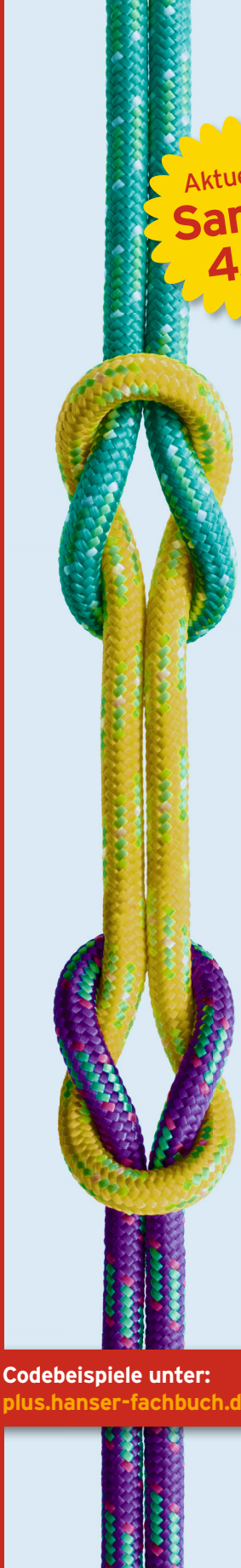

Aktuell zu Samba 4.14

Stefan KANIA

SAMBA 4

Das Handbuch für Administratoren

2. Auflage

Codebeispiele unter:
plus.hanser-fachbuch.de

HANSER

Kania

Samba 4

Ihr Plus – digitale Zusatzinhalte!

Auf unserem Download-Portal finden Sie zu diesem Titel kostenloses Zusatzmaterial.

Geben Sie auf **plus.hanser-fachbuch.de** einfach diesen Code ein:

plus-4sb82-nat45

Bleiben Sie auf dem Laufenden!

Unser **Computerbuch-Newsletter** informiert Sie monatlich über neue Bücher und Termine. Profitieren Sie auch von Gewinnspielen und exklusiven Leseproben. Gleich anmelden unter:

www.hanser-fachbuch.de/newsletter

Stefan Kania

Samba 4

Das Handbuch für Administratoren

2., überarbeitete und erweiterte Auflage

HANSER

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.

Lektorat: Brigitte Bauer-Schiewek
Copy editing: Jürgen Dubau, Freiburg/Elbe
Layout: le-tex publishing services GmbH
Umschlagdesign: Marc Müller-Bremer, www.rebranding.de, München
Umschlagrealisation: Max Kostopoulos
Titelmotiv: © istockphoto.com/malerapaso
Druck und Bindung: Kösel, Krugzell
Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702
Printed in Germany

Print-ISBN: 978-3-446-46977-8
E-Book-ISBN: 978-3-446-46978-5
E-Pub-ISBN: 978-3-446-46979-2

Inhalt

Vorwort

Eine neue Auflage des Samba-4-Buchs ist fertig. Nachdem seit dem Beginn der Arbeiten zur vorherigen Auflage mehr als zwei Jahre vergangen sind, wurde es Zeit, die Inhalte zu überarbeiten. Sehr viel hat sich seit der damals verwendeten Samba-Version 4.8 geändert. Vieles ist komplett überarbeitet worden wie die Konfiguration von CTDB. Viel wichtiger hingegen, es sind auch eine Menge an neuen Funktionen und Möglichkeiten in der Zeit dazugekommen. Eine der aktuellsten und in meinen Augen größten Neuerungen sind die Gruppenrichtlinien für Linux-Clients. Damit ist es jetzt auch möglich, über das Active Directory Teile der Linux-Client-Konfiguration zentral über Gruppenrichtlinien zu steuern. Auch ist im Hintergrund, also in dem Teil, der keine neuen Funktionen bietet, viel getan worden. So wurde der gesamte SMB-Stack überarbeitet und zusammen mit den verbesserten Funktionen des Kernels ab 5.4 die Performance verbessert. Eine der wohl größten Änderungen ist die Umgestaltung des VFS-Systems. Das Datenbank-Backend *lmdb* hat Einzug gehalten, damit können jetzt die Datenbanken erheblich größer werden und somit mehr Objekte im Active Directory verwaltet werden.

Alle Dinge aufzuzählen, die sich im Hintergrund getan haben, würde die Liste zu lang werden lassen.

Auch für Sie als Administrator hat sich seit der Version 4.8 sehr viel getan. Hier im Buch verwende ich die Version 4.14, die beim Erscheinen des Buchs die gerade aktuelle Version ist. Wenn Sie jetzt erst von 4.8 umsteigen und den Wechsel auf 4.14 vollziehen, werden Sie am Anfang gleich sehen, was sich alles getan hat. Rufen Sie nur einmal das Kommando `samba-tool` auf und vergleichen Sie die Möglichkeiten mit älteren Versionen, da ist jetzt schon so einiges mehr möglich. Natürlich habe ich alle wichtigen Neuerungen auch ins Buch aufgenommen, sodass Sie schnell auf dem aktuellen Stand sind und die neuen Möglichkeiten kennenlernen.

Ich hoffe, dass ich Ihnen mit diesem Buch wieder eine Anleitung an die Hand gegeben habe, die Sie von vorne bis hinten der Reihe nach abarbeiten können, aber Sie können auch gezielt einzelne Kapitel nutzen.

Ich weiß, viele Leser suchen als Erstes immer, was denn bei einem Buch im Vergleich zur letzten Auflage rausgefallen und was neu dazugekommen ist. Rausgefallen ist das Compilieren von Samba. Es gibt mittlerweile so viele Möglichkeiten, aktuelle Versionen als Pakete zu bekommen, dass das Selberbauen, um aktuelle Versionen zu bekommen, nicht mehr unbedingt notwendig ist. Durch die Umstellung auf Python3 und andere technische Änderungen ist das Bauen auch etwas komplexer geworden. Das alles hat mich zu dem Entschluss gebracht, diesen Teil zugunsten anderer Themen aus dem Buch zu nehmen.

Genau so wichtig ist auch immer, was ist denn neu im Buch? Ja, Neues gibt es. Das Kapitel zum Thema Freigaben habe ich erheblich erweitert. Ich habe hier jetzt eine komplette Beschreibung zur Einrichtung von servergespeicherten Profilen und der Ordnerumleitung über Gruppenrichtlinien geschrieben. Denn das ist eines der Themen, die auch meinen Kunden immer wieder Schwierigkeiten bereiten. Natürlich das gesamte Thema Gruppenrichtlinien für Linux-Clients ist komplett neu. Bei der Client-Verwaltung habe ich mich mal an die Einbindung von macOS-Clients gewagt.

