4.6 zeigt das gekürzte Ergebnis der Einrichtung.

**Listing 4.6** Provisioning mit zusätzlichen Parametern

```
samba-tool domain provision --domain=example --backend-store=mdb \
          --option="ad dc functional level = 2016" \
          --function-level=2016 --real=example.net --adminpass=Passw0rd
```

Wenn Sie das Kommando so nutzen, haben Sie jetzt eine neue Domäne mit dem LMDB-Backend, dem neuen Function Level 2016 und dem internen DNS-Server eingerichtet.

Schauen Sie sich einmal die neue smb.conf an, dort finden Sie die Einträge aus Listing 4.7:

**Listing 4.7** Die neue smb.conf

```
[global]
        ad dc functional level = 2016
        dns forwarder = 1.1.1.1
        netbios name = DC01
        realm = EXAMPLE.NET
        server role = active directory domain controller
        workgroup = EXAMPLE
```

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

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

Der Parameter *ad dc function level = 2016* zeigt an, dass die Domäne bereits mit dem neuen Function Level ausgestattet ist. Das können Sie mit dem Kommando `samba-tool domain level show` prüfen. Die Ausgabe des Kommandos sehen Sie in Listing 4.8:

**Listing 4.8** Anzeige des Function Levels

```
root@dc01:~# samba-tool domain level show
Domain and forest function level for domain 'DC=example,DC=net'

Forest function level: (Windows) 2016
Domain function level: (Windows) 2016
Lowest function level of a DC: (Windows) 2016
```

Das verwendete Schema können Sie nur über das Kommando `ldbsearch` erfragen. Sollte das Kommando noch nicht zur Verfügung stehen, installieren Sie das Paket ldb-tools nach. Listing 4.9 zeigt die gekürzte Ausgabe:

**Listing 4.9** Abfrage des Schemas

```
ldbsearch -H /var/lib/samba/private/sam.ldb -b 'cn=Schema,\
             cn=Configuration,dc=example,dc=net' -s base
# record 1
dn: CN=Schema,CN=Configuration,DC=example,DC=net
objectClass: top
objectClass: dMD
cn: Schema
instanceType: 13
whenCreated: 20241118185233.0Z
uSNCreated: 13
showInAdvancedViewOnly: TRUE
name: Schema
objectGUID: 321edf54-392a-463a-a90d-9c79f9d287e9
objectCategory: CN=DMD,CN=Schema,CN=Configuration,DC=example,DC=net
msDS-NcType: 0
objectVersion: 88
```

Relevant ist das Attribut *objectVersion: 88*. Das zeigt an, dass es sich hier mindestens um das Schema 2019 handelt. Mehr zu dem Thema finden Sie unter https://wiki.samba.org/index.php/AD_Schema_Version_Support.

### 4.2.3 Nach dem Provisioning mit dem internen DNS

Nachdem Sie das Provisioning durchgeführt haben und den Dienst das erste Mal starten wollen, prüfen Sie die folgenden Punkte:

- Stellen Sie sicher, dass jetzt in der Datei /etc/resolv.conf die IP-Adresse des Servers selbst eingetragen ist.
- Denken Sie daran, dass das Passwort des Administrators unter Samba 4, im Gegensatz zu Windows, ein Ablaufdatum hat.
- Prüfen Sie, ob der richtige Forwarder in der smb.conf eingetragen wurde.
- Kopieren Sie die Datei /var/lib/samba/private/krb5.conf in das Verzeichnis /etc.

Jetzt können Sie den Samba-Domaincontroller das erste Mal mit dem Kommando `systemctl restart samba-ad-dc` neu starten. Der Domaincontroller kann jetzt genutzt werden.

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

In Teil 2 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, installieren Sie vor dem Provisioning auf jeden Fall die drei Pakete bind9, bind9utils und dnsutils, zusätzlich zu den Samba-Paketen.

**Wichtig**

Wenn Sie zusammen mit dem Bind9 als DNS-Backend auch das LMDB-Datenbankformat nutzen wollen, wird zusätzlich noch das Paket lmdb-utils benötigt.

