
Setting up a Samba Active Directory

Autor:
Stefan KANIA

Ort:
St. Michaelisdonn

May, 9th 2023

Inhalt

1 Einführung	3
2 Vorteile von Samba 4	3
3 Nachteile von Samba 4	3
4 Installation der Software	4
4.1 Installation aus den Repositories der Distribution	4
4.1.1 Vorteile der Installation über die Repositories	5
4.2 Pakete von Drittherstellern	5
4.2.1 Nachteile der Pakete von Drittherstellern	5
4.3 Kommerzielle Pakete	5
4.3.1 Nachteile kommerzieller Pakete	6
5 Welche Version wählen?	6
6 Welche Funktionen kann Samba bereitstellen	6
7 Der erste Domaincontroller	8
7.1 Installation der Pakete	8
7.2 Pakete für einen File- oder Printserver	8
8 Einrichtung des ersten Domaincontrollers	9
8.1 Einrichtung des Bind9	10
8.2 Vorbereitung des Starts	11
8.3 Nach dem Neustart	12
8.4 Einrichten des Zeitervers	14
9 Benutzerverwaltung	14
10 Ein zweiter Domaincontroller	15
10.1 Vorbereitung des zweiten Domaincontrollers	15
10.2 Beitritt zur Domäne	16
10.3 Weitere Schritt	16
10.4 Nach dem Neustart	16
11 Replikation der Freigabe sysvol	19
11.1 Einrichten der Replikation	19

12 Einbinden von Linux-Clients	21
12.1 Vorbereitung eines Linux-Clients	21
12.2 Aufnehmen des Clients in die Domäne	23
13 Der Fileserver	23
13.1 Die administrative Freigabe	24
13.2 Basisverzeichnis der Benutzer	25
14 Linux-Client und smb-mount	26
14.1 Einrichtung von libpam-mount	26
15 Was geht sonst noch mit Samba?	28
16 Fazit	28
Stichwortverzeichnis	28

1 Einführung

Dieses Jahr geht es um die Einrichtung einer Active Directory Domäne mit Samba4, dabei geht es nicht nur um die eigentliche Einrichtung, sondern auch um die Vorteile und auch die Nachteile einer Samba Domäne, im Vergleich zu einer Windows Domäne.

Sie stehen eventuell vor der Entscheidung ein bestehende alt Domäne auf einen neuen Stand zu bringen, oder Sie wollen eine komplett neue Umgebung einrichten. Warum dann Samba4 nutzen und nicht Microsoft Active Directory?

Im diesjährigen Tutorial will ich Ihnen zeigen, wie einfach es ist, ein Active Directory mit Samba4 einzurichten und zu verwalten und welche Unterschiede zu einem Microsoft Active Directory bestehen.

2 Vorteile von Samba 4

Eine großer Vorteile von Samba4 als Active Directory sind wohl die Lizenzkosten. Das ist auch der Punkt, der am häufigsten erwähnt wird. Wobei nicht immer die eigentlich entstehenden Kosten die Entscheidung für Samba4 ausschlaggebend sind, sondern oft die Schwierigkeiten, überhaupt festzustellen, welche Lizenzen werden denn überhaupt benötigt. Oft führt alleine schon dieser Punkt zum Ausschluss von Microsoft.

Aber Sie sollten den Blick nicht unbedingt nur auf die Lizenzen begrenzen, viele andere Punkte sprechen für die Verwendung von Samba4 als Active Directory.

- Sie können, jetzt und auch in Zukunft, Ihre gesamte Infrastruktur in Ihrem Unternehmen halten. Microsoft geht immer mehr in Richtung SaaS und IaaS.
- Die Hardwareausstattung der Server hat geringere Ansprüche. Gerade wenn es darum geht, einen bestehenden Umgebung zu aktualisieren, kann das ein Punkt sein, der den Vorteil von Samba4 deutlich zeigt.
- Zusammen mit anderen open Source Produkten, wie GlusterFS/Ceph und CTDB, lassen sich auch hochverfügbare Fileserver ohne zusätzliche Lizenzkosten auf Standardhardware realisieren.

3 Nachteile von Samba 4

Wo viele Licht ist, ist auch Schatten, aus dem Grund sollen auch die Nachteile des Einsatz von Samba4 hier angesprochen werden.

- Neben den Kenntnissen im Bereich Active Directory sind für die Administration der System immer auch gute Linux-Kenntnisse notwendig. Wenn Sie in Ihrem Unternehmen nicht auf gute Linux-Kenntnisse zurückgreifen können, sollten Sie immer auch die Kosten für die Weiterbildung im Auge behalten. Eventuell macht es Sinn, entsprechende Experten einzustellen oder, zumindest für eine Übergangszeit, externe Fachleute hinzuzuziehen.
- Eine Einbindung von Microsoft-Exchange ist nicht möglich. Der Grund ist der, dass für MS-Exchange das Schema des Active Directories erweitert werden muss und diese Erweiterung wird von Samba4 nicht unterstützt. Auch eine Migration eine Windows-Domäne in der ein Exchange eingebunden ist, ist nicht möglich. Selbst dann nicht, wenn der Exchange-Server vorher aus der Domäne entfernt wird. Denn es bleiben immer noch Reste der Exchange-Umgebung im Active Directory bestehen.
- Die Replikation der wichtigen Sysvol-Freigabe wird nicht automatisch unterstützt, sondern muss durch zusätzliche Dienste bereitgestellt werden.

- Nicht alle Möglichkeiten der Administration der Server und der Active Directory-Umgebung lassen sich über die Remote Server Administration Tools (RSAT) realisieren. Für manche administrativen Tätigkeiten ist es notwendig, die Kommandozeile zu nutzen.
- Nicht alle Funktionen, wie zum Beispiel ein Baum aus mehreren Domänen, werden nicht unterstützt.

4 Installation der Software

Samba lässt sich über verschiedene Quellen installieren, die folgenden Möglichkeiten haben Sie. Bei allen Möglichkeiten sollten Sie immer darauf achten, dass Sie möglichst aktuelle Samba-Versionen einsetzen. Das Samba-Team pflegt grundsätzlich immer nur die letzten drei Versionen. Verwenden Sie ältere Versionen, sollten Sie sicherstellen, dass sich eventuelle Sicherheitslücke schließen lassen. Bei einem Releasezyklus vom 6 Monaten bis zur nächsten Version, heißt das, nach 1,5 Jahren sollten Sie spätestens ein Update auf eine aktuellere Version durchführen.

Installation aus den Quellen

Da es sich bei Samba um open Source Software handelt, haben Sie immer die Möglichkeit den aktuellen Quelltext zu nehmen und Samba selber zu kompilieren, dadurch sind Sie auf jeden Fall immer auf dem aktuellen Stand.

Vorteile des selbst kompilieren von Samba

Sie haben immer den aktuellen Softwarestand. Sie können einzelne Teile beim Kompilieren ausschließen und somit ist jede Installation genau auf die Belange des Systems angepasst. Wenn die Kenntnisse vorhanden sind, haben Sie natürlich die Möglichkeit den Quellcode zu verändern und gezielt an Ihre Belange anzupassen.

Nachteile des selber kompilieren von Samba

Sie brauchen eine Entwicklungsumgebung um Samba zu kompilieren, die dann entweder auf jedem System vorhanden sein muss, oder zentral bereitgestellt wird. Die kompilierte Version muss dann auf die verschiedenen Systeme kopiert werden. Änderung an bestimmten Bibliotheken (zum Beispiel durch Updates), können dazu führen, dass der Samba Dienst nicht mehr ordnungsgemäß funktioniert. Jede selbst kompilierte Version sollte immer erst auf einem Testsystem überprüft werden. Für das Kompilieren und eventuelles Anpassen des Quellcodes sind zusätzliche Kenntnisse erforderlich. Bei eventuell auftretenden Sicherheitslücken, sind Sie verantwortlich, die benötigten Pakete selbst zu kompilieren.

4.1 Installation aus den Repositories der Distribution

Alle Distributionen bringen Samba-Pakete mit sich. Aber, da Samba, zumindest im Moment, immer noch abhängig vom Heimdal-Kerberos ist, kann der Domaincontroller für das Active Directory nicht auf jeder Distribution installiert werden. Bei allen Redhat basierten Distributionen ist eine Installation eines Domaincontrollers mit den Distributionspaketen nicht möglich. Das selbe gilt für Suse-Produkte. Wobei Suse Samba-Domaincontroller unterstützt, dabei aber auf den (noch) experimentellen MIT-Kerberos setzt.

4.1.1 Vorteile der Installation über die Repositories

Die Pakete können direkt über den jeweiligen Paketmanager installiert werden. Abhängigkeiten werden automatisch aufgelöst. Soweit Sie Versionen Ihrer Distribution einsetzen die noch mit Updates unterstützt wird, werden Sicherheitslücken hier schnell geschlossen. Durch die einfache Installation können Samba-Server auch von Administratoren mit nur geringen Linux-Kenntnissen eingerichtet und verwaltet werden. Wenn Sie auf einheitliche Distributionen achten, sind die Samba-Versionen, und dadurch auch der Funktionsumfang, immer identisch.

Nachteile der Installation über die Repositories

Sie sind immer auf die Betreuer der Distribution angewiesen, was die Updates angeht. In den meisten Distributionen werden nicht die aktuellsten Versionen von Samba bereitgestellt, sodass Sie eventuell benötigten Funktionen von aktuellen Versionen nicht sofort nutzen können. Abhängig von den Funktionen die ein Samba-Server bereitstellt, kann es aber durchaus sinnvoll sein, die aktuellste Version zu nutzen. Mehr dazu später.

4.2 Pakete von Drittherstellern

Für einige Distributionen werden Repositories von einzelnen Entwicklern bereitgestellt, die dann von Ihnen in Ihre Distribution eingebunden und installiert werden können. Diese Pakete sind oft sehr gut gepflegt und daher könnten Sie eine Alternative zum selber Kompilieren sein.

Vorteile der Pakete von Drittherstellern

Die Pakete sind meist auf dem aktuellen Stand und können ohne große Probleme in die entsprechenden Distribution eingebunden werden. Die Pakete werden meist von engagierten Samba-Team Mitgliedern bereitgestellt.

4.2.1 Nachteile der Pakete von Drittherstellern

Die Pakete werden oft nur von einer Person gepflegt, kompiliert und bereitgestellt. Wenn diese Person, aus welchem Grund auch immer, die Aktualisierung der Pakete nicht mehr oder nur noch sehr schleppend durchführt, kann es zu Sicherheitsproblemen kommen. Schlimmstenfalls müssen Sie alle Server neu installieren um wieder sichere Systeme betreiben zu können.

4.3 Kommerzielle Pakete

Auch für Samba gibt es kommerzielle Pakete, wie zum Beispiel die Pakete der Firma Sernet, diese Pakete werden Ihnen über eine Subskription angeboten. Der Preis der Subskription ist abhängig davon, wie viele Server Sie für wie lange nutzen wollen. Die Pakete werden hier mit allen Funktionen für eine Vielzahl von Distributionen bereitgestellt. Auch wird dort die Funktion des Domaincontrollers für Redhat basierte Distributionen mit angeboten. Die Kosten für die Subscriptions sind nicht der Preis für die Software, bei Samba handelt es sich auch in dem Fall um open Source, sondern für den enthaltenen Support der Updates und der zusätzlichen Funktionen, wie zum Beispiel Nutzung der Redhat-Distributionen als Domaincontroller.