Beim Thema Cluster habe ich den Teil mit GlusterFS etwas aufgebohrt, denn dazu kamen in der letzten Zeit vermehrt Fragen und die Bitte, das Thema doch mal etwas umfangreicher zu gestalten.

Beim Kapitel zur Fehlersuche sind das Logging und das Auditing dazugekommen.

Zwei neue Kapitel gibt es dieses Mal im Buch: einmal ein eigenes Kapitel zur Einrichtung des VFS-Moduls *virusfilter* zusammen mit *ClamAV* als Scan-Engine und das Thema Ansible. Da zeige ich, wie Sie eine komplette Umgebung mit zwei Domaincontrollern und einem Fileserver automatisch mit Ansible einrichten können. Die Rollen stelle ich alle als Download bereit.

Und die anderen Kapitel? Fast alle Kapitel habe ich komplett überarbeitet und auf die aktuelle Samba-Version 4.14 angepasst. Zu vielen Kapiteln sind auch neue Funktionen hinzugekommen. Alles in allem sind gut 100 Seiten neu hinzugekommen, und ich hoffe, dass auch für alle Leser etwas Neues dabei ist.

Danksagung

Bei den Danksagungen möchte ich dieses Mal mit Ihnen beginnen, denn was wäre ein Buch ohne die Leser? Ganz klar, nicht da. Deshalb danke an alle Leser, an die, für die dieses die erste Auflage ist, aber besonders an die Leser, die schon mehrere Auflagen dieses Buches besitzen.

Danke auch an den Hanser Verlag, dass ich das Buch, bei dem es sich ja schon um ein Nischenprodukt handelt, wieder neu auflegen durfte.

Mein besonderer Dank gilt drei Personen, ohne die es nicht möglich gewesen wäre, die Auflage so schnell herauszubringen und dabei die gerade aktuelle Samba-Version zu nutzen. Danke, Louis van Belle, für die Bereitstellung der Pakete zu 4.14 ab dem ersten Tag des Erscheinens des rc1-Release.

Auch Björn Baumbach von der Firma SerNet hat mir wieder sehr viel geholfen -- beim Auffinden von Bugs und anderen Fragen. Manchmal hatte ich schon Angst, bei ihm auf die Blacklist seines Mailprogramms zu kommen. Auch er hat dafür gesorgt, dass ich die SerNet-Pakete zu 4.14 schon mit dem rc1-Release nutzen konnte.

Danken möchte ich auch Ralph Böhme von der Firma SerNet, der mir bei der Erstellung des Abschnitts zu macOS-Clients geholfen und den Teil des Kapitels auch gegengelesen hat, um mir als Nicht-Mac-User das eine oder andere zu erklären.

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

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

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 kursiv geschrieben, zum Beispiel so: *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. Zurzeit unterstützen nur Ubuntu und Debian die Funktion des Active Directory-Domaincontrollers aus den eigenen Repositories. Der Grund ist der, dass bis zur Version 4.6 nur der Heimdal-Kerberos Server bei Samba zum Einsatz gekommen ist. Nur Debian und Ubuntu stellen den Heimdal-Server noch zur Verfügung, alle anderen Distributionen verwenden nur noch den MIT-Kerberos, um die aktuellen Versionen nutzen zu können. Die Nutzung des MIT-Kerberos ist immer noch experimentell und kann nur verwendet werden, wenn Sie Samba entsprechend selber bauen.

Eine weitere Möglichkeit für die Installation auf Debian-Systemen sind die Pakete von Louis van Belle *https://apt.van-belle.nl/*. Ich werde diese Pakete hier im Buch einsetzen, um die aktuelle Samba-Version vorstellen zu können.

Die wichtigsten Unterscheidungsmerkmale finden sich hauptsächlich in der Installation. Die Administration ist anschließend 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 System immer deaktivieren, da es in diesem Buch nicht um das Thema Systemsicherheit 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.
- 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.

Einige der hier im Buch beschriebenen Distributionen bringen nicht die Funktion des Domaincontrollers mit, da der Domaincontroller den Heimdal-Kerberos-Server benötigt und nicht alle Distributionen diesen unterstützen. An der entsprechenden Stelle werde ich auf diese Thematik noch genauer eingehen.

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. Aber sehr oft kommt das Protokoll doch noch zum Einsatz, um zum Beispiel die Netzwerkumgebung im Explorer unter Windows weiterverwenden zu können.

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 Seite von Microsoft als auch auf Seite 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.

2.1.1 Was hat sich bei Samba getan?

Im letzten Buch habe ich die damals aktuelle Version 4.8 genutzt. Wie schon in der Einleitung beschrieben, verwende ich dieses Mal die Version 4.14. Da sich in den Versionen von 4.8 bis 4.14 eine Menge geändert hat, folgt hier eine kurze Übersicht über alle Änderungen zum SMB-Protokoll.

Version 4.10

Erstmal unterstützen in dieser Version die smbtools wie `smbclient` SMBv2. In den vorherigen Versionen funktionierten die *smbtools* nicht, wenn auf einem Server oder Domain-

controller SMBv1 deaktiviert wurde. Die Kommandos lieferten dann nur eine Fehlermeldung. Auch das wichtige Werkzeug `samba-tool` auf den Domaincontrollern unterstützt jetzt SMBv2.

Version 4.11

Hier wird es dann ernst, ab dieser Version wurde SMBv1 grundsätzlich deaktiviert. Wer ab der Samba-Version 4.11 noch SMBv1 benötigt, kann das nur, wenn es explizit in der smb.conf aktiviert wird. Bei den beiden Parametern *client min protocol* und *server min protocol* ist der Standardwert jetzt *SMB2_02*.

Das bedeutet, dass Clients, die nicht mindestens SMBv2 unterstützen, keine Verbindung mehr zu einem Samba-Server aufbauen können.

Version 4.12

Einige Interna des SMBv3-Protokolls wurden verbessert, zusammen mit einem Kernel >= 5.1 (am besten ab Kernel 5.6.16) wurde die Performance erheblich verbessert.

Version 4.13

Die Möglichkeit, SMBv1 zu nutzen, wurde weiter eingeschränkt. Alle Parameter, die sich lediglich auf Sicherheitsmechanismen beziehen, die lediglich von SMBv1 unterstützt werden, wurden als *deprecated* markiert und werden in den nächsten Versionen vollständig entfernt. Die folgenden Parameter fallen darunter:

- raw NTLMv2 auth
- client plaintext auth
- client NTLMv2 auth
- client lanman auth
- client use spnego

2.2 Das Protokoll NetBIOS

NetBIOS ist dagegen 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.