Nachdem Sie alle benötigten Pakete installiert haben, können Sie jetzt das Provisioning so wie in Listing 4.10 durchführen. Im Beispiel werde ich das Provisionieren direkt mit den Parametern beim Aufruf des Kommandos `samba-tool` durchführen. Achten Sie bei der Angabe des *DNS-Backend* darauf, den Wert *BIND9_DLZ* in Großbuchstaben anzugeben. Zusätzlich wird auch gleich das neue Function Level 2016 eingerichtet:

**Listing 4.10** Provisioning mit bind9

```
root@dc01:~# samba-tool domain provision --domain=example \
        --realm=example.net --host-ip=192.168.56.21 --backend-store=mdb \
        --adminpass=Passw0rd --dns-backend=BIND9_DLZ \
        --option="ad dc functional level = 2016" --function-level=2016

             ...
2417: gkdi/gmsa root key added with guid 39efd12e-f822-3867-1625-
    f17fc42a6397
2428: A Kerberos configuration suitable for Samba AD has been generated at
     \
      /var/lib/samba/private/krb5.conf
2430: Merge the contents of this file with your system krb5.conf or
    replace it \
      with this one. Do not create a symlink!
492: Once the above files are installed, your Samba AD server will be
    ready to use
497: Server Role:           active directory domain controller
498: Hostname:              dc01
499: NetBIOS Domain:        EXAMPLE
500: DNS Domain:            example.net
501: DOMAIN SID:            S-1-5-21-1422239512-53721656-1909266601
~
```

Zwei Zeilen bei dem Provisioning sind interessant für die Einrichtung des Bind9, Listing 4.11 zeigt die beiden Zeilen:

**Listing 4.11** 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 den Bind9 konfigurieren.

Nachdem Sie das Provisioning durchgeführt haben, können Sie jetzt die Datei /etc/bind/named.conf.options anpassen. In Listing 4.12 sehen Sie die geänderten Zeilen und Bereiche:

**Listing 4.12** Einstellungen in der named.conf.options

```
forwarders {
      1.1.1.1;
};
```

```
tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";

dnssec-validation no;
```

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 durchführt, 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. Der Bind9 benötigt noch die Zonendateien, für die er verantwortlich ist. Da Sie hier keine statischen Zonen im üblichen Format einrichten, sondern auf Zonen im Active Directory zugreifen, tragen Sie in der Datei /etc/bind/named.conf.local nur die Zeile aus Listing 4.13 ein:

**Listing 4.13** 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.

Jetzt können Sie den Bind9 mit dem Kommando `systemctl restart named` neu starten. Prüfen Sie anschließend im Journal, ob Sie die Zeilen aus Listing 4.14 sehen:

**Listing 4.14** Erster Test des Bind9

```
root@dc01:~# journalctl -n 200 -u named.service
dc01 named[961]: samba_dlz: started for DN DC=example,DC=net
dc01 named[961]: samba_dlz: starting configure
dc01 named[961]: samba_dlz: configured writeable zone 'example.net'
dc01 named[961]: samba_dlz: configured writeable zone '_msdcs.example.net'
```

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

Im Gegensatz zu den vorherigen Versionen werden bei den Samba-Paketen aus den Backports eigene Pakete für den Domaincontroller installiert. Aus diesem Grund brauchen Sie keine Samba-Dienste zu deaktivieren, und der Domaincontrollerdienst muss auch nicht aktiviert werden. Starten Sie den Domaincontroller mit dem `systemctl restart samba-ad-dc`. Damit ist der Domaincontroller einsatzbereit. Sie können den folgenden Schritt überspringen.