Vorteile kommerzieller Pakete

Neben der Bereitstellung der Pakete, können Sie zusätzlich einen Support buchen, der Ihnen bei der Einrichtung und dem Betrieb Ihrer Samba-System Unterstützung bietet. Die Pakete werden für verschiedene Version der Distributionen bereitgestellt. Alle Updates und Sicherheitsupdates werden zeitnah bereitgestellt und können, wie auch schon die Erstinstallation, über den Paketmanager der Distribution eingespielt werden. Auch beim Umstieg auf eine neuere Samba-Version können Sie davon ausgehen, dass der Updateprozess getestet wurde und funktioniert.

4.3.1 Nachteile kommerzieller Pakete

Die Subscriptions sind nicht kostenfrei. Aber für das Geld das Sie für die Subscriptions zahlen, erhalten Sie auch die regelmäßige Updates, die aktuellsten Versionen und eine schnelle Reaktion auf Sicherheitslücken.

5 Welche Version wählen?

Nach der Aufzählung der Möglichkeiten stellt sich jetzt die Frage: Welche Installationsart ist für mich die beste? Diese Antwort ist immer abhängig von der Funktion die Sie nutzen wollen und den Kenntnissen in Ihrem Unternehmen.

Immer wenn es darum geht, dass Sie Domaincontroller einsetzen wollen, ist es sinnvoll, möglichst immer eine sehr aktuelle Version von Samba nutzen, denn in dem Bereich Domaincontroller werden die meisten Änderungen durchgeführt. Achten Sie dabei immer auf die Release Notes, in denen werden die Neuerungen beschrieben. Wenn Sie eine der neuen Funktionen nutzen wollen, geht das nur mit einem Update.

Auch beim Einsatz von *Cluster Trival Data BaseCTDB* als Cluster sollten Sie möglichst aktuelle Versionen von Samba einsetzen, denn auch hier kommt es sehr häufig zu Änderungen bei neuen Versionen.

Beim Einsatz als einfacher Fileserver können Sie auch Version einsetzen, die nicht ganz so aktuell sind. So ist es hier durchaus ausreichend, die Pakete aus den Distributionen zu nutzen.

Wenn auf Ihren Clients Linux mit grafischer Oberfläche zum Einsatz kommt, können Sie an dieser Stelle auf jeden Fall die mit der Distribution ausgelieferten Pakete nutzen. Dadurch haben Sie auch immer einen einheitlichen Versionsstand auf Ihren Clients.

6 Welche Funktionen kann Samba bereitstellen

Nach dem ich Ihnen in den vorherigen Abschnitten die unterschiedlichen Arten und deren Vor- und Nachteile beschrieben habe, geht es jetzt darum, welche Dienste Samba im Netz bereitstellen kann.

Domaincontroller

Der *Domaincontroller* ist keine Dienst im eigentlichen Sinne, er setzt sich aus mehreren Diensten zusammen. Die folgenden Dienste zusammengenommen ergeben die Funktion Domaincontroller.

- DNS

Im Active Directory wird immer ein DNS-Server benötigt, der die Dienste, *Kerberos*, *LDAP* und den *global Catalog* für die Clients propagieren kann. Denn der Client fragt immer seine bei ihm eingetragene DNS-Server wo er die entsprechenden Dienste findet. Jeder Domaincontroller stellt dabei einen eigenen DNS-Server bereit. Als DNS-Server kann entweder der interne DNS-Server von Samba genutzt werden, oder der *Bind9*. In größeren Umgebungen ist der Bind9 auf

jeden Fall vorzuziehen, denn nur der Bind9 unterstützt DNS-round-robin, um zum Beispiel bei CTDB ein loadbalancing über DNS durchführen zu können.

- **Kerberos**
Kerberos sorgt für die Verschlüsselung von Passwörtern und der Datenübertragung innerhalb der Domäne. Hier kommt der Heimdal-Kerberos zum Einsatz. Der MIT-Kerberos ist, im Moment noch, *experimental*. Da hier eine Standard-Kerberos zum Einsatz kommt, kann dieser auch für die Authentifizierung für Dienste außerhalb der Active Directory-Domäne eingesetzt werden, zum Beispiel für die Authentifizierung auf Webservern.
- **LDAP**
Im LDAP werden alle Objekte und deren Attribute abgelegt. Hierbei handelt es sich um Benutzer, Gruppen, Computer, DNS-Einträge und andere Objekte. Samba 4 nutzt hierfür einen eigens für Samba entwickelten LDAP-Server, der auch nicht gegen einen andere LDAP-Server, zum Beispiel den OpenLDAP, ausgetauscht werden kann.
- **Global Catalog**
Im *global Catalog* werden Informationen aller Objekte im gesamten *forest* einer Active Directory-Umgebung abgelegt. Das betrifft Informationen aus allen Domänen des Active Directories. Nur so ist es möglich, dass Objekte auch in anderen Domänen des Active Directories gefunden werden können. Hier werden nur die wichtigsten Attribute eines Objekt abgelegt.
- **Zeitserver**
Jeder Domaincontroller muss auch die Funktion des Zeitserver bereitstellen, damit Windows-Clients, bei der Anmeldung die Zeit abgleichen können. Da die Windows-Clients in der Standardeinstellung die Zeit nur annehmen, wenn die Informationen vom Domaincontroller signiert sind, muss der Zeitserver dementsprechend konfiguriert sein.

Fileserver

Samba als *Fileserver* ist wohl die meist verwendete Funktion von Samba. Für die Funktion des Fileservers ist nicht zwingend ein Active Directory notwendig. Auf einem *standalone Fileserver* können Benutzer lokal angelegt werden und dann können Clients auf die dort eingerichteten Freigaben zugreifen. In den meisten Fällen werden Sie einen Fileserver aber zum Mitglied einer Domäne machen. Es spielt dabei keine Rolle, ob es sich um eine Samba 4 Domäne oder eine Microsoft-Domäne handelt, ein Samba-Fileserver kann seine Dienste überall bereitstellen.

Printserver

Samba können Sie in Ihrem Netz auch als *Printserver* einsetzen. Als Printserver kann Samba Drucker für alle Clientbetriebssystem bereitstellen. Für Windows-Clients können Sie auf einem Samba-Printserver auch die Druckertreiber (bis zum Type 3) bereitstellen und beim Zugriff automatisch auf Windows-Clients installieren.

Samba als Cluster

Samba in Verbindung mit *Cluster Trivial Database CTDB* können Sie in Ihrem Netzwerk eine hochverfügbaren und loadbalancing Filservercluster einrichten. Zusammen mit einem Clusterdateisystem wie *GlusterFS* oder *Ceph*. CTDB ist seit der Samba-Version 4.2 ein fester Bestandteil von Samba 4 und kann genau wie Samba selbst auf die oben beschriebenen Arten installiert werden. Für die Einrichtung eines CTDB-Clusters ist keine proprietäre Software notwendig, bei allen Teilen handelt es sich um open Source Produkte. Zusammen mit Standardhardware können Sie so einen kostengünstigen Cluster in Ihr Netz integrieren. Auch eine CTDB-Cluster kann sowohl in einer Samba 4 Domäne als auch in einer Windows-Domäne betrieben werden.

7 Der erste Domaincontroller

Im ersten Teil soll der erste Domaincontroller eingerichtet werden. Dafür sind verschieden Schritte notwendig.

7.1 Installation der Pakete

Die Installation der Samba-Pakete ist der einzige große Unterschied zwischen den Distributionen, da ich hier nicht auf alle Distributionen eingehen kann, liegt der Schwerpunkt hier auf Debian, wobei die selben Kommandos auf Ubuntu-System übernommen werden können. Der Grund ist der, dass nur mit Debian und Ubuntu alle Funktionen mit den Paketen der Distribution genutzt werden können. Damit bietet Debian und Ubuntu die beste Grundlage für den Einsatz von Samba, wenn Sie die Distributionspakete nutzen wollen. Selbstverständlich können Sie auch Samba, je nach Funktion, auf unterschiedlichen Distributionen in Ihrem Netzwerk einrichten, es ist aber sinnvoll, möglichst alle Systeme eines Dienstes auf der selben Distribution zu nutzen, dadurch wird die Administration der Systeme vereinfacht.

Bei der Installation der Pakete unter Debian werden Sie feststellen, dass dort nur die Samba-Version 4.13 installiert wird. Diese Version wird nicht mehr aktiv vom Samba-Team unterstützt. Durch einbinden der *bullseye-backports*, werden wir hier die Samba-Version 4.17 nutzen. Pakete aus den Backports sind aktueller, aber trotzdem so stabil, dass Sie sie auch produktiv nutzen können.

Für das Tutorial haben Sie die benötigten Pakete bereits durch die Einrichtung über Vagrant vorgenommen. Der Grund ist der, dass dadurch sichergestellt ist, dass wir für die Installation nicht zu sehr auf das Wlan angewiesen sind.

Pakete für einen Domaincontroller

Wenn Sie einen Domaincontroller einrichten wollen, ist die erste Überlegung: Soll der interne DNS oder der Bind9 genutzt werden. Denn für den Bind9 werden zusätzliche Pakete benötigt. Wollen Sie den internen DNS-Server nutzen installieren Sie die Pakete aus Listing 7.1.1:

```
apt install -t bullseye-backports samba libpam-heimdal heimdal-clients \
ldb-tools winbind libpam-winbind smbclient libnss-winbind bind9-host
```

Listing 7.1.1: Installation der Pakete interner DNS

Wollen Sie den Bind9 als DNS-Server nutzen, installieren Sie die Pakete aus Listing 7.1.2:

```
apt install -t bullseye-backports samba libpam-heimdal heimdal-clients \
ldb-tools winbind libpam-winbind smbclient libnss-winbind bind9 \
dnsutils bind9-host
```

Listing 7.1.2: Installation der Pakete Bind9 als DNS

Bei der Auswahl des DNS-Servers ist die Entscheidung nicht endgültig, wenn Sie erst den internen DNS nutzen und später auf den Bind9 umstellen wollen, können Sie das mit dem Kommando `samba.upgradedns --dns-backend=BIND9_DLZ`. Dann wird es aber notwendig, den Bind9 noch zu konfigurieren, bevor Sie den Dienst neu starten.

7.2 Pakete für einen File- oder Printserver

Für einen File- oder Printserver benötigen Sie die Pakete aus dem Listing 7.2.1:

```
apt install -t bullseye-backports samba libpam-heimdal heimdal-clients \
winbind libpam-winbind smbclient libnss-winbind bind9-host
```

Listing 7.2.1: Pakete für einen File- oder Printserver

Das sind die Pakete, die Sie für alle Dienste benötigen, zusätzlich benötigen Sie noch das Pakete `cups`, wenn Sie einen Printserver einrichten wollen. Da das eigentliche Drucken von *CUPS* übernommen wird. Samba setzt die Drucker die in CUPS eingerichtet sind nur so um, dass sie sich auch unter Windows nutzen lassen.

Soll Ihr Server Teil eines Clusters werden, installieren Sie zusätzlich das Pakete `ctdb`.