Soll kein NetBIOS mehr zum Einsatz kommen, wird die Verwaltung der Dienste und Rechner in einem Windows-Netzwerk vom Active Directory übernommen, und die Netzwerkumgebung bleibt leer.

Viele Administratoren lassen deshalb NetBIOS aktiv, da sich die Anwender an die Netzwerkumgebung gewöhnt haben und sich nur schwer umstellen können oder wollen.

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 von Louis van Belle zurückgreifen, um dort möglichst die aktuellen Funktionen erklären zu können. Auf den Clients werde ich immer die Pakete der Distributionen 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.

3.1 Unterschiede zwischen den verschiedenen Samba-4-Versionen

Mittlerweile sind die Pakete in den Distributionen relativ aktuell, es hängt immer davon ab, welche Distribution Sie einsetzen.

Durch den vom Samba-Team auf sechs Monate verkürzten Release-Zyklus der Versionen können die Distributionen nicht immer die aktuellste Version bereitstellen. Da der Funktionsumfang von Version zu Version steigt, müssen Sie im Vorfeld genau überlegen, welche Funktion von Samba 4 Sie benötigen, und dann die richtige Version auswählen.

An dieser Stelle möchte ich Ihnen die Änderungen in den Samba-Versionen seit der letzten Auflage aufzählen. Es ist so, dass das Samba-Team immer die letzten drei Versionen direkt mit Updates und Patches versorgt, beim Einsatz von älteren Versionen sind sie immer auf die Herausgeber der Distribution angewiesen, wenn es um Updates geht. Beim Erscheinen dieser Auflage werden die Versionen 4.14, 4.13 und 4.12 vom Samba-Team direkt unterstützt. Da ich in der letzten Auflage aber die Version 4.8 genutzt habe, möchte ich hier auch die Änderung aller Versionen seit 4.9 kurz ansprechen. So können Sie auch sehen, wie die Entwicklung von Samba voran geht.

Version 4.9

Mit der Version 4.9 wurden viele Bereiche und Funktionen überarbeitet. Hier eine Übersicht über die neuen Funktionen:

- Erweitertes Auditing
  In vielen Bereichen ist die Datenbank um die Möglichkeit des Auditings erweitert worden. So können Sie jetzt die Datenbank überwachen, um Änderungen an Objekten und und vor allen Dingen an Passwörtern zu kontrollieren.
- Unterstützung der `Password Settings Objects (PSOs)`
  Mit den PSOs können Sie für einzelne Benutzer oder Gruppen die Passwortrichtlinien der Domäne übersteuern und so für bestimmte Benutzergruppen stärkere oder schwächere Passwortregeln festlegen. Die PSOs setzen Sie mit dem neuen Kommando `samba-tool domain passwordsettings pso`.
- Domain Backup und Restore (online)
  Jetzt können Sie Ihre Active Directory-Datenbank direkt mit dem `samba-tool` im laufenden Betrieb sichern und im Falle eines Komplettausfalls der Domäne wiederherstellen, Sie benötigen für diese Aufgaben kein eigenes Skript mehr. Das Kommando `samba-tool` wurde dafür um die beiden Kommandos `samba-tool domain backup online` und `samba-tool domain backup restore` erweitert.
- Verwalten von OUs mithilfe von *samba-tool*
  Ein komplett neues Sub-Kommando für die Verwaltung von OUs wurde entwickelt. So können Sie jetzt auch auf der Kommandozeile OUs anlegen, löschen und umbenennen.
- DNS-Einträge werden bereinigt
  Wenn Sie einen Domaincontroller aus der Domäne mit der Option *demote* entfernen, werden jetzt auch alle DNS-Einträge für den Domaincontroller entfernt.
- Die Funktionen der Vertrauensstellungen wurde verbessert
  Endlich ist es möglich, Gruppen und Benutzer aus der vertrauten Domäne zu einer Gruppe hinzuzufügen. Sie können jetzt den SID einer Gruppe oder eines Benutzers zu einer lokalen Gruppe hinzufügen. Dabei wird auch automatisch der benötigte *Foreign Security Principal (FSP)* angelegt. Dieser Principal wird benötigt, um einem Objekt aus einer vertrauten Domäne Rechte geben und es in eine Gruppe der eigenen Domäne aufnehmen zu können.
- Änderungen an CTDB
  CTDB wurde fast komplett überarbeitet. Die Konfigurationsdatei entspricht jetzt der smb.conf. Die Event-Skripte wurden verändert und werden jetzt effektiver verwaltet. Im CTDB wurden wohl die meisten Änderungen durchgeführt.
- Domain backup and restore
  Mit der Version wurde eine neue Möglichkeit bereitgestellt, mit der Sie die Datenbank Ihres Active Directory sichern und wiederherstellen können. In dieser Version war es aber nur möglich, das Backup auf einem laufenden Domaincontroller durchzuführen, daher der Name *online-backup*.
- DRS mit summary
  Wenn Sie die Replikation aller Ihrer Domaincontroller testen wollen, wurde Ihnen beim Kommando `samba-tool drs showrepl` immer jede einzelne Replikationsart zwischen allen Domaincontrollern aufgelistet. Je mehr Domaincontroller Sie im Einsatz

haben, desto länger wurde die Liste. So konnte es passieren, dass Sie eventuelle Fehler zwischen allen Meldungen übersehen haben. Mit der Version 4.9 wurde die Option *--summary* aufgenommen. Wenn Sie jetzt ein `samba-tool drs showrepl --summary` ausführen und alle Replikationen funktionieren ordnungsgemäß, erhalten Sie lediglich die Meldung *ALL GOOD*. Sollte es zu Fehlern kommen, werden auch nur die Fehler angezeigt.