Verwenden Sie die Debian- oder Ubuntu-Standardpakete, sorgen Sie über den `systemd` noch dafür, dass der Domaincontroller auch gestartet wird. Denn als Standardeinstellung ist dort immer der Standalone-Server eingerichtet. In Listing 4.15 sehen Sie die

entsprechenden Kommandos. Prüfen Sie vorab, ob Ihr System noch genau so konfiguriert ist. Bei den Samba-Paketen aus den Debian-Backports brauchen Sie die Dienste nicht mehr zu deaktivieren, denn das System erkennt aufgrund Ihrer Konfiguration, welche Dienste gestartet werden sollen. Bei den SerNet-Paketen passen Sie die Datei /etc/default/sernet-samba so an wie schon beim ersten Domaincontroller beschrieben:

**Listing 4.15** Einstellung des Systemd

```
root@dc01:~# systemctl stop smbd nmbd winbind

root@dc01:~# 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@dc01:~# systemctl unmask samba-ad-dc
Removed /etc/systemd/system/samba-ad-dc.service.

root@dc01:~# systemctl start samba-ad-dc

root@dc01:~# 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
```

Sorgen Sie jetzt noch dafür, dass die eigene IP-Adresse des Domaincontrollers in der Datei /etc/resolv.conf eingetragen ist. Nur dann ist der Domaincontroller in der Lage, die eigenen Einträge und die *SRV-Records* auflösen zu können.

Zum Abschluss kopieren Sie die Datei /var/lib/samba/private/krb5.conf in das Verzeichnis /etc.

### Aktivieren des DCs bei den SerNet-Paketen

Wenn Sie die SerNet-Pakete für Ihren Samba-Server einsetzen, werden die zu startenden Dienste über eine Änderung in der Datei /etc/default/sernet-samba aktiviert. Dort setzen Sie die Variable *SAMBA_START_MODE="dc"*. Das Gute daran ist, egal auf welcher Distribution Sie die SerNet-Pakete installieren, Sie legen den Startmodus immer über diese Datei fest.

## 4.4 Testen des Domaincontrollers

Bevor Sie die folgenden Tests durchführen, sorgen Sie dafür, dass die eigene IP-Adresse des Domaincontrollers als Resolver in der Datei /etc/resolv.conf eingetragen ist.

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. Diese Tests können Sie alle durchführen, egal welchen DNS-Server Sie einsetzen.

### 4.4.1 Testen der Prozesse

Im ersten Test soll sichergestellt werden, dass auch alle Prozesse gestartet wurden. In Listing 4.16 sehen Sie die Tests mit den zu erwartenden Ergebnissen:

**Listing 4.16** Testen der Prozesse

```
root@dc01:~# ps ax | grep samba
    563 ?        Ss     0:00 samba: root process
    568 ?        S      0:00 samba: tfork waiter process(569)
    569 ?        S      0:00 samba: task[s3fs] pre-fork master
    570 ?        S      0:00 samba: tfork waiter process(571)
    571 ?        S      0:00 samba: task[rpc] pre-fork master
    572 ?        S      0:00 samba: tfork waiter process(574)
    573 ?        S      0:00 samba: tfork waiter process(576)
    574 ?        S      0:00 samba: task[nbt] pre-fork master
    575 ?        S      0:00 samba: tfork waiter process(577)
    577 ?        S      0:00 samba: task[wrepl] pre-fork master
    578 ?        S      0:00 samba: tfork waiter process(579)
    579 ?        S      0:00 samba: task[ldap] pre-fork master
    580 ?        S      0:00 samba: tfork waiter process(582)
    581 ?        S      0:00 samba: tfork waiter process(586)
    582 ?        S      0:00 samba: task[cldap] pre-fork master
    583 ?        S      0:00 samba: tfork waiter process(584)
    584 ?        S      0:00 samba: task[kdc] pre-fork master
    585 ?        S      0:00 samba: tfork waiter process(588)
    586 ?        S      0:00 samba: task[rpc] pre-forked worker(0)
    587 ?        S      0:00 samba: tfork waiter process(593)
    588 ?        S      0:00 samba: task[drepl] pre-fork master
    589 ?        S      0:00 samba: tfork waiter process(591)
    590 ?        S      0:00 samba: tfork waiter process(599)
    591 ?        S      0:00 samba: task[winbindd] pre-fork master
```

```
    592 ?        S      0:00 samba: tfork waiter process(595)
    593 ?        S      0:00 samba: task[rpc] pre-forked worker(1)
    594 ?        S      0:00 samba: tfork waiter process(597)
    595 ?        S      0:00 samba: task[ntp_signd] pre-fork master
    596 ?        S      0:00 samba: tfork waiter process(602)
    597 ?        S      0:00 samba: task[rpc] pre-forked worker(2)
    598 ?        S      0:00 samba: tfork waiter process(609)
    599 ?        S      0:00 samba: task[kdc] pre-forked worker(0)
    600 ?        S      0:00 samba: tfork waiter process(603)
    601 ?        S      0:00 samba: tfork waiter process(605)
    602 ?        S      0:00 samba: task[kcc] pre-fork master
    603 ?        S      0:00 samba: task[kdc] pre-forked worker(1)
    604 ?        S      0:00 samba: tfork waiter process(610)
    606 ?        S      0:00 samba: tfork waiter process(607)
    607 ?        S      0:00 samba: task[dnsupdate] pre-fork master
    609 ?        S      0:00 samba: task[rpc] pre-forked worker(3)
    610 ?        S      0:00 samba: task[kdc] pre-forked worker(2)
    611 ?        S      0:00 samba: tfork waiter process(612)
    612 ?        S      0:00 samba: task[kdc] pre-forked worker(3)
    625 ?        S      0:00 samba: tfork waiter process(626)
    626 ?        S      0:00 samba: task[ldap] pre-forked worker(0)
    627 ?        S      0:00 samba: tfork waiter process(628)
    628 ?        S      0:00 samba: task[ldap] pre-forked worker(1)
    629 ?        S      0:00 samba: tfork waiter process(630)
    630 ?        S      0:00 samba: task[ldap] pre-forked worker(2)
    631 ?        S      0:00 samba: tfork waiter process(632)
    632 ?        S      0:00 samba: task[ldap] pre-forked worker(3)
    679 pts/0    S+     0:00 grep samba

root@dc01:~# ps ax | grep named
    551 ?        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 4.17 sehen Sie den Test:

**Listing 4.17** Testen der Ports

```
root@dc01:~# ss -tlpn | awk '{print $1" "$2" "$3" "$4}'
State Recv-Q Send-Q Local
LISTEN 0 10 127.0.0.1:53
LISTEN 0 10 0.0.0.0:636
```

```
LISTEN 0 10 0.0.0.0:3268
LISTEN 0 10 0.0.0.0:3269
LISTEN 0 50 0.0.0.0:139
LISTEN 0 10 0.0.0.0:135
LISTEN 0 10 192.168.56.21:53
LISTEN 0 10 10.0.2.15:53
LISTEN 0 10 0.0.0.0:88
LISTEN 0 10 0.0.0.0:49152
LISTEN 0 10 0.0.0.0:49153
LISTEN 0 10 0.0.0.0:49154
LISTEN 0 128 0.0.0.0:22
LISTEN 0 10 0.0.0.0:464
LISTEN 0 10 0.0.0.0:389
LISTEN 0 50 0.0.0.0:445
LISTEN 0 5 127.0.0.1:953
LISTEN 0 10 [fe80::a00:27ff:fe26:7492]%enp0s8:53
LISTEN 0 10 [::]:636
LISTEN 0 10 [::1]:53
LISTEN 0 10 [::]:3268
LISTEN 0 10 [::]:3269
LISTEN 0 50 [::]:139
LISTEN 0 10 [::]:135
LISTEN 0 10 [::]:88
LISTEN 0 5 [::1]:953
LISTEN 0 10 [::]:49152
LISTEN 0 10 [::]:49153
LISTEN 0 10 [::]:49154
LISTEN 0 128 [::]:22
LISTEN 0 10 [::]:464
LISTEN 0 10 [::]:389
LISTEN 0 50 [::]:445
LISTEN 0 10 [fe80::a00:27ff:fe09:b042]%enp0s3:53
```

**Hinweis**

Da hier nur die Portnummer interessant ist, 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 4.18 sehen Sie verschiedenen Tests:

**Listing 4.18** Die verschiedenen DNS-Tests

```
root@dc01:~# host dc01
dc01.example.net has address 192.168.56.21

root@dc01:~# host -t SRV _ldap._tcp.example.net
_ldap._tcp.example.net has SRV record 0 100 389 dc01.example.net.

root@dc01:~# host -t SRV _kerberos._tcp.example.net
_kerberos._tcp.example.net has SRV record 0 100 88 dc01.example.net.

root@dc01:~# host -t SRV _gc._tcp.example.net
_gc._tcp.example.net has SRV record 0 100 3268 dc01.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 Samba-4-Server testen.

