

M159 - Directory Services

Thema 2

Arbeitsblatt 5

1 Lernziele

Im AB 5 verfolgen wir folgende Lernziele:

- Sie können auf Linux Shares anlegen und auslesen (lokal und remote)
- Sie wissen, wie man im Profil des Users Heimatverzeichnisse definiert und schaffen auf dem Server die Voraussetzungen
- Sie kennen die Befehle um Verzeichnis-Berechtigungen zu lesen

2 Verwaltung von Shares auf vmls2 über die Registry

Jetzt, da Sie in Ihrem System Benutzer, Gruppen und Fileserver angelegt haben, soll es hier darum gehen, wie Sie Ihren Benutzern Freigaben auf vmls2 bereitstellen können. Die Verwaltung der Freigaben wird hier über die Registry beschrieben.

Freigaben sorgen für die Bereitstellung von Daten für Ihre Benutzer. Für die Benutzer sind die Freigaben die Verbindung zu Ihrer Serverumgebung. Mithilfe von Gruppenrichtlinien weisen Sie die Freigaben Ihren Benutzern direkt bei der Anmeldung mittels bestimmten Laufwerksbuchstaben zu.

Bei der Einrichtung der Freigaben haben Sie verschiedene Möglichkeiten der Konfiguration. In diesem AB werden wir lernen, wie Freigaben im Netzwerk verwaltet werden können.

Wenn Samba 4 mit sehr vielen Clients im Netzwerk eingesetzt wird, sollten Sie die Freigaben nicht mehr in der Datei *smb.conf* verwalten, sondern in der Registry von Samba4. Die Verwaltung der Freigaben in der Registry hat den Vorteil, dass nicht mehr jeder *smbd*-Prozess im System die Datei *smb.conf* neu lesen muss, wenn Sie eine neue Freigabe erstellt haben, denn bei jeder Änderung der *smb.conf* muss jeder *smbd*-Prozess die Datei erneut lesen. Da für jeden angemeldeten Benutzer in der Domäne je ein *smbd*-Prozess gestartet wird, kann die Auslastung des Systems dann sehr hoch werden. Für beide Möglichkeiten der Verwaltung von Freigaben über die Registry stehen Ihnen dieselben Parameter zur Verfügung, wie bei der Konfiguration über die *smb.conf*.

2.1 Erstellen eines Shares

Jetzt soll die erste Freigabe erstellt werden. Wenn Sie eine Freigabe in der Registry anlegen, haben Sie erst einmal nur die Möglichkeit, die Optionen **writable**, **guest_ok** und einen Kommentar zur Freigabe hinzuzufügen. Alle weiteren Parameter lassen sich erst nachträglich eintragen. In folgendem Listing sehen Sie ein Beispiel für das Eintragen einer Freigabe:

```
root@vmls2:~# mkdir -p /daten/reg-share
root@vmls2:~# net conf addshare reg-share /daten/reg-share writeable=y guest_ok=n "Share
in der Registry"
```

Listing 1: Eintragen eines Shares in die Registry auf vmls2

Mit **net conf** verwalten Sie die Konfigurationseinträge der Registry. In diesem Fall soll eine Freigabe *reg-share* hinzugefügt werden. Danach folgen der Pfad zur Freigabe, Angaben dazu, ob auf die Freigabe geschrieben werden darf und ob ein Gastzugriff erlaubt ist, und ein Kommentar. Jetzt können Sie sich die Freigabe anzeigen lassen mit:

```

root@vmls2:~# net registry export hkml\\software\\samba /dev/stdout
Windows Registry Editor Version 5.00

[HKLM\\software\\samba]

[HKLM\\software\\samba\\smbconf]

[HKLM\\software\\samba\\smbconf\\global]
"workgroup"="sam159"
"realm"="SAM159.IET-GIBB.CH"
"security"="ADS"
"winbind enum users"="yes"
"winbind enum groups"="yes"
"winbind use default domain"="yes"
"winbind refresh tickets"="yes"
"template shell"="/bin/bash"
"idmap config * : range"="10000 - 19999"
"idmap config SAM159 : backend"="rid"
"idmap config SAM159 : range"="1000000 - 1999999"
"inherit acls"="yes"
"store dos attributes"="yes"
"vfs objects"="acl_xattr"

[HKLM\\software\\samba\\smbconf\\reg-share]
"path"="/daten/reg-share"
"comment"="Share in der Registry"
"guest ok"="no"
"read only"="no"

[HKLM\\software\\samba\\Group Policy]
;Local Variables:
;coding: UTF-8
;End:

```

Listing 2: Auslesen der Registry um Share anzuzeigen

Selbstverständlich können Sie sich die einzelnen Schlüssel und ihre Werte auch von einem anderen Server aus über das Netzwerk auflisten lassen. Versuchen Sie die Abfrage von `vmLS1` aus mit:

```

root@vmls1:~# net rpc registry enumerate HKLM\\software\\samba\\smbconf\\reg-share -k -S
vmLS2.sam159.iet-gibb.ch
Valuename  = path
Type       = REG_SZ
Value      = "/daten/reg-share"

Valuename  = comment
Type       = REG_SZ
Value      = "Share in der Registry"

Valuename  = guest ok
Type       = REG_SZ
Value      = "no"

Valuename  = read only
Type       = REG_SZ
Value      = "no"

```

Listing 3: Auslesen des shares reg-share übers Netz mit Kerberos-Authentifizierung

2.2 Zugriff auf Share aus der Registry

Wenn Sie jetzt mit dem Kommando `smbclient -L localhost` einen anonymen Zugriff auf den Server durchführen, wird Ihnen die gerade erstellte Freigabe aufgelistet:

```

root@vmls2:~# smbclient -L vmls2
lp_load_ex: changing to config backend registry
Enter SAM159\root's password: sm12345
Anonymous login successful

```

Sharename	Type	Comment
-----	----	-----
IPC\$	IPC	IPC Service (Samba 4.7.6-Ubuntu)
reg-share	Disk	Share in der Registry

```
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful
```

Server	Comment
-----	-----
Workgroup	Master
-----	-----
SAM159	VMLS2

Listing 4: Zugriff auf Share mit `smbclient`

oder mit Kerberos:

```
root@vmls2:~# kinit administrator
administrator@SAM159.IET-GIBB.CH's Password:
root@vmls2:~# smbclient -L vmls2 -k
lp_load_ex: changing to config backend registry

Sharename      Type      Comment
-----
IPC$           IPC       IPC Service (Samba 4.7.6-Ubuntu)
reg-share      Disk      Share in der Registry
Reconnecting with SMB1 for workgroup listing.
```

Server	Comment
-----	-----
Workgroup	Master
-----	-----
SAM159	VMLS2

Listing 5: Zugriff auf Share mit `smbclient` und Kerberos Authentifizierung

2.3 Aufgabe 1

Verbinden Sie sich mit `vmWP1` auf den Share `reg-share`! Können sie auf dem Share schreiben? Warum nicht?

2.4 Freigabe der Home-Verzeichnisse

Damit Sie die Heimatverzeichnisse der Benutzer auf dem Fileserver ablegen können, soll jetzt eine entsprechende Freigabe angelegt werden. Für diese Freigabe müssen Sie spezielle Rechte setzen, um später über die RSAT beim Zuweisen der Heimatverzeichnisse diese auch auf dem entsprechenden Server anlegen zu können.

Samba 4 verwendet als Standard immer das Verzeichnis `/home/<Domainname>` für die Heimatverzeichnisse. Besonders wichtig ist das für die Linux-Clients.

Im folgenden Listing sehen Sie, wie das Verzeichnis angelegt wird. Beachten Sie die Rechte.

```
root@vmls2:~# mkdir /home/SAM159
root@vmls2:~#
root@vmls2:~#
root@vmls2:~# chmod 755 /home/SAM159/
root@vmls2:~#
root@vmls2:~#
root@vmls2:~# chgrp 'SAM159\Domain Admins' /home/SAM159/
root@vmls2:~# chown 'SAM159\administrator' /home/SAM159/
root@vmls2:~#
root@vmls2:~# net conf addshare users /home/SAM159 writeable=y guest_ok=n "Home-Dirs"
root@vmls2:~#
root@vmls2:~#
root@vmls2:~# net conf setparm users "browsable" "no"
root@vmls2:~#
root@vmls2:~#
root@vmls2:~# net conf setparm users "create mask" "700"
root@vmls2:~#
root@vmls2:~#
```

```
root@vmls2:~# net conf setparm users "directory mask" "700"
```