8 Einrichtung des ersten Domaincontrollers

Vor der eigentlichen Einrichtung des ersten Domaincontrollers ist es wichtig, dass Sie die folgenden, grundlegenden, Einstellungen auf Ihrem System vorgenommen und/oder überprüft haben:

- Prüfen Sie, ob in der Datei `/etc/hosts` nur die Einträge auf *localhost* und die eigen IP-Adresse mit dem *fqdn* und dem *hostname* eingetragen ist. Diese Werte werden beim Einrichten des Domaincontrollers aus der Datei gelesen.
- Stellen Sie sicher, dass das System eine feste IP-Adresse besitzt. Ein Domaincontroller ist immer an eine IP-Adresse gebunden. Eine spätere Änderung der IP-Adresse ist nur sehr schwer möglich.
- Prüfen Sie, ob Ihnen mit dem Kommando `hostname -f` der *fqdn* des Systems angezeigt wird.
- Löschen Sie die Datei `/etc/samba/smb.conf`. Diese Datei stammt von der Installation der Pakete (Wenn Sie die Sernet-Pakete nutzen, ist diese Datei nicht vorhanden). Beim Provisioning wird die Datei automatisch generiert.

Eines der wichtigsten Werkzeuge für die Verwaltung einer Active Directory Domäne ist das Programm `samba-tool`. Mithilfe des Programms können Sie nahezu alle Aufgaben der Domäne durchführen. Geben Sie, nachdem die Pakete installiert wurden, das Kommando `samba-tool` ohne weitere Parameter ein und Sie erhalten eine Übersicht über die verschiedenen Aufgaben, die Sie mit *samba-tool* durchführen können.

Nachdem Sie die Punkte berücksichtigt haben, folgt jetzt die Einrichtung *Provisionierung* des Domaincontrollers. Für das *Provisioning* haben Sie zwei verschiedene Möglichkeiten. Zum Einen können Sie einfach das Kommando `samba-tool domain provision` aufrufen, dann werden alle benötigten Informationen interaktiv abgefragt. Nach der Abfrage folgt dann das Provisioning.

Die andere Möglichkeit ist die, dass Sie alle benötigten Parameter an das Kommando `samba-tool domain provision` auf der Kommandozeile übergeben. Dabei haben Sie die Möglichkeit zusätzliche Parameter zu übergeben, die Sie bei der interaktiven Einrichtung nicht haben. Alle möglichen Parameter können Sie sich mithilfe des Kommandos `samba-tool domain provision -h` anzeigen lassen.

Die einfachste Art des Provisionings ist das interaktive Vorgehen, das soll auch hier genutzt werden. In Listing 8.1 sehen Sie die Ausgaben des Provisioning:

```
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]: BIND9_DLZ
Administrator password:
Retype password:
...
Server Role:          active directory domain controller
Hostname:             addc-01
NetBIOS Domain:       EXAMPLE
DNS Domain:           example.net
DOMAIN SID:           S-1-5-21-2057776938-3237700937-2176600150
```

Listing 8.1: Description

Außer bei der Auswahl des zu verwendenden DNS-Server und dem Passwort des Administrator, können Sie hier alle Fragen einfach mit RETURN bestätigen. Achten Sie bei dem Passwort auf die Komplexitätsregeln. Das Passwort muss mindestens sieben Zeichen lang sein und mindestens drei der vier Kategorien (Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen) enthalten. Weiterhin ist es wichtig zu wissen, dass das Passwort, im Gegensatz zu Microsoft, ein Ablaufdatum von 42 Tagen hat.

HINT! ☺

Sie können das Passwort des Administrators jeder Zeit, als root, mit dem Kommando `samba-tool user setpassword administrator` ändern.

8.1 Einrichtung des Bind9

Da wir hier den *Bind9* als DNS-Server nutzen wollen, der DNS-Server aber ein Hauptbestandteil des Domaincontrollers ist, muss dieser erst eingerichtet werden, bevor der eigentliche Dienst gestartet werden kann. Dazu sind Änderungen an zwei Dateien notwendig. Als erstens passen Sie die Datei `/etc/bind/named.conf.options` wie in Listing 8.1.1 an:

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

dnssec-validation no;
```

Listing 8.1.1: Anpassung der Datei `named.conf.options`

Der Eintrag *forwarders* legt fest, welcher DNS-Server gefragt wird, wenn der lokale Bind9 eine Anfrage nicht auflösen kann. Der *tkey-gssapi-keytab* Eintrag zeigt auf die Keytab-Datei die benötigt wird, damit sich der Bind9 gegenüber dem Kerberos-Dienst authentifizieren kann. Da der Bind9 Informationen lesen und schreiben können muss und die Informationen alle im Active Directory abgelegt sind, ist eine Authentifizierung erforderlich. Da keine DNSSec genutzt wird, sollte die Option hier abgeschaltet werden.

Jetzt fehlen dann noch die Änderungen an der Datei `named.conf.local`. In der Datei werden, wenn der Bind9 ohne Active Directory genutzt wird, die Zonen eingetragen für die der Bind9 zuständig ist. Da im Active Directory alle Zonen im Active Directory eingetragen sind, wird hier nur die Anbindung an das Active Directory konfiguriert. Die Einträge die Sie hier vornehmen sehen Sie in Listing 8.1.2:

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

Listing 8.1.2: Anpassungen der Datei `named.conf.local`

Hier wird nur auf die entsprechende Konfigurationsdatei verwiesen, die beim Provisioning erstellt wird. In der Datei selbst wird nur eine Eintrag für die eigene Bind9-Version aktiviert.

Jetzt kann der Bind9 neu gestartet werden und Sie können prüfen, ob der Bind9 auch auf das Active Directory zugreifen kann. In Listing 8.1.3 sehen Sie die entsprechenden Schritte und das Ergebnis des Tests:

```
root@addc-01:~# systemctl restart bind9
root@addc-01:~# tail -n 200 /var/log/syslog
...
samba_dlz: started for DN DC=example,DC=net
samba_dlz: starting configure
samba_dlz: configured writeable zone 'example.net'
samba_dlz: configured writeable zone '_msdcs.example.net'
...
```

Listing 8.1.3: Erster Start des Bind9

Nach dem Neustart wird das Ende der Log-Datei angezeigt. Scrollen Sie die Anzeige hoch, bis Sie die hier gezeigten Zeilen sehen. Jetzt ist der Bind9 konfiguriert und gestartet.

8.2 Vorbereitung des Starts

Bevor Sie den Dienst des Domaincontrollers starten können, ist es notwendig, weitere Schritte durchzuführen.

Kerberos Client-Datei kopieren

Kopieren Sie die Datei `/var/lib/samba/privat/krb5.conf` in das Verzeichnis `/etc`. So stellen Sie sicher, dass der Kerberos-Server auch erreicht werden kann. Es existiert zwar schon eine `krb5.conf` in der sind aber viele Einträge überflüssig und nicht alle benötigten Einträge sind vorhanden.

NAT-Device ausklammern

Hier in der Umgebung des Tutorials fehlt noch eine weitere Anpassung. Wenn Sie mit Vagrant und Linux arbeiten, wird immer eine Netzwerkkarte die via NAT konfiguriert wird benötigt. Da Samba immer auf allen Netzwerkkarten des Systems aktiv ist und auch immer alle IP-Adressen die aktiv sind den DNS eingetragen werden, müssen wir hier dafür sorgen, dass nur die zweite Netzwerkkarte genutzt wird.

Das Problem ist, dass bei allen NAT-Einträgen aller Hosts immer die IP-Adresse 10.0.2.15 genutzt wird. Wenn sich jetzt alle Systeme mit der IP-Adresse ins DNS eintragen, kommt es zu Konflikten. Tragen Sie daher die zwei Zeilen aus Listing 8.2.1 in den globalen Bereich der `smb.conf` ein:

```
interfaces = 192.168.56.41
bind interfaces only = yes
```

Listing 8.2.1: Auswahl der Netzwerkkarte

Das gilt für alle System die während des Tutorials genutzt werden.

Anpassen des Resolvers

Fehlt noch die Anpassung des *Resolvers*. In Zukunft soll der Domaincontroller immer den eigenen DNS-Server abfragen wenn eine Name aufgelöst werden muss. Passen Sie dazu die Datei `/etc/network/interfaces` wie in Listing 8.2.3 an:

```
allow-hotplug eth0
iface eth0 inet static
    address 10.0.2.15
    netmask 255.255.255.0
    gateway 10.0.2.2
    dns-nameservers 192.168.56.41
    dns-search example.net
```

Listing 8.2.2: Description

Aktivieren der Dienste

Wenn Sie Samba installieren, werden alle Dienst standardmäßig als *standalone Server* konfiguriert. Dementsprechend werden auch die benötigten Dienste gestartet. Um nun Samba auch als Domaincontroller zu starten, führen Sie die Kommandos aus Listing 8.2.2 aus:

```
root@addc-01:~# systemctl disable --now 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
Removed /etc/systemd/system/multi-user.target.wants/nmbd.service.
Removed /etc/systemd/system/multi-user.target.wants/winbind.service.
Removed /etc/systemd/system/multi-user.target.wants/smbd.service.

root@addc-01:~# systemctl unmask samba-ad-dc
Removed /etc/systemd/system/samba-ad-dc.service.

root@addc-01:~# systemctl enable --now 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
Created symlink /etc/systemd/system/multi-user.target.wants/\
samba-ad-dc.service -> /lib/systemd/system/samba-ad-dc.service.

```

Listing 8.2.3: Aktivieren der Dienste

Mit dem ersten Kommando `systemctl disable --now smbd nmbd winbind` werden alle standalone-Dienste deaktiviert und auch sofort gestoppt. Denn der Domaincontroller bringt eigene Instanzen dieser Dienst mit sich. Mit dem nächsten Kommando `systemctl unmask samba-ad-dc` wird überhaupt erst die Möglichkeit gegeben, den Dienst zu starten. Das Dritte Kommando `systemctl enable --now samba-ad-dc` aktiviert den Dienst und starte ihn sofort. Jetzt wird bei einem Neustart des Systems auch immer sofort der Domaincontroller gestartet.

HINWEIS! ⓘ

Hier im Beispiel handelt es sich um die Einstellungen für System in der Vagrant-Umgebung.

Um sicher zu stellen, dass alle Dienste auch bei einem Neustart des Systems wieder ordnungsgemäß gestartet werden, booten Sie jetzt das System neu.

8.3 Nach dem Neustart

Nachdem der Domaincontroller neu gestartet wurde, folgen jetzt ein paar Tests, die die Funktion der Dienste überprüfen.

Testen des DNS

Als erstes soll der DNS-getestet werden. Listing 8.3.1 zeigt die Kommandos und die erwarteten Ergebnisse:

```

root@addc-01:~# host addc-01
addc-01.example.net has address 192.168.56.41

root@addc-01:~# host -t srv _ldap._tcp.example.net
_ldap._tcp.example.net has SRV record 0 100 389 addc-01.example.net.

root@addc-01:~# host -t srv _kerberos._tcp.example.net
_kerberos._tcp.example.net has SRV record 0 100 88 addc-01.example.net.

root@addc-01:~# host -t srv _gc._tcp.example.net
_gc._tcp.example.net has SRV record 0 100 3268 addc-01.example.net.

```

Listing 8.3.1: Testen des DNS

Die Tests zeigen, dass der eigen Hostname und die Dienste die der Domaincontroller bereitstellt, aufgelöst werden können.

Testen des Kerberos

Zum testen des Kerberos-Servers soll jetzt ein Ticket für den Administrator angefordert werden, anschließend wir das Ticket angezeigt. In Listing 8.3.2 sehen Sie die Kommandos und Ergebnisse:

```
root@addc-01:~# kinit administrator
administrator@EXAMPLE.NET's Password:

root@addc-01:~# klist
Credentials cache: FILE:/tmp/krb5cc_0
    Principal: administrator@EXAMPLE.NET

    Issued                Expires                Principal
Jan 11 14:22:11 2023    Jan 12 00:22:11 2023    krbtgt/EXAMPLE.NET@EXAMPLE.NET
```

Listing 8.3.2: Testen des Kerberos

Im ersten Schritt wird das Ticket angefordert. Im zweiten Schritt werden alle Tickets des Benutzer angezeigt. Da zu diesem Zeitpunkt noch kein Zugriff auf einen Dienst stattgefunden hat, wird hier nur das eigene *Ticket-granting-Ticket(tgt)* angezeigt.

Testen des Verbindungsaufbau

Auf jedem Domaincontroller werden auch immer zwei Freigaben `sysvol` und `netlogon` eingerichtet. Diese Freigaben existieren auch auf jedem Windows-Domain Domaincontroller. Mit dem Test zum Verbindungsaufbau wird geprüft, ob der Domaincontroller diese Freigabe auch bereitstellen kann. Listing 8.3.3 zeigt den Test:

```
root@addc-01:~# smbclient -L addc-01 -N

    Sharename      Type      Comment
    -----
    sysvol         Disk
    netlogon       Disk
    IPC$           IPC       IPC Service (Samba 4.17.4-Debian)
SMB1 disabled -- no workgroup available

root@addc-01:~# klist
Credentials cache: FILE:/tmp/krb5cc_0
    Principal: administrator@EXAMPLE.NET

    Issued                Expires                Principal
Jan 11 14:22:11 2023    Jan 12 00:22:11 2023    krbtgt/EXAMPLE.NET@EXAMPLE.NET
Jan 11 14:43:52 2023    Jan 12 00:22:11 2023    cifs/addc-01@EXAMPLE.NET
```

Listing 8.3.3: Verbindungsaufbau testen

Die Option `-N` sorgt dafür, dass nicht mehr nach einem Passwort gefragt wird. Da Sie vorher schon eine Kerberos-Ticket angefordert haben, wird hier sofort Kerberos für die Authentifizierung genutzt. Am Ergebnis des zweiten Kommandos sehen Sie dann auch sofort, dass Sie ein entsprechendes Serviceticket erhalten haben.

Testen des LDAP-Servers

Als letzter Dienst soll jetzt der LDAP geprüft werden. Da in der Tutorialumgebung das Paket `ldb-utils` installiert wurde, sind auch die entsprechenden Kommandos für den Zugriff auf den LDAP-Server vorhanden. Beim Zugriff auf den LDAP-Server wird das Protokoll `ldap`, zusammen mit `kerberos` genutzt. Die Verbindung wird durch den Einsatz von Kerberos verschlüsselt. Auf Grund von Sicherheitsproblemen wurde, schon vor einiger Zeit, der Zugriff über `ldaps` deaktiviert. Listing 8.3.4 zeigt den Zugriff auf den LDAP und anschließend werden erneut die Kerberos-Tickets aufgelistet:

```

root@addc-01:~# ldbsearch -H ldap://addc-01 cn=administrator -k yes
# record 1
dn: CN=Administrator,CN=Users,DC=example,DC=net
...

root@addc-01:~# klist
Credentials cache: FILE:/tmp/krb5cc_0
Principal: administrator@EXAMPLE.NET

    Issued                Expires                Principal
Jan 11 14:22:11 2023    Jan 12 00:22:11 2023    krbtgt/EXAMPLE.NET@EXAMPLE.NET
Jan 11 14:43:52 2023    Jan 12 00:22:11 2023    cifs/addc-01@EXAMPLE.NET
Jan 11 14:53:17 2023    Jan 12 00:22:11 2023    ldap/addc-01@EXAMPLE.NET

```

Listing 8.3.4: Testen des LDAP

Jetzt haben Sie alle Dienste die der Domaincontroller bereitstellt getestet.

8.4 Einrichten des Zeitervers

Bleibt als letztes noch die Einrichtung des Zeitervers, damit die Windows-Clients bei der Anmeldung die Zeit abgleichen können. Dazu wird als erstes das Paket `ntp` installiert. Kopieren Sie anschließend die Datei `/data/ntp.conf` in das Verzeichnis `/etc`. Die wichtige Zeile in der Datei ist `ntpsigndsocket /var/lib/samba/ntp-signd/` denn in dem hier angegeben Verzeichnis liegt der Socket, der die Zeitpakete an den Client signiert. Nur stimmen an dem Verzeichnis die Berechtigungen nicht, die Gruppe `ntp` muss an dem Verzeichnis die Rechte `r-x` besitzen. Ändern Sie die besitzende Gruppe mit dem Kommando `chgrp ntp /var/lib/samba/ntp-signd/`. Starten Sie anschließend den `ntp` neu.

Damit ist die komplette Einrichtung des ersten Domaincontrollers abgeschlossen.

9 Benutzerverwaltung

An dieser Stelle möchte ich ganz kurz auf die Verwaltung der Benutzer und Gruppen eingehen. Benutzer und Gruppen können Sie sowohl über die Kommandozeile der Domaincontroller verwalten, als auch über die von Microsoft bereitgestellten *Remote Server Administration Tools (RSAT)*. Alle Aktionen die Sie für Benutzern und Gruppen auf der Kommandozeile durchführen, können Sie in der RSAT nachvollziehen und umgekehrt. Um die RSAT zu nutzen, benötigen Sie eine Windows-Client der Mitglied der Domäne ist. Das Hinzufügen eine Windows-Clients zur Domäne unterscheidet sich nicht von dem Hinzufügen zu einer Windows-Domäne.

Die Verwaltung der Benutzer führen Sie mit dem Kommando `samba-tool user` durch. Wenn sie nur das Kommando eingeben, bekommen Sie alle möglichen Optionen angezeigt.

Für die Verwaltung der Gruppen nutzen Sie das Kommando `samba-tool group`. Auch hier erhalten Sie eine Auflistung der Möglichkeiten wenn Sie nur das Kommando eingeben.

In Abbildung 9.1 sehen Sie die Übersicht über Benutzer und Gruppen.

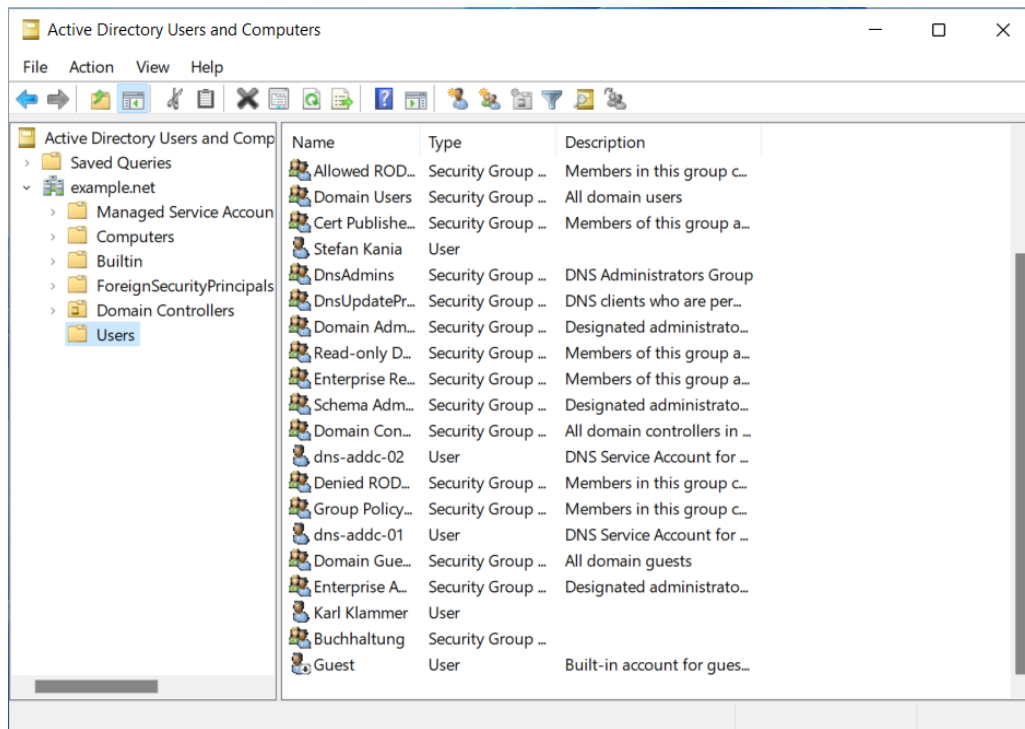


Abbildung 9.1: Benutzer und Gruppen

10 Ein zweiter Domaincontroller

Bis zu diesem Zeitpunkt betreiben Sie in Ihrer Domäne nur einen Domaincontroller. Fällt der eine Domaincontroller aus, kann sich niemand mehr in der Domäne anmelden. Lässt sich der Domaincontroller auch nicht mehr neu starten, verlieren Sie eventuell alle Benutzerinformationen und Sie haben erhebliche Ausfallzeiten. Um diese *single point of failure* zu umgehen, ist es ratsam immer mindestens zwei Domaincontroller in einer Domäne zu betreiben.

Die Maschine für den zweiten Domaincontroller ist bereits installiert. Jeder weiterer Domaincontroller kann immer alle Dienste bereitstellen, sodass der Ausfall eines Domaincontrollers nicht zum Ausfall der gesamten Domäne führt.

10.1 Vorbereitung des zweiten Domaincontrollers

Wie schon beim ersten Domaincontroller, werden als erstes die Pakete installiert. Dieser Schritt ist hier im Tutorial bereits erfolgt. Zusätzlich zu den Grundeinstellungen die Sie bereits auf dem ersten Domaincontroller vor dem Provisioning durchgeführt haben, ist es wichtig, dass Sie den *Resolver* des zweiten Systems so einstellen, dass als *Nameserver* die IP-Adresse des ersten Domaincontrollers eingetragen ist, da sonst die Domäne nicht gefunden werden kann und der neue Domaincontroller nicht der Domäne beitreten kann. Erst wenn Sie den Hostnamen des ersten Domaincontrollers und die *srv-records* auflösen können, dürfen Sie mit den nächsten Schritten fortfahren. Listing 10.1.1 zeigt noch einmal die entsprechenden Kommandos:

```
root@addc-02:/# host addc-01
addc-01.example.net has address 192.168.56.41

root@addc-02:/# host -t srv _ldap._tcp.example.net
_ldap._tcp.example.net has SRV record 0 100 389 addc-01.example.net.

root@addc-02:/# host -t srv _kerberos._tcp.example.net
_kerberos._tcp.example.net has SRV record 0 100 88 addc-01.example.net.
```