In Listing 4.19 sehen Sie den Test des Verbindungsaufbaus mit dem Kommando `smbclient`:

**Listing 4.19** Ein erster Verbindungsaufbau

```
root@dc01:~# smbclient -L dc01
Password for [EXAMPLE\root]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        sysvol          Disk
        netlogon        Disk
        IPC$            IPC       IPC Service \
        (Samba 4.21.1-Debian-4.21.1+dfsg-2~bpo12+1)

SMB1 disabled -- no workgroup available
```

Hier können Sie sehen, dass SMBv1 deaktiviert wurde; für alle Anfragen mit `smbclient` wird SMBv2 verwendet. Sollte das Kommando `smbclient` auf Ihrem System nicht zur Verfügung stehen, installieren Sie das Paket smbclient. Wenn Sie Samba aus den Backports von Debian verwenden, müssen Sie hier auch die Backports für die Installation des Pakets nutzen.

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 Buchs 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 Buchs 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. Steht Ihnen das Kommando auf Ihrem Domaincontroller nicht zur Verfügung, installieren Sie das Paket heimdal-clients.

Während der Installation des Pakets wird eine Datei /etc/krb5.conf erzeugt. Diese Datei können Sie so aber nicht verwenden. Kopieren Sie die Datei, die beim Provisioning von Samba 4 erstellt wird. Beim Provisioning wird auch angezeigt, wo Sie diese Datei finden.

Im Verzeichnis /var/lib/samba/private/ finden Sie die Datei krb5.conf Ihres Samba-4-Servers. Den Inhalt der Datei sehen Sie in Listing 4.20:

**Listing 4.20** Inhalt der Datei krb5.conf

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

[realms]
EXAMPLE.NET = {
        default_domain = example.net
```

```
}

[domain_realm]
        dc01 = EXAMPLE.NET
```

In Listing 4.21 sehen Sie jetzt das Ergebnis eines Kerberos-Tests:

**Listing 4.21** Testen des Kerberos-Servers

```
root@dc01:~# kinit administrator
administrator@EXAMPLE.NET's Password:
root@dc01:~# klist
Credentials cache: FILE:/tmp/krb5cc_0
        Principal: administrator@EXAMPLE.NET

  Issued                Expires               Principal
Nov 19 20:19:53 2024  Nov 20 06:19:53 2024  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.

**Hinweis**

Sollte auf Ihrem Domaincontroller das Kommando `kinit` nicht verfügbar sein, installieren Sie das Paket heimdal-clients.

In Listing 4.22 sehen Sie ein Beispiel für die Authentifizierung mit Kerberos:

**Listing 4.22** Verbindung mit Kerberos

```
root@dc01:~# smbclient -L dc01 --use-kerberos=required
        Sharename       Type      Comment
        ---------       ----      -------
        sysvol          Disk
        netlogon        Disk
        IPC$            IPC       IPC Service (Samba 4.21.1-Debian-4.21.1+
            dfsg-2~bpo12+1)
SMB1 disabled -- no workgroup available

root@dc01:~# klist
Credentials cache: FILE:/tmp/krb5cc_0
        Principal: administrator@EXAMPLE.NET

  Issued                Expires               Principal
Nov 19 20:19:53 2024  Nov 20 06:19:53 2024  krbtgt/EXAMPLE.NET@EXAMPLE.NET
Nov 19 20:22:54 2024  Nov 20 06:19:53 2024  cifs/dc01@EXAMPLE.NET
```