Listing 6: Anlegen des shares für die Home-Verzeichnisse

Die Freigabe können sie sich anzeigen lassen:

```
root@vmls2:~# net rpc registry enumerate HKLM\\software\\samba\\smbconf\\users\\ -k -S
vmls2.sam159.iet-gibb.ch
Enter administrator's password:
Valuename = path
Type      = REG_SZ
Value     = "/home/SAM159"

Valuename = comment
Type      = REG_SZ
Value     = "Home-Dirs"

Valuename = guest ok
Type      = REG_SZ
Value     = "no"

Valuename = read only
Type      = REG_SZ
Value     = "no"

Valuename = browseable
Type      = REG_SZ
Value     = "no"

Valuename = create mask
Type      = REG_SZ
Value     = "700"

Valuename = directory mask
Type      = REG_SZ
Value     = "700"
```

Listing 7: Anzeigen des Shares für die Home-Verzeichnisse

Jetzt können Sie mit RSAT für einen bestehenden Benutzer ein Heimatverzeichnis anlegen. Meldet sich ein Benutzer an einem Client in der Domäne an, wird ihm automatisch ein Laufwerksbuchstabe mit seinem Heimatverzeichnis bereitgestellt.

2.5 Aufgabe 2

Setzen sie für einen Benutzer das Heimatverzeichnis. Verwenden Sie dazu die RSAT-Tools! Diese erstellen das Verzeichnis automatisch. Die RSAT-Tools müssen sie mit dem administrator starten.

2.6 Aufgabe 3

Wie sind die Berechtigungen des Home-Verzeichnisses gesetzt?

2.7 Aufgabe 4

Melden sie sich mit dem User an und kontrollieren Sie, ob das Home-Verzeichnis eingebunden ist. Siehe Abbildung.

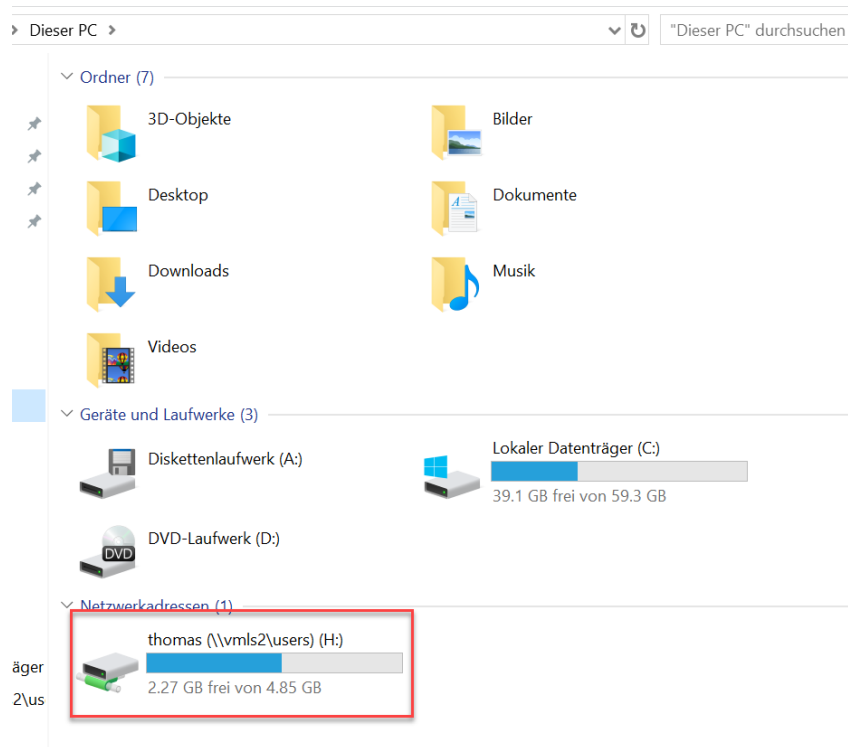


Abbildung 1: Homeverzeichnis wird automatisch eingebunden

2.8 Aufgabe 5

Betrachten Sie mit dem Kommando `getfacl` die ACL's des Heimatverzeichnisses. `getfacl` erhalten sie mit `sudo apt install acl`. Die ACL's wurden von RSAT automatisch vergeben und sind komplex. Es ist deshalb keine gute Idee, die Heimatverzeichnisse auf der Konsole von Hand zu erstellen.

Sie sollten die Verzeichnisse IMMER durch RSAT anlegen lassen.

Betrachten Sie unter Windows die Eigenschaften des Heimatverzeichnisses! Wie sehen diese aus?