

Samba - Freigaben



Inhaltsverzeichnis

- [Tutorial-Freigabe-Planung](#)
- [Windows Workgroups \(mit Linux\)](#)
- [Samba-Server auf `deb-srv` installieren](#)
- [`nmbd` - und `smbd` -Dienste prüfen](#)
- [Konfigurationsdatei `smb.conf`](#)
- [Freigaben prüfen](#)
- [Samba-Benutzerverwaltung](#)
- [Samba-Benutzer hinzufügen](#)

- Freigaben nochmals prüfen
- Schreibzugriff auf Freigabe einstellen
- Zwei Benutzer-Verwaltungen - Warum?

Tutorial-Freigabe-Planung

In diesem Tutorial wollen wir die Heimatverzeichnisse von Linux-Benutzern auf dem Linux-Server `deb-srv` mit Samba freigeben und später auf dem Linux-Client `debian` und auf dem Windows-Client einbinden.

Dazu muss der Samba-Server auf `deb-srv` und der Samba-Client auf `debian` installiert und konfiguriert werden.

Für die Freigabe der Heimat-Verzeichnisse bringt die Installation des Samba-Servers auch schon eine geeignete Standardkonfiguration `[homes]` mit, die wir nur leicht anpassen müssen.

Außerdem erstellen wir auf `deb-srv` eine weitere explizite, selbst konfigurierte Freigabe `[hermann-data1]`, die später auch auf `debian` und unter Windows eingebunden wird.

Windows Workgroups (mit Linux)

- Windows-Computer in einem Netzwerk können in einer Arbeitsgruppe (Workgroup) organisiert sein.
- Die Arbeitsgruppe ist ein logischer Verbund von Computern, die alle den selben Arbeitsgruppennamen im Netzwerk (über das NetBIOS-Protokoll) propagieren.
- Microsoft implementierte dieses Konzept 1992 in Windows 3.1, Windows 3.11.
- Erst später wurde von Microsoft mit Windows NT das Konzept der Domänen eingeführt. Dieses Konzept bietet eine zentralisierte Benutzerverwaltung und -authentifizierung.

- Das Domänen-Konzept erhielt später den Namen *Active Directory*. Heute ist das *Active Directory* in die Cloud gewandert, hieß zunächst *Microsoft Azure Active Directory* und firmiert heute unter dem Namen *Entra ID*.
- Um einer Domäne anzugehören, muss ein Computer aktiv "der Domäne beitreten".
- Ein Windows-10/11-Computer, der keiner Domäne angehört, ist auch heute noch standardmäßig in der Arbeitsgruppe **WORKGROUP** organisiert.
- Der Arbeitsgruppenname lässt sich ändern.

- Anfang der 90er Jahre begann Andrew Tridgell mit der Entwicklung von Samba und musste, um mit der Windows-Welt kompatibel zu sein, auch das Workgroup-Konzept von Windows implementieren.
- Heute kann ein Linux-Computer auch einer Domäne beitreten oder sogar die Rolle eines Domänen-Controllers übernehmen.
- Standardmäßig ist auch ein Linux-Computer mit Samba in der Arbeitsgruppe `WORKGROUP` organisiert.
- In der Konfigurationsdatei `/etc/samba/smb.conf` steht der Eintrag `workgroup = WORKGROUP`.

- Der Arbeitsgruppenname lässt sich ändern. Er sollte dem Arbeitsgruppennamen der anderen Computer im Netzwerk-Verbund entsprechen.
- In diesem Tutorial arbeiten wir ausschließlich mit dem Workgroup-Konzept und verwenden den Standard-Arbeitsgruppennamen **WORKGROUP**.