- Samba-tool computer
  Mit der neuen Option *computer* des `samba-tool` können Sie Computer-Konten in der Domäne ändern und anlegen. Wenn Sie ein Computer-Konto anlegen, wird beim *join* des Clients nicht mehr das Konto des Domainadministrators benötigt, es reicht ein lokales Admin-Konto.
- Samba-tool group
  Jetzt sind Sie in der Lage, sich mit dem Kommando `samba-tool group stats` eine Statistik anzeigen zu lassen, wie sich Ihre Benutzer über alle Gruppen verteilen. Auch wurde die *verbose*-Option um die Anzeige der Anzahl der Gruppenmitglieder erweitert.
- Python3-Unterstützung
  Das ist die erste Version mit Python3-Unterstützung und gleichzeitig die letzte Version mit Python2-Unterstützung.
- SMBv2 samba-tool support
  Bis zur vorherigen Version war es nicht möglich, `samba-tool` gegen einen Domaincontroller ohne SMBv1 zu nutzen. Jetzt wird auch beim `samba-tool` kein SMBv1 mehr benötigt.
- glusterfs_fuse VFS module
  Das neue VFS-Modul bringt einen erheblichen Performance-Gewinn beim Einsatz von *GlusterFS* als Storage.
- Das neue experimentelle LMDB(LDB)-backend wird bereitgestellt
  Mit dem neuen Datenbank-Backend wird es Schritt für Schritt möglich werden, die Datenbanken für die Objekte größer werden zu lassen. Das bedeutet, dass Sie in Zukunft mehr Objekte in der Datenbank ablegen können.

Version 4.10

Auch in der Version 4.10 wurden verschiedenste Änderungen und Neuerungen eingeführt, die Sie direkt bei der Administration Ihrer Domäne unterstützen können. Neben den bei der Administration sichtbaren Änderungen wurden auch hier wieder viele Änderungen durchgeführt, die die Stabilität und Sicherheit von Samba verbessern.

- Save and recover GPOs
  Mithilfe des `samba-tool` können Sie jetzt alle eingerichteten GPOs sichern und wiederherstellen. Das ist besonders wichtig, wenn Sie auch die Datenbanken des Samba-Servers mit dem `samba-tool` gesichert haben. Dann können Sie mit dem Backup der GPOs und dem Backup der Datenbanken im schlimmsten Fall, dem Totalausfall Ihrer Domäne, Ihre Domäne komplett wiederherstellen.
- Domain Backup und Restore (offline)
  Jetzt ist es auch möglich, eine Domäne mit allen Datenbanken zu sichern, wenn ein Domaincontroller offline ist. Der Vorteil des Offline-Backups gegenüber dem Online-

Backup ist der, dass es schneller ist und zusätzliche Informationen gespeichert werden, die eventuell für forensische Zwecke genutzt werden können.

Version 4.11

Mit der Version 4.11 nähert sich das Ende von SMBv1 immer mehr. Spätestens mit dieser Version ist es sinnvoll, alle alten Clients zu aktualisieren. Wenn Sie einen Domaincontroller auf 4.11 aktualisiert haben, dürfen Sie auf keinen Fall mehr eine ältere Samba-Version einspielen, da sich das Datenbankformat geändert hat. Beim Downgrade auf eine ältere Version kann es zur Zerstörung der Datenbank kommen und damit zum Verlust aller Daten.

- SMBv1 wurde disabled
  In der Standardkonfiguration ist SMBv1 jetzt disabled. Es kann zwar noch wieder aktiviert werden, birgt aber jede Menge Sicherheitsrisiken. Die Kommandozeilenwerkzeuge nutzen alle nur noch SMBv2. Nur mit der Option *--option='client min protocol=NT1'* können Sie diese /Werkzeuge noch mit SMBv1 nutzen.
- Bind9 mit FLATFILE ist deprecated
  Sollten Sie noch den Bind9 zusammen mit Zonendateien im ASCII-Format einsetzen, ist spätestens jetzt eine Umstellung auf DLZ (Directory Loaded Zone) nötig.
- Standard Schema ist jetzt 2012_R2
  Das AD-Schema ist jetzt 2012_R2, aber leider ist es immer noch nicht möglich, das *function level* auf 2012_R2 zu setzen. Hier sind Sie immer noch auf das alte 2008_R2-Level angewiesen. Zurzeit ist da auch keine Änderung in Sicht. Es fehlen Entwickler, Zeit und die Finanzierung.
- GnuTLS 3.2 notwendig
  Wollen Sie Samba aus den Quellen selber bauen, benötigen Sie ab Version 4.11 GnuTLS in der Version 3.2, unabhängig welche Funktion Sie mit Samba realisieren wollen.
- Weitreichende Änderung am LMDB-Backend
  Jetzt kann das Datenbank-Backend *LMDB* produktiv genutzt werden. Beim Anlegen der Datenbank kann die Größe mit angegeben werden. Der Standardwert ist 8 GB. Damit ist es möglich, erheblich mehr Objekte in der Datenbank zu speichern. Weithin wurden verschiedene Änderungen vorgenommen, die die Performance des Backends erheblich verbessern. Ich werde bei der Installation der Systeme auf jeden Fall auch die praktischen Aspekte des neuen Backends betrachten.
- Keine Python2-Unterstützung mehr
  In dieser Version wurde die Python2-Unterstützung komplett entfernt, nur noch Python3 wird unterstützt, mindestens in der Version 3.4.

Version 4.12

Bei der Version ist mindestens GnuTLS 3.4.7 und Python 3.5 nötig. Folgende Änderungen wurden vorgenommen.

- Die zlib-Library ist notwendig
  In den vorherigen Versionen war die *zlib*-Library in den Quellen enthalten, das ist jetzt nicht mehr der Fall. Wollen Sie Samba aus den Quellen bauen, benötigen Sie die Development-Pakete der Library auf dem System.

- Neue Funktionen und Filter im samba-tool
  Neue Funktionen wie das Hinzufügen von Kontakten zu Gruppen sind jetzt möglich. Bei der Auflistung von Benutzern und Gruppen können Sie jetzt über Filter festlegen, ab welcher OU gesucht werden soll. Das grenzt das Suchergebnis ein und macht dadurch das Ergebnis übersichtlicher.
- Neue Funktionen für MAC-Clients
  Das Spotlight-Backend für MAC unterstützt jetzt auch *elasticsearch*.

Version 4.13

Jetzt wird mindestens Python 3.6 benötigt für Samba. Das ist die erste Version, in der die NT-Style Domänen als *deprecated* gekennzeichnet sind. Wenn Sie noch NT-Style-Domänen betreiben, wird es jetzt Zeit, auf Active Directory umzustellen. Der SMB-Protokollstack wurde überarbeitet. Zusammen mit einem aktuellen Kernel in der Version > 5.3 verbessert sich die Performance von Samba. Was ist sonst noch neu?

- Wide links Funktionalität
  Wenn Sie in Ihrer Konfiguration noch *wide links = yes* nutzen, müssen Sie mit dieser Version auf das neue VFS-Modul *vfs_widelinks* umstellen, denn die Funktion wurde in das VFS-Modul ausgelagert. Die Funktion der *wide links* über das VFS-Modul ist erheblich sicherer als das alte Vorgehen.