```
root@addc-02:/# host -t srv _gc._tcp.example.net
_gc._tcp.example.net has SRV record 0 100 3268 addc-01.example.net.
```

Listing 10.1.1: Testen der Namensauflösung

10.2 Beitritt zur Domäne

Nach dem Sie alle Voreinstellung vorgenommen habe, können Sie jetzt den Domaincontroller zur Domäne hinzufügen. Dafür wird wieder das Programm `samba-tool` verwendet. Dieses Mal wird der Vorgang aber direkt über die Kommandozeile durchgeführt, da bestimmte Parameter benötigt werden, die bei der interaktiven Nutzung des Programms nicht übergeben werden können. Listing 10.2.1 zeigt das Kommando und eine gekürzte Ausgabe des Ergebnis:

```
root@addc-02:~# samba-tool domain join --dns-backend=BIND9_DLZ example.net DC \
--realm=example.net -U administrator
Finding a writeable DC for domain 'example.net'
Found DC addc-01.example.net
...
Joined domain EXAMPLE (SID S-1-5-21-2057776938-3237700937-2176600150) as a DC
```

Listing 10.2.1: Hinzufügen des zweiten Domaincontrollers

Während des Vorgangs werden alle Daten des Active Directories vom ersten Domaincontroller auf den zweiten repliziert und eine Replikation wird zwischen den beiden Domaincontroller eingerichtet, sodass alle Änderungen, egal auf welchem Domaincontroller Sie die Änderungen durchführen, immer auf den jeweils anderen Domaincontroller repliziert werden.

10.3 Weitere Schritt

Damit der Domaincontroller dann auch vollständig in die Domäne integriert ist, sind jetzt noch die folgenden Schritte notwendig.

- Kopieren Sie die beiden Konfigurationsdateien `named.conf.options` und `named.conf.local` auf den zweiten Domaincontroller. Hier im Tutorial finden Sie die beiden Dateien im Verzeichnis `/data` des zweiten Domaincontrollers.
- Kopieren Sie die Datei `/var/lib/samba/privat/krb5.conf` in das Verzeichnis `/etc`.
- Sorgen Sie dafür, dass nach einem Neustart des Systems, die eigene IP-Adresse als Resolver in der Datei `/etc/resolv.conf` eingetragen ist.
- Editieren Sie die Datei `/etc/samba/smb.conf`, so wie schon auf dem ersten Domaincontroller, das nur die IP-Adresse 192.168.56.42 vom Samba verwendet wird.
- Wie schon beim ersten Domaincontroller ist es notwendig, dass Sie die standalone-Dienste deaktivieren und den `samba-ad-dc`-Dienst aktivieren.

Nur bei Verwendung der Vagrant-Umgebung

Beim hinzufügen zur Domäne werden für den neuen Domain Domaincontroller alle Netzwerkkarten im DNS eingetragen, auch das NAT-Interface mit der IP 10.0.2.15. Da alle Systeme die selbe IP-Adresse für das NAT-Interface nutzen, müssen Sie unbedingt die IP-Adresse aus dem DNS mit dem Kommando aus Listing ?? entfernen:

```
root@addc-01:/home/vagrant# samba-tool dns delete addc-01 example.net addc-02 A 10.0.2.15 -N
Record deleted successfully
```

Listing 10.3.1: Entfernen des NAT-Interfaces

Starten Sie anschließend den Server neu.

10.4 Nach dem Neustart

Nach dem Neustart können Sie die Tests, die Sie schon beim ersten Domaincontroller durchgeführt haben, auch auf dem zweiten Domaincontroller durchführen.

Einen großen Unterschied werden Sie bei der Abfrage der srv-Records feststellen, denn dort werden jetzt beide Domaincontroller angezeigt. Das ist auch die korrekte Anzeige, denn die Dienste werden von beiden Domaincontrollern angeboten und somit auch über DNS propagiert. Wenn Sie eines der Kommandos zur Auflösung des srv-Records mehrfach wiederholen, werden Sie feststellen, dass die Einträge immer in anderer Reihenfolge angezeigt werden. Dafür sorgt der Bind9 der die Einträge via DNS-round-robin immer wieder in der Reihenfolge ändert. So werden die Anfragen der Clients immer an andere Domaincontroller weitergeleitet und beide Domaincontroller werden genutzt. Auch das spricht für die Nutzung des Bind9 als Nameserver.

Es ist sinnvoll gelegentlich zu prüfen, ob die Replikation zwischen den Domaincontroller funktioniert. Listing 10.4.1 zeigt das Kommando und die Ausgabe:

```
root@addc-01:/home/vagrant# samba-tool drs showrepl
Default-First-Site-Name\ADDC-01
DSA Options: 0x00000001
DSA object GUID: 7410dc40-16c2-400c-b3a7-7582f7e83e74
DSA invocationId: 4b9a305e-fca3-49eb-af5b-09a6b2caae40

==== INBOUND NEIGHBORS ====

DC=ForestDnsZones,DC=example,DC=net
  Default-First-Site-Name\ADDC-02 via RPC
    DSA object GUID: b19f98d3-ed2c-4a17-ba76-bd81546f1034
    Last attempt @ Wed Jan 11 18:12:28 2023 UTC was successful
    0 consecutive failure(s).
    Last success @ Wed Jan 11 18:12:28 2023 UTC

CN=Configuration,DC=example,DC=net
  Default-First-Site-Name\ADDC-02 via RPC
    DSA object GUID: b19f98d3-ed2c-4a17-ba76-bd81546f1034
    Last attempt @ Wed Jan 11 18:12:28 2023 UTC was successful
    0 consecutive failure(s).
    Last success @ Wed Jan 11 18:12:28 2023 UTC

CN=Schema,CN=Configuration,DC=example,DC=net
  Default-First-Site-Name\ADDC-02 via RPC
    DSA object GUID: b19f98d3-ed2c-4a17-ba76-bd81546f1034
    Last attempt @ Wed Jan 11 18:12:28 2023 UTC was successful
    0 consecutive failure(s).
    Last success @ Wed Jan 11 18:12:28 2023 UTC

DC=example,DC=net
  Default-First-Site-Name\ADDC-02 via RPC
    DSA object GUID: b19f98d3-ed2c-4a17-ba76-bd81546f1034
    Last attempt @ Wed Jan 11 18:12:28 2023 UTC was successful
    0 consecutive failure(s).
    Last success @ Wed Jan 11 18:12:28 2023 UTC

DC=DomainDnsZones,DC=example,DC=net
  Default-First-Site-Name\ADDC-02 via RPC
    DSA object GUID: b19f98d3-ed2c-4a17-ba76-bd81546f1034
    Last attempt @ Wed Jan 11 18:12:28 2023 UTC was successful
    0 consecutive failure(s).
    Last success @ Wed Jan 11 18:12:28 2023 UTC

==== OUTBOUND NEIGHBORS ====

DC=ForestDnsZones,DC=example,DC=net
  Default-First-Site-Name\ADDC-02 via RPC
```

```

        DSA object GUID: b19f98d3-ed2c-4a17-ba76-bd81546f1034
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

CN=Configuration,DC=example,DC=net
    Default-First-Site-Name\ADDC-02 via RPC
        DSA object GUID: b19f98d3-ed2c-4a17-ba76-bd81546f1034
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

CN=Schema,CN=Configuration,DC=example,DC=net
    Default-First-Site-Name\ADDC-02 via RPC
        DSA object GUID: b19f98d3-ed2c-4a17-ba76-bd81546f1034
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

DC=example,DC=net
    Default-First-Site-Name\ADDC-02 via RPC
        DSA object GUID: b19f98d3-ed2c-4a17-ba76-bd81546f1034
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

DC=DomainDnsZones,DC=example,DC=net
    Default-First-Site-Name\ADDC-02 via RPC
        DSA object GUID: b19f98d3-ed2c-4a17-ba76-bd81546f1034
        Last attempt @ NTTIME(0) was successful
        0 consecutive failure(s).
        Last success @ NTTIME(0)

==== KCC CONNECTION OBJECTS ====

Connection --
    Connection name: 40b844fa-13c7-4530-9c95-44ba24fba175
    Enabled          : TRUE
    Server DNS name  : addc-02.example.net
    Server DN name   : CN=NTDS Settings,CN=ADDC-02,CN=Servers,\
CN=Default-First-Site-Name,CN=Sites,CN=Configuration,\
DC=example,DC=net
    TransportType: RPC
    options: 0x00000001
Warning: No NC replicated for Connection!

Listing 10.4.1: Prüfung der Replikation

```

Die Abfrage wurde auf dem zweiten Domaincontroller durchgeführt. Hierbei wird zwischen der *INBOUND NEIGHBORS* und der *OUTBOUND NEIGHBORS* Replikation unterschieden. Also was kommt an Daten rein und was wird raus gesendet. Hier sind jetzt nur zwei Domaincontroller im Einsatz, wenn Sie mehrere Domaincontroller betreiben, ist die Liste entsprechend lang. Meist will man aber nur die eventuell auftretenden Fehler sehen und nicht das was funktioniert hat. Aus diesem Grund gibt es die Option *--summary* die nur ein kurzes Ergebnis zeigt wenn alles funktioniert. Sollte es zu Fehlern an irgendeiner Stelle der Replikation kommen, werden auch nur die Fehler angezeigt. Listing 10.4.2 zeigt die zusammengefasste Anzeige:

```

root@addc-01:/home/vagrant# samba-tool drs showrepl --summary
[ALL GOOD]

```

Listing 10.4.2: Zusammengefasste Anzeige des Replikationstests

Solange nur diese eine Zeile angezeigt wird, ist auch alles in Ordnung.

Fehlt nur noch die Einrichtung des Zeitserver. Gehen Sie dabei genau so vor, wie schon beim ersten Domaincontroller. Zu diesem Zeitpunkt werden jetzt alle Informationen aus dem LDAP auf beide Domaincontroller repliziert. Egal auf welchem der Domaincontroller Änderungen vornehmen, der andere Domaincontroller wird die Änderungen übernehmen.

Jetzt fehlt nur noch die Replikation der Freigabe `sysvol`. Die Replikation der Freigabe folgt im nächsten Abschnitt.

11 Replikation der Freigabe `sysvol`

Neben der Datenbank mit den Objekten des Active Directories, die auf allen Domaincontrollern vorhanden ist, werden auch noch die Daten der Freigabe `sysvol` benötigt. In dieser Freigabe befinden sich die Informationen zu den *Gruppenrichtlinien*(GPO) und den eventuell noch vorhandenen Logon-Skripten. Auch diese Informationen müssen auf allen Domaincontrollern bereitgestellt werden. In einem Microsoft Active Directory wird die Replikation der Freigabe über ein eigenes Protokoll realisiert, das ist leider unter Samba so nicht möglich. Deshalb ist es notwendig, dass Sie die Replikation der Freigabe manuell einrichten.

Bei der Replikation der Freigabe `sysvol` in einer Samba4 Domäne wird immer einer der Domaincontroller die schreibende Instanz sein und alle anderen Domaincontroller werden die Daten nur vom diesem Domaincontroller replizieren. Nur welcher der Domaincontroller soll diese Rolle übernehmen? Im Prinzip kann die Rolle jeder Domaincontroller übernehmen. Aber, es gibt einen Domaincontroller der prädestiniert ist, diese Rolle zu übernehmen.

Die fsmo Rollen

Laut Microsoft ist jeder Domaincontroller einer Domäne gleichberechtigt und Sie können alle Daten auf allen Domaincontrollern ändern. Das ist aber nicht die ganze Wahrheit. Es gibt sieben zusätzliche Rollen die *flexible single master operation roles* (*fsmo*). Diese Rollen legen bestimmte Funktionen auf einen Domaincontroller der Domäne fest. Unter anderen gibt es dort die Rolle *PdcEmulationMasterRole*. Wenn der Domaincontroller mit dieser Rolle nicht erreichbar ist, lassen sich bestimmte Änderungen, wie zum Beispiel Passwortänderungen, nicht mehr durchführen. Auch ist der Domaincontroller mit dieser Rolle immer die Standardauswahl wenn Sie das Werkzeug zur Bearbeitung der GPOs starten. Da die Informationen der GPOs standardmäßig dort geändert werden, ist es sinnvoll, auch diesen Domaincontroller als Master der Replikation einzurichten. Wie Sie den Domaincontroller ermitteln der diese, und auch alle anderen Rollen, hält, sehen Sie in Listing 11.1:

```
root@addc-02:~# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=ADDC-01,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
InfrastructureMasterRole owner: CN=NTDS Settings,CN=ADDC-01,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
RidAllocationMasterRole owner: CN=NTDS Settings,CN=ADDC-01,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=ADDC-01,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
DomainNamingMasterRole owner: CN=NTDS Settings,CN=ADDC-01,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=ADDC-01,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=ADDC-01,CN=Servers,\
    CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
```

Listing 11.1: Auflistung aller fsmo

Es spielt dabei keine Rolle, auf welchem Ihrer Domaincontroller Sie die Abfrage starten.

In unserem Fall liegen alle Rollen auf dem `addc-01`. Das ist auch der erste Domaincontroller den wir eingerichtet haben. Alle Rollen können, wenn es notwendig wird, später auf einen anderen Domaincontroller übertragen werden. Ein Grund wäre zum Beispiel, wenn Sie den Domaincontroller endgültig aus der Domäne entfernen wollen.

11.1 Einrichten der Replikation

Für die Replikation der Freigabe `sysvol` wird das Programm `rsync` verwendet. Zusammen mit dem `systemd` wird auf dem ersten Domaincontroller ein `rsync-Server` eingerichtet. Auf allen weiteren Domaincontrollern wird `rsync` als Client genutzt um die Informationen vom Server zu replizieren.

Einrichtung des `rsync-Server`

Installieren Sie als erstes das Paket `rsync`. Für den `rsync-Server` benötigen Sie eine Konfigurationsdatei `/etc/rsyncd.conf`. Den Inhalt der Datei sehen Sie in Listing 11.1.1:

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

Listing 11.1.1: Die Datei `rsyncd.conf`

Eine Kopie der Datei finden Sie auf dem Domaincontroller `addc-01` im Verzeichnis `/data`. Kopieren Sie die Datei ins Verzeichnis `/etc`. Erstellen Sie im Verzeichnis `/etc/samba` die Datei `rsync.secret` mit dem Inhalt aus Listing 11.1.2:

```
sysvol-repl:geheim
```

Listing 11.1.2: Inhalt der Datei `rsync.secret`

Stellen Sie anschließend sicher, dass die Datei dem Benutzer und der Gruppe `root` gehört und die Datei die Berechtigungen `600` hat. Stimmen die Berechtigungen nicht, lässt sich der Dienst nicht starten. Starten Sie anschließend den Dienst mit dem Kommando `systemctl restart rsync` neu. Prüfen Sie den Status mit `systemctl status rsync`.

Einrichten des `rsync-Client`

Auf allen anderen Domaincontrollern wird `rsync` benötigt um die Daten vom `rsync-Server` zu replizieren. Installieren Sie daher auch auf dem anderen Domaincontroller `rsync`.

Nach der Installation legen Sie eine Datei `/etc/samba/rsync.pass` an. In der Datei darf nur das Passwort des auf dem `rsync-Server` definierten Benutzers stehen. Achten Sie auch hier auf die selben Berechtigungen wie schon auf dem Server.

Jetzt können Sie, mit dem Kommando aus Listing 11.1.3 den ersten Test durchführen. Der Parameter `--dry-run` sorgt dafür, dass erst einmal nur getestet wird, ob das Richtige repliziert wird. Den Parameter `--delete-after` dürfen Sie auf keine Fall vergessen, denn dieser Parameter sorgt dafür, dass Dateien die auf dem `rsync-Server`, seit der letzten Replikation gelöscht wurden, auch auf dem Client gelöscht werden.

```
root@addc-02:~# rsync -XAavz --delete-after --dry-run \
    --password-file=/etc/samba/rsync.pass \
    rsync://sysvol-repl@addc-01/sysvol \
    /var/lib/samba/sysvol/
receiving file list ... done
./
example.net/
example.net/Policies/
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/
```

```
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/USER/
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/USER/
example.net/scripts/
```

```
sent 59 bytes received 1,128 bytes 791.33 bytes/sec
total size is 40 speedup is 0.03 (DRY RUN)
```

Listing 11.1.3: Erster Test der Replikation

Erst wenn Sie dieses Ergebnis sehen, können Sie den Parameter *--dry-run* aus dem Kommando entfernen und die Replikation durchführen. Ein Blick in das Verzeichnis `/var/lib/samba/sysvol/example.net/` zeigt jetzt, dass die Daten repliziert wurden.

Nachdem die erste Replikation erfolgreich war, sorgen Sie jetzt dafür, dass die Replikation regelmäßig ausgeführt wird. Hierzu können Sie das Kommando direkt in die *crontab* des Benutzers *root* schreiben, oder Sie erstellen erst ein Shell-Skript das dann über den *Cron* ausgeführt wird. Im Verzeichnis `/data`, auf dem Domaincontroller *adde-02*, finden Sie ein Skript mit dem Namen *sysvol-repl.bash*, das Sie hierfür nutzen können. Wie häufig Sie das Skript laufen lassen, ist davon abhängig, wie viele Änderungen Sie an GPOs und Login-Skripten vornehmen.

Damit haben Sie jetzt eine Domäne mit zwei Domaincontrollern, die alle benötigten Daten replizieren. Im nächsten Abschnitt geht es dann um die Integration von Linux-Clients und Fileservern.

12 Einbinden von Linux-Clients

Der Begriff *Linux-Client* ist hier immer im Bezug auf die Active Directory-Domäne zu sehen. Sowohl eine späterer Linux-Fileserver, als auch eine Linux-Arbeitsstation sind, aus der Sicht der Domäne, immer nur Clients, die die zentrale Authentifizierung über das Active Directory nutzen wollen. Die Einrichtung des eigentlichen Fileservers folgt erst im nächsten Abschnitt.

Auf einem Linux-Client installieren Sie die identischen Samba-Pakete wie schon auf den Domaincontrollern, die Pakete für den Bind9, genau wie das Paket *ldb-utils* benötigen Sie hier nicht. Für das Tutorial sind bereits alle notwendigen Pakete installiert.

Da die folgenden Schritte auf allen Client-Systemen identisch sind, spielt es keine Rolle, auf welchem der System Sie beginnen. Ich werde hier in den Beispielen den Vagrant-Host *fs01* nutzen, da dieser im Anschluss als Fileserver konfiguriert werden soll.

12.1 Vorbereitung eines Linux-Clients

auf dem Client führen Sie jetzt die nachfolgenden Schritte aus:

- Auch hier können Sie als erstes die Datei `/etc/samba/smb.conf` löschen, da diese für die Nutzung als Active Directory-Client unbrauchbar ist.
- Prüfen Sie die Datei `/etc/hosts` dort darf, neben der *localhost*-Zeile, nur eine Zeile mit der eigene IP-Adresse, dem fqdn und dem Kurznamen stehen.
- Sorgen Sie dafür, dass als *Resolver* mindestens einer Domaincontroller, besser zwei, eingetragen ist.
- Prüfen Sie, ob mit dem Kommando `hostname -f` der fqdn des Clients angezeigt wird

Jetzt fehlt noch die neue *smb.conf* die jetzt mit den Inhalten aus Listing 12.1.1 gefüllt wird:

```
[global]
    workgroup = EXAMPLE
    realm = EXAMPLE.NET
    security = ADS
    winbind refresh tickets = Yes
    winbind use default domain = yes
    template shell = /bin/bash
    idmap config * : range = 10000 - 19999
    idmap config EXAMPLE : backend = rid
    idmap config EXAMPLE : range = 10000000 - 19999999
    interfaces = 192.168.56.51
    bind interfaces only = yes
```

Listing 12.1.1: die Datei `smb.conf` für den Client

Eine vorbereitete Datei finden Sie im Verzeichnis `/data`, sowohl auf dem *client-01* als auch auf dem Fileserver *fs-01*.

Diese Einstellungen sind auf allen Linux-Clients in Ihrer Domäne identisch. Die Parameter haben die folgenden Bedeutungen:

- *workgroup = example*
Hier wird der NetBIOS-Name der Domäne angegeben. Auch als Mitglied im AD heißt der Parameter *workgroup*.
- *realm = EXAMPLE.NET*
Bei dem *realm* handelt es sich um die Information für die Kerberos-Domäne. Für diesen Realm wird sich der Samba-Server einen KDC suchen.
- *security = ADS*
Damit legen Sie fest, dass Ihr Server ein Mitglied in einer AD-Domäne ist.
- *winbind refresh tickets = yes*
Mit diesem Parameter werden Kerberos-Tickets automatisch erneuert, wenn der Benutzer angemeldet ist und das Ticket abläuft.
- *winbind use default domain = yes* Wenn Sie sich die Benutzer mit `wbinfo -u` anzeigen lassen, werden die Benutzer immer mit dem Domänennamen vorangestellt angezeigt. Wenn Sie nur eine Domäne haben, ohne jegliche Vertrauensstellungen zu anderen Domänen, können Sie über diesen Parameter dafür sorgen, dass der Benutzername ohne den Domänennamen aufgelistet wird. Das hat den Vorteil, dass Sie auch nur mit dem Benutzernamen bei der Vergabe der Berechtigungen arbeiten können. Das gilt natürlich auch für die Gruppen aus Ihrer Domäne.
- *template shell = /bin/bash*
Diesen Parameter dürfen Sie auf gar keinen Fall vergessen. Ohne ihn kann sich ein Benutzer aus dem AD zwar anmelden, aber er wird sofort wieder abgemeldet, da der Benutzer im AD keine Shell zugewiesen bekommt, diese aber für eine erfolgreiche Anmeldung benötigt wird.
- *idmap config * : range = 10000 - 19999*
Neben den Gruppen und Benutzern, die Sie als Administrator anlegen, gibt es noch die Built-in-Groups. Diese Gruppen haben eine eigene verkürzte SID. Für diese Gruppen müssen Sie auch das ID-Mapping konfigurieren. Die Konfiguration der Built-in-Groups über den Stern ist *idmap config * : range = 1000000 - 1999999*. Den Parameter *idmap config * : backend = tdb* müssten Sie eigentlich auch noch konfigurieren, aber dieser Parameter wird von Samba4 automatisch gesetzt. Testen können Sie das mit dem Kommando *testparm*.
- *idmap config EXAMPLE : backend = rid*
Die IDs der Benutzer müssen aus den SIDs der AD-Benutzer generiert werden. Dazu gibt es verschiedene Möglichkeiten. Die Standardeinstellung für den *winbind* ist die Verwendung von *.tdb*-Dateien. Dabei werden zufällige UIDs generiert und den Benutzern zugewiesen und in der *.tdb*-Datei gespeichert. Der Nachteil dieses Verfahrens ist, dass so jeder Benutzer auf jedem Linux-System eine andere UID bekommt. Durch den Wechsel auf das Backend *idmap_rid* wird immer der RID des Benutzers aus der AD-Domäne gewählt. Da dieser eindeutig ist, ist

die ID der Benutzer und Gruppen auf dem Linux-System auch eindeutig. Der Benutzer hat dadurch auf allen Linux-Systemen in der gesamten Domäne immer dieselbe UID. Ein Problem bekommen Sie so aber nicht in den Griff, und zwar werden auf den DCs Ihrer Domäne die UIDs immer im AD verwaltet und somit immer anders als auf den anderen Systemen in der Domäne. Am einfachsten umgeht man dieses Problem, indem man die Domaincontroller nicht als Fileserver verwendet und alle Dateien immer auf anderen Samba-Servern in der Domäne ablegt.

- *idmap config EXAMPLE : = 1000000 - 1999999*

Hier legen Sie den Bereich fest, in dem sich die UIDs der Benutzer befinden sollen.

12.2 Aufnehmen des Clients in die Domäne

Jetzt ist es soweit, der Client kann in die Domäne aufgenommen werden. Für das Aufnehmen in die Domäne benötigen Sie ein Benutzerkonto in der Domäne und der Benutzer muss Mitglied in der Gruppe *domain admins* sein. In Listing 12.2.1 sehen Sie das Kommando, die dazugehörigen Ausgaben und den Test, ob das Aufnehmen erfolgreich war:

```
root@fs-01:~# net ads join -U administrator
Password for [EXAMPLE\administrator]:
Using short domain name -- EXAMPLE
Joined 'FS-01' to dns domain 'example.net'
```

```
root@fs-01:~# net ads testjoin
Join is OK
```

```
root@fs-01:~# host fs-01
fs-01.example.net has address 192.168.56.51
```

Listing 12.2.1: Aufnahme des Clients

Damit haben Sie den ersten Client in die Domäne aufgenommen. um alle Dienste korrekt starten zu lassen, ist es am einfachsten, wenn Sie den Client neu starten. Eine Anpassung der Dienste, wie auf den Domaincontrollern, ist hier nicht notwendig.

Testen sie jetzt, ob alle Benutzer und Gruppen aus der Domäne, auch gefunden werden. Nutzen Sie hierzu das Kommando `wbinfo -u` und `wbinfo -g`. Alle Benutzer und Gruppen werden jetzt angezeigt.

Versuchen Sie aber einem Benutzer oder ein Gruppe auf dem Client Rechte im Dateisystem zu geben, schlägt das noch fehl. Die lokale Benutzerverwaltung kennt die Benutzer und Gruppen der Domäne noch nicht, dafür benötigen Sie noch die Anpassung aus Listing 12.2.2 in der Datei `/etc/nsswitch.conf`:

```
root@fs-01:~# host fs-01
fs-01.example.net has address 192.168.56.51
```

Listing 12.2.2: Anpassungen an der nsswitch.conf

HINWEIS! ©

Bei manchen Distributionen wird die Anpassung durch das hinzufügen zur Domäne bereits automatisch durchgeführt.

Jetzt können Sie die Benutzer und Gruppen zur Vergabe von Berechtigungen nutzen, auch das Kommando `getent passwd <Benutzername>`, zeigt Ihnen jetzt den Benutzer im `passwd`-Format an.

Damit ist der Client nun Mitglied der Domäne.

13 Der Fileserver

Was macht einen Linux-Client zum Fileserver? Nur die Bereitstellung von Freigaben. Nachdem Sie den Linux-Client *fs01* zur Domäne hinzugefügt haben, können Sie jetzt die Freigaben einrichten. Die Freigaben sollen später auf einem Windows-Client nutzbar sein und zwar so, dass der Anwender keinen Unterschied zu einem Windows-Fileserver bemerkt. Das Verhalten beim Anlegen und Bearbeiten von Dateien und Verzeichnissen soll identisch sein. Die Verwaltung der Dateisystemrechte soll genau den auf einem Windows-Fileserver entsprechen.

Um genau das zu erreichen, ist es wichtig, möglichst viele Aufgaben direkt unter Windows durchzuführen, vor allen Dingen, die Vergabe von Berechtigungen.

13.1 Die administrative Freigabe

Die erste Freigabe die Sie einrichten, sollte immer eine administrative Freigabe sein. In dieser Freigabe werden dann, unter Windows, die Verzeichnisse für die Anwender eingerichtet und mit Rechten versehen. Dann werden die dazugehörigen Freigaben angelegt, die dann von den Anwendern genutzt werden. So stellen Sie sicher, dass alle Berechtigungen exakt identisch sind mit denen auf einem Windows-Server.

Einrichten der administrativen Freigabe

Für die Freigabe legen Sie das Verzeichnis */admin* an und setzen Sie die besitzende Gruppe auf *domain admins* und die Rechte auf *775*.

Alle Freigaben werden in der *smb.conf* eingetragen. Auch die Aktivierung der Windows-konformen Berechtigungen werden hier eingestellt. In Listing 13.1.1 sehen Sie die geänderte *smb.conf*:

```
[global]
    workgroup = EXAMPLE
    realm = EXAMPLE.NET
    security = ADS
    winbind refresh tickets = Yes
    winbind use default domain = yes
    template shell = /bin/bash
    idmap config * : range = 10000 - 19999
    idmap config EXAMPLE : backend = rid
    idmap config EXAMPLE : range = 10000000 - 19999999
    interfaces = 192.168.56.51
    bind interfaces only = yes
    vfs objects = acl_xattr
    inherit acls = yes
    acl group control = yes
    inherit owner = windows and unix

[admin-share]
    path=/admin
    read only = no
    browsable = no
    administrative share = yes
```

Listing 13.1.1: Die administrative Freigabe

Im Abschnitt *global* sind vier neue Parameter hinzugekommen:

- *vfs objects = acl_xattr*

Die Option sorgt dafür, dass die Windows-konformen Berechtigungen gesetzt werden können und das Verhalten dem eines Windows-Server entspricht. Dazu gehört auch, dass der *Administrator*, auf einen Ordner, an dem er keine Berechtigung hat nicht zugreifen kann.

- *inherit acls = yes*
Durch diese Option werden alle ACLs immer auch auf alle Unterordner vererbt.
- *acl group control = yes*
Unter Linux kann nur der besitzende Benutzer Rechte ändern, unter Windows hingegen kann das auch eine Gruppe wenn sie Besitzer eines Eintrag ist. Mit diesem Parameter sorgt Samba dafür, dass das in einer Freigabe auch möglich ist.
- *inherit owner = windows and linux*
Mit diesem Parameter sorgen Sie dafür, dass sowohl der SID des Windows-Benutzer als auch die UID des Linux-Benutzer als Besitzer eingetragen werden und diese Informationen auch auf neue Einträge übertragen werden.

HINWEIS! ©

Die vier Parameter können Sie auch in jede Freigabe einzeln schreiben, dann können Sie die Behandlung der Berechtigungen in den Freigaben unterschiedlich einrichten. Wenn Sie die Parameter im globalen Bereich der **smb.conf** eintragen, gelten die Werte für alle Freigaben.

Das sind die einzigen Schritte die Sie direkt auf dem Samba-Server vornehmen, alle weiteren Verzeichnisse, die Sie anschließend freigeben wollen, erstellen Sie unter Windows, in der Adminfreigabe, und vergeben auch dort die Rechte. Nur dieser Weg sorgt dafür, dass die Berechtigungen denen eines Windows-Servers entsprechen.

Jeder weitere Freigabe zeigt jetzt immer auf ein Verzeichnis innerhalb der administrativen Freigabe, das unter Windows angelegt und mit Rechten versehen wurde. Aus diesem Grunde können Sie die Einträge in der **smb.conf** immer identisch halten. In Listing 13.1.2 sehen Sie den Ausschnitt aus der **smb.conf** für eine zusätzliche Freigabe:

```
[files]
    path=/admin/files
    read only = no
    browsable = no
```

Listing 13.1.2: Zusätzliche Freigabe

Benutzer können sich jetzt mit der Freigabe verbinden. Sie können Freigaben auch über GPOs bereitstellen, sodass bei der Anmeldung eines Benutzers die Freigaben automatisch eingebunden werden. Die Verwaltung und Einrichtung von GPOs ist aber nicht mehr Bestandteil dieses Tutorials.

13.2 Basisverzeichnis der Benutzer

Eine zusätzliche Freigabe möchte ich hier noch anlegen und zwar die Freigabe für das *Basisverzeichnis* der Benutzer. Der Grund ist der, dass ich Ihnen im nächsten Abschnitt zeigen will, wie Sie die Freigaben am einfachsten auf einem Linux-Client mounten können.

Das Verzeichnis auf das die Freigabe zeigen soll, soll **/home/EXAMPLE** heißen. Der Grund ist der, dass für den Fall, dass Sie später noch Vertrauensstellungen zu anderen Domänen aufbauen, Sie dann auch für diese Benutzer der anderen Domäne ein Basisverzeichnis bereitstellen können, ohne eventuell auf Namenskonflikte zu stoßen. In Listing 13.2.1 sehen Sie alle dafür erforderlichen Kommandos, inklusive des setzen der Rechte.

```
root@fs-01:~# mkdir /home/EXAMPLE
root@fs-01:~# chgrp "domain users" /home/EXAMPLE/
root@fs-01:~# chmod 775 /home/EXAMPLE/
```

Listing 13.2.1: Erstellen des Basisverzeichnis

HINWEIS! ©

Hier im Tutorial legen Sie die Verzeichnisse für die Benutzer von Hand an. In der Praxis würden Sie diesen Vorgang über eine GPO regeln.

Fehlt nur noch die Freigabe. Den Eintrag für die **smb.conf** sehen Sie in Listing 13.2.2:

```
[users]
    path=/home/EXAMPLE
    read only = no
    browsable = no
```

Listing 13.2.2: Freigabe für das Basisverzeichnis

Legen Sie jetzt noch in dem Verzeichnis `/home/EXAMPLE` ein Verzeichnis für einen Ihrer Benutzer an und geben dem Benutzer alle Rechte an seinem Verzeichnis. Alle Schritte sehen Sie in Listing 13.2.3:

```
root@fs-01:~# getent passwd skania
skania:*:10001109:10000513::/home/EXAMPLE/skania:/bin/bash

root@fs-01:~# mkdir /home/EXAMPLE/skania

root@fs-01:~# chown skania /home/EXAMPLE/skania/

root@fs-01:~# chmod 770 /home/EXAMPLE/skania/
```

Listing 13.2.3: Anlegen des Verzeichnis für einen Benutzer

Damit sind Sie jetzt gut vorbereitet für den letzten Abschnitt des Tutorials.

14 Linux-Client und smb-mount

Da sie jetzt schon die Berechtigungen unter Windows setzen und alle Rechte den Windows-Rechten entsprechen, macht es Sinn, dass Benutzer die eventuell mit Linux-Clients auf den selben Datenbestand zugreifen sollen wie die Windows-Benutzer, einheitlich das SMB-Protokoll nutzen. Denn wenn Sie die Freigaben Ihres Samba-Servers via *CIFS* mounten, werden die Rechte beim Ändern oder anlegen von Einträgen in der Freigabe immer identisch sein. Würden Sie an dieser Stellen jetzt zusätzlich *NFS* einrichten und auf den selben Datenbestand zugreifen, wären die Berechtigungen nicht mehr konsistent.

Wie aber die Verbindung zum Samba-Server herstellen? Am einfachsten ist es, wenn der Linux-Client auch Mitglied im Active Directory ist, dann ist die Nutzung der Freigaben recht einfach zu realisieren.

Eine Problematik ist bei der Nutzung von SMB-Freigaben besonders zu beachten: Für den Zugriff auf eine Freigabe muss eine Authentifizierung durchgeführt werden. Keine gute Lösung ist die, dass in der `fstab` Benutzername und Passwort eingetragen werden. Besser ist es, eine Authentifizierung zu nutzen, die eh schon vorhanden ist, nämlich die Kerberos-Authentifizierung. Denn immer wenn sich ein Benutzer an einer Linux-Maschine anmeldet, die Mitglied der Domäne ist, erhält der Benutzer auch ein Kerberos-Ticket, mit dem er sich authentifizieren kann. Diese Ticket kann dann von *libpam-mount* genutzt werden, dass sich der Benutzer am Fileserver authentifiziert und die Freigabe auch sofort gemountet wird.

14.1 Einrichtung von libpam-mount

Als erstes sorgen Sie dafür, dass die Vagrant-VM *client01* Mitglied der Domäne wird. Eine passende `smb.conf` finden Sie im Verzeichnis `/data` kopieren Sie die Datei in das Verzeichnis `/etc/samba` und nehmen Sie die Maschine in die Domäne auf, genau wie vorher schon den Fileserver. Denken Sie an die Einstellungen für den Resolver.

Das Paket *libpam-mount* ist bereits auf dem Client installiert. Konfiguriert wird *libpam-mount* über die Datei `/etc/security/pam_mount.conf.xml` Wichtig ist der Teil im unteren Bereich. Die benötigten Einträge erstellen Sie vor der Zeile `</pam_mount>` an dieser Stelle soll jetzt die Freigabe `files` und `users` automatisch bei der Anmeldung eines Benutzer gemountet werden. Dazu benötigen Sie die Einträge aus Listing 14.1.1:

```

<volume
    fstype="cifs"
    server="fs-01.example.net"
    path="/users/%(DOMAIN_USER)"
    mountpoint="/home/EXAMPLE/%(DOMAIN_USER)"
    sgrp="domain users"
    options="nodev,nosuid,sec=krb5,user=%(USER),cuid=%(USERUID),\
        workgroup=EXAMPLE,vers=3.1.1" />

<volume
    fstype="cifs"
    server="fs-01.example.net"
    path="/files"
    mountpoint="/files"
    sgrp="domain users"
    options="nodev,nosuid,sec=krb5,user=%(USER),cuid=%(USERUID),\
        workgroup=EXAMPLE,vers=3.1.1" />

```

Listing 14.1.1: Einträge in der Datei `pam_mount.conf.xml`

Die Parameter haben dabei die folgenden Bedeutungen:

- `user="%(DOMAIN_USER)"`
Durch den Parameter `user` beschränken Sie die Verfügbarkeit der Freigabe auf bestimmte Benutzer -- in diesem Fall auf alle Benutzer der Domäne.
- `"fstype="cifs"`
Hier wird der Dateisystemtyp festgelegt -- in diesem Fall `cifs`.
- `server="fs-01.example.net"`
Bei diesem Parameter geben Sie den Server an, auf dem Sie die Freigabe eingerichtet haben.
- `path="/users%(DOMAIN_USER)"`
Hierbei handelt es sich um die Freigabe und den Pfad innerhalb der Freigabe, der gemountet werden soll. Im ersten Beispiel wird immer das Heimatverzeichnis des entsprechenden Benutzers gemountet. Im zweiten Beispiel wird nur der Name der Freigabe angegeben, da hier die gesamte Freigabe gemountet werden soll.
- `mountpoint="/home/EXAMPLE/%(DOMAIN_USER)"`
Hier geben Sie den Mountpoint auf dem lokalen System an, in den die Freigabe gemountet werden soll.
- `sgrp="domain users"` Der Parameter gibt an, in welcher Gruppe der Benutzer Mitglied sein muss, damit diese Mountoption abgearbeitet wird. Hier haben wir die Gruppe `domain users` angegeben, so wird der Mountpoint für jeden im Active Directory existenten Benutzer angelegt, nicht aber für lokale Benutzer die nur auf dem Client vorhanden sind. So sorgen Sie dafür, dass es beim Anmelden von lokalen Benutzern nicht zu Fehlermeldungen kommt.
- `option="sec=krb5,cuid=%(USERUID),workgroup=EXAMPLE,vers=3.1.1"`
Bei dem Parameter `option` können Sie verschiedene Mountparameter angeben. Über die Option `sec=krb5` legen Sie die Sicherheitsstufe bei der Authentifizierung fest (standardmäßig `ntlmv1`). Da Samba 4 Kerberos bereitstellt, soll hier auch Kerberos für die Authentifizierung verwendet werden. Deshalb wird an dieser Stelle der Parameter `sec=krb5` gesetzt. Zusätzlich wird der Parameter `cuid=%(USERUID)` benötigt. Dieser Parameter sorgt dafür, dass der richtige Benutzer-Realm bei der Kerberos-Authentifizierung übergeben wird. Ohne diesen Parameter schlägt die Kerberos-Authentifizierung fehl. Über die Option `workgroup=EXAMPLE` setzen Sie die Domäne, in der sich der Benutzer befindet.

WICHTIG! ⚠

Vergessen Sie auf gar keinen Fall den Parameter `vers=3.1.1`. Dieser Parameter legt fest, welche SMB-Version für den Zugriff auf die Freigabe verwendet wird. Der Standardwert ist hier SMBv1, diese Version ist unsicher und wird von Samba, in der Grundinstallation, auch nicht mehr unterstützt.

Die komplette Datei finden Sie im Verzeichnis `/data` auf dem Vagrant Host *client01*.

Die *Mountpoints* brauchen Sie nicht anzulegen oder zu löschen, das geschieht automatisch durch die Zeile `<mkmountpoint enable="1" remove="true" >`

TIPP! ☺

Sollte das Mounten nicht funktionieren, können Sie in der Datei `pam_mount.conf.xml` in der Zeile `debug enable="0"` das Debuglevel hochsetzen und dann mit `journalctl -f` im Log sehen wo der Fehler auftritt. Sinnvoll ist hier ein Debuglevel von 3.

Nach der Anmeldung als Domainuser finden Sie die Meldungen aus Listing 14.1.2 wenn Sie das Kommando `mount` eingeben:

```
skania@client-01:~$ mount
...
//fs-01.example.net/users/skania on /home/EXAMPLE/skania type cifs\
(rw,nosuid,nodev,relatime,vers=3.1.1,sec=krb5,cuid=10001109,\
cache=strict,username=skania,domain=EXAMPLE,uid=10001109,forceuid\
gid=10000513,forcegid,addr=192.168.56.51,file_mode=0755,dir_mode=0755\
,soft,nounix,serverino,mapposix,rsize=4194304,wsz=4194304,\
bsize=1048576,echo_interval=60,actimeo=1,user=skania)

//fs-01.example.net/files on /files type cifs\
(rw,nosuid,nodev,relatime,vers=3.1.1,sec=krb5,cuid=10001109,\
cache=strict,username=skania,domain=EXAMPLE,uid=10001109,forceuid\
,gid=10000513,forcegid,addr=192.168.56.51,file_mode=0755,dir_mode=0755\
,soft,nounix,serverino,mapposix,rsize=4194304,wsz=4194304,\
bsize=1048576,echo_interval=60,actimeo=1,user=skania)
```

Listing 14.1.2: Ausgabe des Kommandos "mount"

So können Sie jetzt auf jedem Linux-Client, ob mit oder ohne GUI, die Freigaben des Samba-Servers nutzen.

15 Was geht sonst noch mit Samba?

Alles kann in einem Tag nicht abgehandelt werden, neben den hier angesprochenen Themen wären für den Betrieb einer Domäne noch die folgenden Themen wichtig:

- Verwaltung von GPOs.
- Möglichkeiten der Migration, zum Einen von bestehenden Windows-Domänen und zum Anderen die Migration von alten Samba 3 Domänen.
- Einrichtung von Vertrauensstellungen zu anderen Domänen.
- Disaster recovery um nach einem etwaigen Totalausfall einer Domäne möglichst schnell alle Objekte wiederherstellen zu können.
- Nutzung des Kerberos zur Authentifizierung von Diensten.
- Implementierung von DHCP-Server mit DDNS.
- Einbinden von Netzwerkpapierkörben und Virenschnüggern.
- Verwendung von Clustern mit CTDB.
- Einrichtung von Dateisystem Quotas.
- Servergespeicherte Profile zusammen mit der Ordnerumleitung.
- Eine mögliche Schemaerweiterung.

16 Fazit

Natürlich lässt sich an einem Tag nicht das gesamte Spektrum an Möglichkeiten einer Samba-Domäne abhandeln, aber Sie haben hier einen Überblick über die Möglichkeiten erhalten und sehen, dass die Einrichtung einer Domäne, eines Fileserver und der Clients ohne größere Schwierigkeiten möglich ist. Auch zeigt das Tutorial, dass es für die Anwender keine Rolle spielt, ob sich im Hintergrund eine Samba oder Windows-Domäne befindet.

Index

- acl group control, 24
- acl_xattr, 24

- Basisverzeichnis, 25
- Benutzerverwaltung, 14
- Bind9, 6, 8, 10
- bullseye-backports, 8

- Ceph, 7
- CIFS, 26
- Cron, 21
- crontab, 21
- CTDB, 6, 7
- CUPS, 9

- DNS, 6
- DNS-Server, 6
- Domaincontroller, 6

- Fileserver, 7, 23
- forest, 7
- forwarders, 10
- fqdn, 9
- fsmo, 19

- global Catalog, 6, 7
- GlusterFS, 7
- GPO, 19
- Gruppenrichtlinien, 19
- Gruppenverwaltung, 14

- Heimdal-Kerberos, 7

- inherit owner, 24

- Kerberos, 6, 7
- krb5.conf, 11

- LDAP, 6, 7
- ldap, 13
- ldaps, 13
- libpam-mount, 26
- libpam.mount, 26
- Linux-Client, 21

- MIT-Kerberos, 7
- Mountpoint, 27

- named.conf.local, 10
- named.conf.options, 10
- Nameserver, 15
- NETBIOS-Name, 22
- ntlm, 27
- ntp, 14
- ntp.conf, 14

- pam_mount.conf.xml, 26
- PdcEmulationMasterRole, 19

- Printserver, 7
- provisioning, 9

- realm, 22
- Remote Server Administration Tools, 14
- Resolver, 12, 21
- RSAT, 14
- rsync, 19
- rsync-Server, 19
- rsyncd.conf, 20

- samba-tool, 9, 16
- srv-record, 15
- Subscription, 6
- systemd, 19
- sysvol, 18, 19

- tgt, 13
- tkey-gssapi-keytab, 10