Samba-Server auf **deb-srv** installieren

```
hermann@deb-srv:~$ sudo apt update && sudo apt install -y samba
```

Die Installation des Samba-Servers besteht aus zwei Server-Diensten:

- **nmbd** - Der NetBIOS-Name-Service Daemon sorgt für die Namensauflösung in SMB-Netzwerken (entfernt vergleichbar mit DNS).
- **smbd** - Der SMB-Server-Daemon ist der eigentliche Datei- und Druckdienst, der die Freigaben an die SMB/CIFS-Clients bereitstellt.

nmbd - und **smbd** -Dienste prüfen

Prozesse

```
hermann@deb-srv:~$ ps -ef | grep nmbd | grep -v grep
root    557    1    0 21:37 ?      00:00:00 /usr/sbin/nmbd --foreground --no-process-group
```

```
hermann@deb-srv:~$ ps -ef | grep smbd | grep -v grep
root    567    1    0 21:37 ?      00:00:00 /usr/sbin/smbd --foreground --no-process-group
root    571  567    0 21:37 ?      00:00:00 /usr/sbin/smbd --foreground --no-process-group
root    572  567    0 21:37 ?      00:00:00 /usr/sbin/smbd --foreground --no-process-group
```

Ports von `nmbd` - und `smbd`

- `nmbd` lauscht auf den UDP-Ports **137** und **138**.
- `smbd` lauscht auf den TCP-Ports **139** und **445**.

Das zeigt das Kommando `netstat` mit den Optionen -tulpn``

- `-t`: TCP
- `-u`: UDP
- `-l`: nur lauschende (listening) Ports
- `-p`: Prozess-ID und -Name
- `-n`: numerische IP-Adressen statt Hostnamen

```

hermann@deb-srv:~$ sudo netstat -tulpn
[sudo] Passwort für hermann:
Aktive Internetverbindungen (Nur Server)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:445	0.0.0.0:*	LISTEN	1074/smbd
tcp	0	0	0.0.0.0:139	0.0.0.0:*	LISTEN	1074/smbd
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	550/sshd: /usr/sbin
tcp6	0	0	:::445	:::*	LISTEN	1074/smbd
tcp6	0	0	:::139	:::*	LISTEN	1074/smbd
tcp6	0	0	:::22	:::*	LISTEN	550/sshd: /usr/sbin
udp	0	0	0.0.0.0:68	0.0.0.0:*		510/dhclient
udp	0	0	172.21.79.255:137	0.0.0.0:*		1062/nmbd
udp	0	0	172.21.64.14:137	0.0.0.0:*		1062/nmbd
udp	0	0	0.0.0.0:137	0.0.0.0:*		1062/nmbd
udp	0	0	172.21.79.255:138	0.0.0.0:*		1062/nmbd
udp	0	0	172.21.64.14:138	0.0.0.0:*		1062/nmbd
udp	0	0	0.0.0.0:138	0.0.0.0:*		1062/nmbd

Systemd-Dienst **nmbd** - Status

```
hermann@deb-srv:~$ sudo systemctl status nmbd
● nmbd.service - Samba NMB Daemon
   Loaded: loaded (/lib/systemd/system/nmbd.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-12-28 21:37:25 CET; 1min 49s ago
     Docs: man:nmbd(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 546 ExecCondition=/usr/share/samba/is-configured nmb (code=exited, status=0/SUCCESS)
 Main PID: 557 (nmbd)
    Status: "nmbd: ready to serve connections..."
     Tasks: 1 (limit: 1028)
    Memory: 14.3M
       CPU: 124ms
    CGroup: /system.slice/nmbd.service
            └─557 /usr/sbin/nmbd --foreground --no-process-group

...

Dez 28 21:37:25 deb-srv systemd[1]: Starting nmbd.service - Samba NMB Daemon...
Dez 28 21:37:25 deb-srv systemd[1]: Started nmbd.service - Samba NMB Daemon.
```

Systemd-Dienst **smbd** - Status

```
hermann@deb-srv:~$ sudo systemctl status smbd
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-12-28 21:37:25 CET; 20min ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 558 ExecCondition=/usr/share/samba/is-configured smb (code=exited, status=0/SUCCESS)
  Process: 560 ExecStartPre=/usr/share/samba/update-apparmor-samba-profile (code=exited, status=0/SUCCESS)
 Main PID: 567 (smbd)
    Status: "smbd: ready to serve connections..."
     Tasks: 3 (limit: 1028)
  Memory: 11.0M
     CPU: 120ms
    CGroup: /system.slice/smbd.service
            └─567 /usr/sbin/smbd --foreground --no-process-group
            └─571 /usr/sbin/smbd --foreground --no-process-group
            └─572 /usr/sbin/smbd --foreground --no-process-group