Version 4.14

Das ist die (auch beim Erscheinen des Buchs) aktuellste Version von Samba. Gerade im Bereich `samba-tool` hat sich eine Menge getan. Viele neue Funktionen können jetzt auf der Kommandozeile durchgeführt werden, ohne unbedingt ein grafisches Werkzeug nutzen zu müssen.

- Verteilen von Druckertreibern wurde verbessert
  Die Verteilung von Druckertreibern ist stabiler geworden. Es werden jetzt auch ARM64-Treiber unterstützt, aber leider immer noch keine Treiber vom Typ 4; Sie sind hier weiterhin auf Treiber vom Typ 3 angewiesen.
- Erweiterte Client Group Policy
  Bei `winbind`-Clients können Sie jetzt erstmals GPOs einsetzen, und zwar für die folgenden Funktionen:
  - Verteilen von Sudoers-Konfigurationen
  - cron jobs für hourly, daily, weekly oder monthly Jobs
  - Anpassung einiger Parameter in der smb.conf
  - Passwort- und Kerberos-Policies (nur Domaincontroller)
  - Message-Policies

  Ich werde auf die Funktion in Kapitel 6, »Gruppenrichtlinie«, näher eingehen.

Wenn Sie sich einen vollständigen Überblick über alle Änderungen in den verschiedenen Versionen machen wollen, empfehle ich Ihnen einen Blick auf die Seite *https://www.samba.org/samba/history/*.

Nachdem Sie jetzt eine Übersicht über die unterschiedlichen Funktionen der einzelnen Versionen haben, 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. Erst ab der Version 4.7 ist eine Umstellung möglich. Aber der vollständige Funktionsumfang ist noch nicht gegeben. Damit fallen die Pakete der Distributionen aus der Auswahl, die nur den MIT-Kerberos bereitstellen. Dazu gehören *Fedora*, *Red Hat*, *Suse* und *CentOS*. Wollen Sie eine dieser Distributionen verwenden, können 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.

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.

3.2 Die verschiedenen Installationsarten

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

3.2.1 Installation eines Domaincontrollers aus den Distributionspaketen

Bei Debian 10 wird die Version 4.9 verwendet. Bei der nächsten Version Debian 11 steht dann schon Samba 4.13 zur Verfügung. Bei Ubuntu ist momentan die Version 20.04 als LTS Version verfügbar, dort wird die Samba-Version 4.11 eingesetzt.

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. 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.

3.2.2 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.

3.2.3 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.

3.2.4 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 ist die Migration auf eine höhere Samba-Version 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.

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.

3.2.5 Installation der Pakete von Louis van Belle

Wie ich schon in der Einleitung angesprochen habe, gibt es für Debian Pakete von Louis van Belle, er stellt eigene Repositories zur Verfügung und auch immer die aktuellsten Pakete. Auf seiner Website *https://apt.van-belle.nl/* finden Sie die Repositories für Debian und Ubuntu. Diese Pakete unterstützen den Domaincontroller und alle Clients.

Vor- und Nachteile der Pakete von Louis van Belle

Sie bekommen immer die aktuellsten Pakete und können durch die Einbindung seiner Repositories die Aktualisierung zusammen mit einem Systemupdate durchführen. Nachteilig ist nur, dass es nur einen Maintainer gibt, der sich um die Pakete kümmert. Sollte er die Unterstützung einstellen, müssten Sie sich eine andere Quelle für Ihre Samba-Pakete suchen.

3.3 Installationen unter den verschiedenen Distributionen

Dieser Teil wird hier erblich kürzer als noch in der letzten Auflage, da ich nicht mehr auf das Selberbauen von Samba eingehe.

In diesem Abschnitt können Sie die verschiedenen Arten der Installation, bezogen auf Ihre bevorzugte Distribution, nachlesen. Ich werde hier alle Möglichkeiten der Installation ansprechen, sodass Sie für die gewünschte Distribution den von Ihnen gewünschten Weg gehen können.

Da bei *Red Hat*, *CentOS* und *Suse* die Installation eines Domaincontrollers aus den Paketen der Distribution nicht möglich ist, werde ich keine der Distributionen bei der Einrichtung des Domaincontrollers nutzen und erklären.

Hinweis

Wenn Sie im nächsten Abschnitt mehrere Installationsarten ausprobieren wollen, achten Sie darauf, dass Sie Samba immer nur auf eine Art auf Ihrem System installiert haben. Wenn Sie Samba aus verschiedenen Quellen auf demselben System installieren, führt das zu Konflikten, und es kann Ihnen passieren, dass Samba gar nicht mehr startet.

3.3.1 Debian 10

Beim Einsatz von Debian hier im Buch werde ich immer Debian 10 nutzen. Wenn nach Erscheinen des Buchs die nächste Version von Debian bereits verfügbar seien sollte, können Sie auch die neue Version einsetzen.

Kernel aktualisieren

Bevor Sie mit der Installation der Pakete auf einem Debian 10 beginnen, kann ich Ihnen nur raten, dass Sie Ihr System auf einen Kernel >=5.4 bringen. Denn nur dann können Sie alle aktuellen Möglichkeiten des SMB-Protokolls voll nutzen. Einen passenden Kernel können Sie recht einfach über die *Backports* installieren. In Listing 3.1 sehen Sie die einzelnen Schritte. Zum Zeitpunkt des Erscheinens dieses Buchs kann es sein, dass Sie dort schon eine aktuellere Version vorfinden. Wichtig ist nur, dass die Kernel-Version >=5.4 ist:

Listing 3.1 Installation des Kernels aus den Backports

```
root@sambabuch:~# uname -r
4.19.0-13-amd64

root@sambabuch:~#vi /etc/apt/sources.list
## Am Ende der Datei eintragen:
#buster backports
deb http://http.debian.net/debian buster-backports main

root@sambabuch:~# apt update

root@sambabuch:~# apt -t buster-backports upgrade

root@sambabuch:~# reboot

root@sambabuch:~# uname -r
5.9.0-0.bpo.5-amd64
```

Sollte nach dem `reboot` noch kein neuer Kernel auf dem System installiert sein, können Sie den Kernel jetzt nachinstallieren. In Listing 3.2 sehen sie die Vorgehensweise:

Listing 3.2 Kernel nachträglich installieren

```
root@sambabuch:~# apt-cache search linux-image
linux-image-5.9.0-0.bpo.5-amd64
```

```
root@sambabuch:~# apt-cache search linux-headers
linux-headers-5.9.0-0.bpo.5-amd64

root@sambabuch:~# apt install linux-image-5.9.0-0.bpo.5-amd64 \
                  linux-headers-5.9.0-0.bpo.5-amd64\
                  -t buster-backports

root@sambabuch:~# reboot
```

Nach dem Neustart des Systems werden Sie bei `uname -r` den aktuellen Kernel angezeigt bekommen.