Dez 28 21:37:25 deb-srv systemd[1]: Starting smbd.service - Samba SMB Daemon...
Dez 28 21:37:25 deb-srv systemd[1]: Started smbd.service - Samba SMB Daemon.
```

Konfigurationsdatei `smb.conf`

Die Installation des Samba-Servers bringt eine Standardkonfiguration mit in der Datei `/etc/samba/smb.conf`.

Diese Datei enthält neben ausführlichen Kommentaren und anderen Abschnitten auch den Abschnitt `[homes]`, der die Freigabe der Home-Verzeichnisse der Benutzer regelt.

Das Kommando `testparm` prüft `smb.conf` auf syntaktische und semantische Korrektheit und gibt die Konfiguration (ohne Kommentare) auf der Standardausgabe aus. (Die Option `-s` erspart uns einen weiteren Druck auf die Eingabetaste.)


```
hermann@deb-srv:~$ testparm -s
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Server role: ROLE_STANDALONE

...
[global]
    log file = /var/log/samba/log.%m
    logging = file
    map to guest = Bad User
    max log size = 1000
    obey pam restrictions = Yes
    pam password change = Yes
    panic action = /usr/share/samba/panic-action %d
    passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spass...
    passwd program = /usr/bin/passwd %u
    server role = standalone server
    unix password sync = Yes
    usershare allow guests = Yes
    idmap config * : backend = tdb
```

```
[homes]
  comment = Home Directories
  browseable = no
  read only = yes
  create mask = 0700
  directory mask = 0700
  valid users = %S
[printers]
  ...
[print$]
  ...
```

- Die Heimatverzeichnisse der Benutzer werden bereits freigegeben, sind aber (auf dem Client) nicht sichtbar (`browseable = no`) und nur lesbar (`read only = yes`).

- Die Berechtigungen für die Erstellung von Dateien und Verzeichnissen sind auf `0700` gesetzt (`create mask = 0700` und `directory mask = 0700`). Damit erhalten neue Dateien und Verzeichnisse die Berechtigungen `rwX-----`.
- Der Eintrag `valid users = %S` sorgt dafür, dass ein Benutzer auf dem Client nur auf die Freigabe des Heimatverzeichnisses des gleichnamigen Benutzers auf dem Server zugreifen kann.
- Dazu muss der Benutzer auf dem Server in der Samba-Benutzerdatenbank eingetragen sein.

Freigaben prüfen

Freigaben auf Samba-Server **deb-srv** prüfen

```
hermann@deb-srv:~$ net rpc share list -U hermann%ibb --long
```

```
Enumerating shared resources (exports) on remote server:
```

Share name	Type	Description
-----	----	-----
print\$	Disk	Printer Drivers
IPC\$	IPC	IPC Service (Samba 4.17.12-Debian)
nobody	Disk	Home Directories

Freigaben auf Samba-Client **debian** prüfen

```
hermann@deb-srv:~$ ssh hermann@debian 'smbclient -L deb-srv -U hermann%ibb'
```

Sharename	Type	Comment
-----	----	-----
print\$	Disk	Printer Drivers
IPC\$	IPC	IPC Service (Samba 4.17.12-Debian)
nobody	Disk	Home Directories