Bei Debian 10 kann über das Repository die Version 4.9.x installiert werden. Mit den Paketen wird sowohl der Domaincontroller als auch der Fileserver installiert. Nur wenn Sie später einen CTDB-Cluster installieren wollen, geht das nicht mit den eigentlichen Samba-Paketen, dann benötigen Sie noch die eigenständigen CTDB-Pakete.

Installation über die Pakete

Wie bei Debian üblich, werden die Pakete hier über die Kommandozeile mittels `apt-get` installiert. Listing 3.3 zeigt die Installation für einen ADDC:

Listing 3.3 Installation unter Debian 10

```
root@sambabuch:~# apt-get install samba libpam-heimdal heimdal-clients \
                  ldb-tools winbind libpam-winbind smbclient libnss-
                      winbind \
                  bind9 bind9utils dnsutils
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut.
Statusinformationen werden eingelesen.... Fertig
.
.
.
Möchten Sie fortfahren? [J/n]
```

Die Pakete *bind9* und *bin9utils* 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.

Wenn Sie einen Fileserver oder einen Client einrichten wollen, benötigen Sie die identischen Pakete mit Ausnahme der Bind9-Pakete.

Hinweis

Während der Installation der Pakete werden Sie nach drei verschiedenen Parametern für die Kerberos-Client-Konfiguration gefragt. An dieser Stelle können Sie die Eingabe einfach mit Return bestätigen. Diese Eingaben würde die Datei /etc/krb5.conf erstellen. Diese Datei wird aber beim Einrichten der Domäne erzeugt und dann an die entsprechende Stelle kopiert.

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.

Bei Debian ist der Systemd so konfiguriert, dass Samba immer als Member- oder Standalone-Server gestartet wird. Wenn Sie einen Domaincontroller einrichten wollen, ist es notwendig, dass Sie die Dienste über den Systemd umstellen.

3.3.2 Ubuntu 20.04

Bei Ubuntu können Sie sowohl die Funktion des Domaincontrollers als auch die des Domainmembers realisieren. Dazu werden keine zusätzlichen Paketquellen benötigt, Sie können die Pakete direkt installieren.

Installation über die Pakete

Die Pakete können Sie am einfachsten und schnellsten über die Kommandozeile installieren. Listing 3.4 zeigt die nötigen Schritte:

Listing 3.4 Installation von Samba unter Ubuntu 20.04

```
root@sambabuch:~# root@sambabuch:~# apt-get install samba libpam-heimdal
    heimdal-clients \
                ldb-tools winbind libpam-winbind smbclient libnss-
                    winbind \
                bind9 bind9utils dnsutils
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut.
Statusinformationen werden eingelesen.... Fertig
.
.
.
Möchten Sie fortfahren? [J/n]
```

Hinweis

Bei der Installation der Pakete werden auch Kerberos-Pakete mit installiert. Während der Installation kommt die Frage nach dem Passwort für Kerberos. Diese Abfrage können Sie übergehen, da später beim Einrichten des Domaincontrollers der Kerberos-Server konfiguriert wird.

Die Konfigurationsdatei smb.conf befindet sich später im Verzeichnis /etc/samba. Die Datenbanken und die sysvol-Freigabe befinden sich im Verzeichnis /var/lib/samba. Auch bei Ubuntu sorgt der Systemd dafür, dass der Samba-Dienst als Member- oder Standalone-Server gestartet wird. Genau wie bei Debian wird später der Systemd umgestellt, damit der Samba-Server als Domaincontroller fungieren kann.

3.3.3 CentOS 7

Bei CentOS gibt es derzeit einen Umbruch. Es gibt zwar eine Version 8, aber das Ende des Supports wurde auf Ende 2021 festgelegt, und somit ist CentOS 8 keine Alternative mehr. Da CentOS 7 noch bis Mitte 2024 mit Updates versorgt wird, werde ich an dieser Stelle die Version CentOS 7 beibehalten. Da Sie hier eh nur den Client oder Fileserver von Samba nutzen können, spielt die Version hier nicht so eine große Rolle. Nur sollten Sie überlegen, ob Sie weiterhin CentOS 7 einsetzen wollen. Bei CentOS ist es wichtig, dass Sie sich auch immer Gedanken über die auf dem System laufende Firewall machen und zusätzlich eventuell die Einstellungen für `SELinux` anpassen. Hier im Buch gehe ich davon aus, dass sowohl die lokale Firewall als auch `SELinux` deaktiviert sind.

Installation aus den Paketen

Die Samba-Pakete lassen sich hier auch am einfachsten über die Kommandozeile installieren. Dazu wird unter CentOS `yum` verwendet. Listing 3.5 zeigt die einzelnen Schritte:

Listing 3.5 Installation der Samba-Pakete unter CentOS

```
[root@sambabuch ~]# yum install samba-dc.x86_64 samba-winbind.x86_64
.
Installiert:
  samba-dc.x86_64 0:4.7.1-6.el7
Komplett!
```

Hier sehen Sie, dass ich ein Paket installiert habe, das `samba-dc` heißt. Kann CentOS also doch als Domaincontroller installiert werden? Nein! Das Paket installiert zwar alle für den Domainmember benötigten Pakete, aber anstelle der ADDC-Pakete wird nur eine Textdatei installiert, die darauf hinweist, dass Samba unter Fedora keinen Domaincontroller unterstützt, weil nicht der MIT-Kerberos verwendet wird. Diese Meldung kommt, obwohl in 4.7 die Verwendung des MIT-Kerberos möglich wäre. Da der MIT-Kerberos aber noch nicht vollständig unterstützt wird, bleibt es dabei, dass der Domaincontroller und CentOS nicht genutzt werden kann.