```
SMB1 disabled -- no workgroup available
```

Damit das Kommando **smbclient** auf dem Client **debian** aufgerufen werden kann, muss das Paket **smbclient** auf **debian** installiert sein.

- Wir erhalten (abgesehen von der Formatierung) die gleiche Ausgabe auf dem Server und auf dem Client.
- Der Server `deb-srv` zeigt mit dem Kommando `net rpc share list` die Freigaben genau so an, wie sie auf dem Client mit `smbclient -L deb-srv` erscheinen.
- Der Freigabename `nobody` besagt, dass die Freigabe für den Benutzer *hermann* auf dem Server `deb-srv` nicht zur Verfügung steht. Damit der Benutzer *hermann* die Freigabe nutzen kann, muss er auf dem Server in der Samba-Benutzerdatenbank eingetragen sein.

Samba-Benutzerverwaltung

Samba-Benutzerdatenbank

Die Samba-Benutzerdatenbank ist eine separate Datenbank, die die Benutzerdaten für den Zugriff auf die Samba-Freigaben - insbesondere Benutzername und Passwort - enthält. Diese wird standardmäßig in `/var/lib/samba/private/{passdb,secrets}.tdb` im neuen Format gespeichert.

```
hermann@deb-srv:~$ ls -l /var/lib/samba/private/{passdb,secrets}.tdb
-rw----- 1 root root 421888 27. Dez 05:27 /var/lib/samba/private/passdb.tdb
-rw----- 1 root root 430080 26. Dez 23:09 /var/lib/samba/private/secrets.tdb
```

- Um die Benutzer im klassischen Unix-Format zu speichern, kann die Samba-Benutzerdatenbank auch in `/etc/samba/smbpasswd` gespeichert werden. Dazu muss in der Konfigurationsdatei `/etc/samba/smb.conf` der Eintrag `passdb backend = tdbsam` durch `passdb backend = smbpasswd` ersetzt werden.
- Eintrag `passdb backend = tdbsam` ist der Standardwert und muss nicht explizit in `smb.conf` eingetragen sein.
- Als Benutzerdatenbank-Backend kann auch LDAP verwendet werden: `passdb backend = ldapsam:ldap://ldap.example.com`.

Kommandos zur Samba-Benutzerverwaltung

- `smbpasswd` - Kommandozeilenprogramm zur Verwaltung der Samba-Benutzerdatenbank. Hier die wichtigsten Optionen:
 - `smbpasswd -a <username>` - Benutzer hinzufügen und Passwort setzen
 - `smbpasswd -x <username>` - Benutzer löschen
 - `smbpasswd -d <username>` - Benutzer sperren (disable)
 - `smbpasswd -e <username>` - Benutzer entsperren (enable)
 - `smbpasswd <username>` - Benutzer-Passwort ändern

- `pdbedit` - Kommandozeilenprogramm zur Anzeige und Verwaltung der Samba-Benutzerdatenbank. Damit können Benutzer hinzugefügt, gelöscht oder geändert werden. Es können sehr vielfältige Benutzerattribute gesetzt oder geändert werden.
 - `pdbedit -L` - Listet alle Benutzer in der Samba-Benutzerdatenbank auf.
 - `pdbedit -L -v` - Listet alle Benutzer in der Samba-Benutzerdatenbank mit ausführlichen Informationen auf.
 - `pdbedit` hat viele weitere Optionen.

Samba-Benutzer hinzufügen

```
hermann@deb-srv:~$ sudo pdbedit -L # no user -> empty luser ist
```

```
hermann@deb-srv:~$ sudo smbpasswd -a hermann # add SMB user 'hermann'  
New SMB password:  
Retype new SMB password:  
Added user hermann.
```

```
hermann@deb-srv:~$ sudo pdbedit -L # 'hermann' is 1st Samba user  
hermann:1000:Hermann Hueck
```

```
hermann@deb-srv:~$ sudo pdbedit -L -v # verbose user info
-----
Unix username:      hermann
NT username:
Account Flags:      [U          ]
User SID:           S-1-5-21-2646715940-2823984399-3845545356-1001
Primary Group SID:  S-1-5-21-2646715940-2823984399-3845545356-513
Full Name:          Hermann Hueck
Home Directory:     \\DEB-SRV\hermann
HomeDir Drive:
Logon Script:
Profile Path:       \\DEB-SRV\hermann\profile
Domain:             DEB-SRV
Account desc:
Workstations:
Munged dial:
Logon time:         0
Logoff time:        Mi, 06 Feb 2036 16:06:39 CET
Kickoff time:       Mi, 06 Feb 2036 16:06:39 CET
Password last set:  Sa, 28 Dez 2024 22:50:42 CET
Password can change: Sa, 28 Dez 2024 22:50:42 CET
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours        : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Freigaben nochmals prüfen

```
hermann@deb-srv:~$ net rpc share list -U hermann%ibb --long
```