Im Gegensatz zu Debian und Ubuntu werden die Dienste nicht sofort gestartet, das zeigt auch die Abfrage des Systemd in Listing 3.6:

Listing 3.6 Abfrage des Systemstatus

```
[root@sambabuch ~]# systemctl list-unit-files | egrep 'smb|nmb|winbind'
nmb.service                                 disabled
smb.service                                 disabled
winbind.service                             disabled
```

Wollen Sie die Dienste direkt aus den Paketen nutzen, aktivieren Sie sie erst. Listing 3.7 zeigt diesen Vorgang:

Listing 3.7 Aktivieren der Samba-Dienste unter CentOS

```
[root@sambabuch system]# systemctl enable smb
ln -s '/usr/lib/systemd/system/smb.service' \
  '/etc/systemd/system/multi-user.target.wants/smb.service'

[root@sambabuch system]# systemctl enable nmb
ln -s '/usr/lib/systemd/system/nmb.service' \
  '/etc/systemd/system/multi-user.target.wants/nmb.service'

[root@sambabuch system]# systemctl enable winbind
ln -s '/usr/lib/systemd/system/winbind.service' \
  '/etc/systemd/system/multi-user.target.wants/winbind.service'
```

Anschließend können Sie die Dienste konfigurieren und starten. Jetzt können Sie CentOS als Domainmember nutzen.

3.3.4 Suse Leap 15.x

Auch Suse nutzt nur noch den MIT-Kerberos-Server für seine Pakete, somit kann auch mit den Samba-Paketen von Suse kein Domaincontroller eingerichtet werden.

Installation aus den Paketen

Die Pakete, die Suse von Samba 4 bereitstellt, können Sie auf zwei verschiedene Arten installieren: einmal über den Yast oder über die Kommandozeile mit `zypper`. Hier im Buch werde ich mich auf die Installation über `zypper` beschränken.

Für die Pakete aus der Distribution müssen keine besonderen Repositories eingebunden sein, Sie können diese Pakete direkt installieren, so wie in Listing 3.8:

Listing 3.8 Installation der Samba-Pakete

```
sambabuch:~ # zypper install samba
.
Zusätzliche RPM-Ausgabe:
Updating /etc/sysconfig/samba...
```

Wenn Sie Samba unter Suse aus den eigenen Paketen installieren, können Sie den Samba-Dienst anschließend über den Yast konfigurieren. So können Sie jetzt einen Memberserver oder einen Client konfigurieren.

3.3.5 Installation der SerNet-Pakete

Für alle hier im Buch aufgeführten 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. Nachdem Sie den Zugang erhalten haben, können Sie sich auf der Website *https://oposso.samba.plus* anmelden und Ihre Subscription verwalten und mit einem Passwort versehen. Der Subscription Key und das von Ihnen vergebene Passwort sind auch die Anmeldedaten für den Download der Pakete.

Erweitern Sie Ihre Datei /etc/apt/sources.list um die Zeilen aus Listing 3.9:

Listing 3.9 Erweiterung der Datei /etc/apt/sources.list

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

Dabei müssen Sie den *KEY* durch Ihren Subscription Key ersetzen und das *PASSWORD* durch das von Ihnen vergebene Passwort für die Subscription.

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 3.10 zeigt diesen Vorgang:

Listing 3.10 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. Listing 3.11 zeigt eine Liste der Pakete:

Listing 3.11 Liste aller SerNet-Pakete

```
root@sambabuch:~# apt-get update

root@sambabuch:~# apt-cache search sernet
```

```
sernet-samba-winbind - Samba nameservice integration server
sernet-samba - SMB/CIFS file, print, and login server for Unix
sernet-samba-libpam-smbpass - Glue package for sernet-samba-libs.
sernet-samba-libsmbclient0 - Shared library that allows applications \
                             to talk to SMB servers
libwbclient0 - Glue package for sernet-samba-libs.
sernet-samba-ctdb - Cluster implementation of the TDB database
sernet-samba-common - Samba common files used by both the server \
                      and the client
sernet-samba-client - a LanManager-like simple client for Unix
sernet-samba-libwbclient-dev - libwbclient static libraries and headers
sernet-samba-ad - Samba Active Directory Domain Controller
sernet-samba-libs - Samba common library files used by both the server \
                    and the client
sernet-samba-dbg - Samba debugging symbols
libsmbclient - Glue package for sernet-samba-libsmbclient0.
sernet-samba-libsmbclient-dev - libsmbclient static libraries and headers
samba-common-bin - Glue package for sernet-samba-client.
samba-common - Glue package for sernet-samba-common.
sernet-samba-ctdb-tests - This package contains CTDB tests
sernet-samba-keyring - GnuPG archive keys of the SerNet Samba archive
samba - Glue package for sernet-samba.
sernet-samba-libwbclient0 - Glue package for sernet-samba-libs.
```

Wollen Sie jetzt einen Domaincontroller installieren, benötigen Sie die Pakete wie in Listing 3.12:

Listing 3.12 Installation der ADDC-Pakete

```
root@sambabuch:~# apt-get install sernet-samba-ad libpam-heimdal
```

Wollen Sie einen Domainmember installieren, benötigen Sie die Pakete aus Listing 3.13:

Listing 3.13 Installation der Member-Pakete

```
root@sambabuch:~# 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 festlegen. 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.

3.3.6 Installation der Pakete von Louis van Belle

Als weitere Möglichkeit der Installation der Samba-Pakete möchte ich hier noch die Pakete von Louis van Belle vorstellen. Diese Pakete sind immer aktuell und lassen sich auf Debian- und Ubuntu-Systemen sehr gut über Repositories installieren. Ich werde hier im Buch alle Schritte auf einem Debian-Server immer über diese Pakete durchführen. Auch wenn Sie diese Pakete nicht verwenden wollen, können Sie allen weiteren Schritten im Buch folgen, da auch hier dieselben Kommandos, Dateien und Pfade verwendet werden wie bei allen anderen Installationsarten auch.

Um die Pakete verwenden zu können, gehen Sie am besten so vor wie auf der Website *https://apt.van-belle.nl/* beschrieben. Für die verschiedenen Distributionen und Samba-Versionen gibt es dort eigene Repositories.

Anschließend können Sie mit *apt update* Ihre Paketliste aktualisieren und dann dieselben Pakete wie bei der Verwendung der Distributionspakete installieren. In Listing 3.14 sehen Sie diesen Vorgang:

Listing 3.14 Installation der Pakete

```
root@sambabuch:~# apt update

root@sambabuch:~# apt install samba \
                  libpam-heimdal heimdal-clients \
                  ldb-tools winbind libpam-winbind smbclient \
                  libnss-winbind \


Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut.
Statusinformationen werden eingelesen.... Fertig
.
.
.
Möchten Sie fortfahren? [J/n]
```

Hinweis

Wenn Sie später den Bind9 als DNS-Server an Stelle des internen DNS-Servers von Samba verwenden wollen, benötigen Sie auch hier auf jeden Fall die drei Pakete bind9, bind9utils und dnsutils.

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.

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. 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 die 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 unab-

hängig 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

```
root@addc-01:~# samba-tool
Usage: samba-tool <subcommand>

Main samba administration tool.