Enumerating shared resources (exports) on remote server:

Share name	Type	Description
-----	----	-----
print\$	Disk	Printer Drivers
IPC\$	IPC	IPC Service (Samba 4.17.12-Debian)
hermann	Disk	Home Directories

```
hermann@deb-srv:~$ ssh hermann@debian 'smbclient -L deb-srv -U hermann%ibb'
```

Sharename	Type	Comment
-----	----	-----
print\$	Disk	Printer Drivers
IPC\$	IPC	IPC Service (Samba 4.17.12-Debian)
hermann	Disk	Home Directories

```
SMB1 disabled -- no workgroup available
```

- Auf `deb-srv` ist der Benutzer *hermann* in der Samba-Benutzerdatenbank eingetragen und kann auf die gleichnamige Freigabe seines Heimatverzeichnis zugreifen. Der Freigabename `nobody` wurde durch `hermann` ersetzt.

Schreibzugriff auf Freigabe einstellen

- Bevor wir Änderungen vornehmen, sichern wir die Konfigurationsdatei `/etc/samba/smb.conf` in `/etc/samba/smb.conf.org`.
- Bis jetzt ist die Freigabe `[homes]` nur lesbar. Die Änderung des Eintrags `read only = yes` in `read only = no` erlaubt den Schreibzugriff auf die Freigabe.
- Nach der Änderung prüfen wir `smb.conf` mit `testparm -s`.
- Nach der Änderung muss der Dämon `smbd` neu gestartet werden. Dabei wird die Konfigurationsdatei neu eingelesen.

```
hermann@deb-srv:~$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.org
hermann@deb-srv:~$ sudo -e /etc/samba/smb.conf
hermann@deb-srv:~$ testparm -s # home shares are now writable
...
[global]
    workgroup = WORKGROUP
    ...
[homes]
    comment = Home Directories
    browseable = no
    # make homes shares writable
    read only = no
    create mask = 0700
    directory mask = 0700
    valid users = %S
[printers]
    ...
```


- Nach Änderung von `smb.conf` `nmbd` und `smbd` neu starten.

```
hermann@deb-srv:~$ sudo systemctl restart nmbd smbd
```

In diesem Fall wäre es ausreichend, nur den `smbd`-Dienst neu zu starten, da die Änderung nur die Freigabe `[homes]` betrifft.

```
hermann@deb-srv:~$ sudo systemctl status smbd
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-12-28 23:17:11 CET; 3s ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 932 ExecCondition=/usr/share/samba/is-configured smb (code=exited, status=0/SUCCESS)
  Process: 936 ExecStartPre=/usr/share/samba/update-apparmor-samba-profile (code=exited, status=0/SUCCESS)
 Main PID: 945 (smbd)
    Status: "smbd: ready to serve connections..."
     Tasks: 3 (limit: 1028)
    Memory: 5.6M
       CPU: 98ms
    CGroup: /system.slice/smbd.service
            └─945 /usr/sbin/smbd --foreground --no-process-group
              └─947 /usr/sbin/smbd --foreground --no-process-group
                └─948 /usr/sbin/smbd --foreground --no-process-group

Dez 28 23:17:11 deb-srv systemd[1]: Starting smbd.service - Samba SMB Daemon...
Dez 28 23:17:11 deb-srv systemd[1]: Started smbd.service - Samba SMB Daemon.
```

Zwei Benutzer-Verwaltungen - Warum?

Mit der Installation von Samba haben wir zwei Benutzer-Verwaltungen auf dem System:

- die reguläre Linux-Benutzer-Verwaltung (`/etc/passwd`, `/etc/shadow`, `/etc/group`)
- die Samba-Benutzer-Verwaltung.

Für die Administration scheint das auf den ersten Blick unpraktisch, wenn derselbe Benutzer in zwei Datenbanken gepflegt werden muss.

Für die separaten Benutzerverwaltungen gibt es jedoch gute Gründe:

- Die Samba-Benutzerverwaltung ist speziell auf die Anforderungen des SMB/CIFS-Protokolls zugeschnitten und ist kompatibel mit der Benutzerverwaltung von Windows-Systemen (nicht mit der Unix/Linux-Benutzerverwaltung).
- Aus diesem Grund unterscheiden sich die Benutzerdatenbanken in der Struktur und den Inhalten, z.B. auch die Algorithmen zur Verschlüsselung der Passwörter.
- Die Linux-Benutzerverwaltung ist viel umfangreicher. Sie enthält auch Systembenutzer, die für den Betrieb des Systems notwendig sind und nicht für den Zugriff auf Samba-Freigaben.

Password-Synchronisation

Die Synchronisation der Passwörter zwischen den beiden Benutzerdatenbanken ist möglich - aber nur in eine Richtung.

```
[global]
...
unix password sync = Yes
passwd program = /usr/bin/passwd %u
...
```

- Ist `unix password sync = Yes` gesetzt, wird das Passwort eines Benutzers in der Samba-Benutzerdatenbank automatisch mit dem Passwort des Benutzers in der Linux-Benutzerdatenbank synchronisiert, wenn der Benutzer sein SMB-Passwort ändert.
- In diesem Fall muss auch der Parameter `passwd program` gesetzt werden. Dabei ist der absolute Pfad zum Linux-Passwort-Änderungsprogramm anzugeben. `%u` ist ein Platzhalter für den Benutzernamen. Dieses Programm wird bei der Änderung des SMB-Passworts aufgerufen, um auch das Linux-Passwort zu ändern: `passwd program = /usr/bin/passwd %u`.

Freigabe `[hermann-data1]` erstellen

- Die virtuelle Freigabe `[homes]` ist **EIN** Freigabe-Eintrag für viele Benutzer. Die Freigabe des Heimat-Verzeichnisses wird automatisch für jeden Benutzer erstellt, der in der Samba-Benutzerdatenbank eingetragen ist. Sie ist auf das Heimatverzeichnis des Benutzers gemappt und nur für den jeweiligen Benutzer sichtbar und zugreifbar.
- Nun erstellen wir eine explizite Freigabe `hermann-data1` für das Verzeichnis `/data1/users/hermann` auf `deb-srv`. Die Freigabe soll für den Benutzer `hermann` lesbar und schreibbar sein.

```
hermann@deb-srv:~$ sudo -e /etc/samba/smb.conf
```

```
# smb.conf
[hermann-data1]
    comment = Hermanns Data (1)
    path = /data1/users/hermann
    browseable = yes
    read only = no
    create mask = 0640
    directory mask = 0750
    valid users = hermann
```

```
hermann@deb-srv:~$ testparm -s # check smb.conf for syntax errors
```

```
hermann@deb-srv:~$ sudo systemctl restart smbd # restart smbd to apply changes
```


Freigaben auf dem SMB-Server anzeigen

```
hermann@deb-srv:~$ net rpc share list -U hermann%ibb --long
```

Enumerating shared resources (exports) on remote server:

Share name	Type	Description
-----	----	-----
print\$	Disk	Printer Drivers
hermann-data1	Disk	Hermanns Data (1)
IPC\$	IPC	IPC Service (Samba 4.17.12-Debian)
hermann	Disk	Home Directories

Freigaben auf dem SMB-Client anzeigen

```
hermann@debian:~/srv$ smbclient -L deb-srv.mshome.net -U hermann%ibb
```

Sharename	Type	Comment
-----	----	-----
print\$	Disk	Printer Drivers
hermann-data1	Disk	Hermanns Data (1)
IPC\$	IPC	IPC Service (Samba 4.17.12-Debian)
hermann	Disk	Home Directories

```
SMB1 disabled -- no workgroup available
```