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

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


Available subcommands:
  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.
  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 Neues Datenbankformat

Wie schon in Kapitel 3, »Installation von Samba«, beschrieben, wurde mit der Samba-Version 4.9 erstmals das neue Datenbank-Backend *LMDB* (*Lightning Memory-Mapped Database*) vorgestellt. In der Version noch experimentell, aber mit der Samba-Version 4.11 auch produktiv nutzbar. Das neue Backend ermöglicht größere Datenbanken, um auch mehr als 100.000 Benutzer, Computer und Gruppen im Active Directory ablegen zu können. Auf jedem Domaincontroller, den Sie in die Domäne aufnehmen, müssen Sie das Datenbankformat explizit angeben. Wenn Sie es nicht nennen, wird weiterhin das alte Standardformat *tdb* verwendet. Neben dem neuen Format können Sie auch die gewünschte Größe der Datenbank angeben. Im Moment ist die Größe auf 8 GB festgelegt und kann nicht geändert werden.

Hinweis

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.

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, müssen Sie erst die dafür benötigten Informationen besorgen. Bei der Konfiguration des Domaincontrollers werden sie abgefragt. Die folgenden Informationen sollten Sie für die Konfiguration bereithalten:

- Den Realm:
  Der `Realm` wird für den Kerberos-Server benötigt. Der Realm wird bei der Einrichtung des DNS-Servers auch als DNS-Domainname verwendet.
- Den NetBIOS-Domainname:
  Der NetBIOS-Domainname ist die Adresse, über die der Server per NetBIOS-Protokoll erreichbar ist. Der NetBIOS-Name sollte immer der erste Teil des Realms sein.
- Die Funktion des Servers:
  Welche Rolle soll der Server in der Domäne übernehmen? In unserem Fall übernimmt er die Rolle des Domaincontrollers.
- Welchen DNS-Server wollen Sie verwenden?
  Sie müssen wissen, 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.

Hinweis

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

Wann brauchen Sie die Attribute?

Immer dann, wenn Sie zum Beispiel eine bestehende Domäne aus Samba 3 und OpenLDAP nach Samba 4 und Active Directory migrieren wollen, aber einen sehr großen Datenbestand mit komplexer Rechtestruktur haben und bei dem die Rechtestruktur auf UIDNumber und GIDNumber basiert. Dann können Sie später bei den Fileservern und den Linux-Clients das ID-Mapping über die UIDNumber und GIDNumber durchführen, und die Rechte bleiben erhalten.

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.

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.

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.

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@addc-01:~# samba-tool domain provision
Realm [EXAMPLE.NET]:
Domain [EXAMPLE]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [
    SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [8.8.8.8]:
Administrator password:
Retype password:
...: Looking up IPv4 addresses
...: More than one IPv4 address found. Using 192.168.56.101
```

```
...: Looking up IPv6 addresses
...: No IPv6 address will be assigned
...: Setting up share.ldb
...: Setting up secrets.ldb
...: Setting up the registry
...: Setting up the privileges database
...: Setting up idmap db
...: Setting up SAM db
...: Setting up sam.ldb partitions and settings
...: Setting up sam.ldb rootDSE
...: Pre-loading the Samba 4 and AD schema
Unable to determine the DomainSID, can not enforce \
     uniqueness constraint on local domainSIDs

...: Adding DomainDN: DC=example,DC=net
...: Adding configuration container
...: Setting up sam.ldb schema
...: Setting up sam.ldb configuration data
...: Setting up display specifiers
...: Modifying display specifiers and extended rights
...: Adding users container
...: Modifying users container
...: Adding computers container
...: Modifying computers container
...: Setting up sam.ldb data
...: Setting up well known security principals
...: Setting up sam.ldb users and groups
...: Setting up self join
Repacking database from v1 to v2 format (first record CN=ms-TAPI-
    Conference-Blob\
     ,CN=Schema,CN=Configuration,DC=example,DC=net)
Repack: re-packed 10000 records so far
Repacking database from v1 to v2 format (first record CN=rpcContainer-
    Display,CN=40B,\
        CN=DisplaySpecifiers,CN=Configuration,DC=example,DC=net)
Repacking database from v1 to v2 format (first record CN=Program Data,DC=
    example,DC=net)
...: Adding DNS accounts
...: Creating CN=MicrosoftDNS,CN=System,DC=example,DC=net
...: Creating DomainDnsZones and ForestDnsZones partitions
...: Populating DomainDnsZones and ForestDnsZones partitions
Repacking database from v1 to v2 format (first record DC=_kerberos._tcp.
    Default-First-Site-Name._sites,DC=example.net,CN=MicrosoftDNS,DC=
    DomainDnsZones,DC=example,DC=net)
Repacking database from v1 to v2 format (first record DC=_kerberos._tcp.
    dc,DC=_msdcs\
     .example.net,CN=MicrosoftDNS,DC=ForestDnsZones,DC=example,DC=net)
...: Setting up sam.ldb rootDSE marking as synchronized
...: Fixing provision GUIDs
...: A Kerberos configuration suitable for Samba AD has been generated at
     \
     /var/lib/samba/private/krb5.conf
```

```
...: Merge the contents of this file with your system krb5.conf or
    replace \
     item with this one. Do not create a symlink!
...: Once the above files are installed, your Samba AD server will be
    ready to use
...: Server Role:           active directory domain controller
...: Hostname:              addc-01
...: NetBIOS Domain:        EXAMPLE
...: DNS Domain:            example.net
...: DOMAIN SID:            S-1-5-21-521251523-4006440997-2509550191
```

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.

Da dieser Vorgang für alle Arten des Provisionings identisch ist, finden Sie den Vorgang nach den Beispielen des Provisionings in Abschnitt 4.3.1.

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 nicht interaktiv durchführen, dann übergeben Sie die benötigten Parameter beim Aufruf des Kommandos `samba-tool` wie in Listing 4.5:

Listing 4.5 Provisioning mit Parametern

```
root@addc-01:~# samba-tool domain provision --domain=example \
                --realm=example.net --host-ip=192.168.56.101 \
```

Wie Sie sehen, habe ich keine Angaben über das zu verwendende DNS-Backend gemacht und auch keine Angaben zur Serverrolle. Für beide Werte wird dann der Standard übernommen. Es wird der interne DNS-Server genutzt, und der Server wird ein Domaincontroller.

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.

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 4.6, 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.

Listing 4.6 Provisioning mit bind9

```
root@addc-01:~# samba-tool domain provision --domain=example \
                --realm=example.net --host-ip=192.168.56.101 \
```