

M159 - Directory Services

Thema 2

Arbeitsblatt 6

1 Lernziele

Im AB 6 verfolgen wir folgende Lernziele:

- Sie können allgemeine Freigaben auf dem Linux-Samba-Fileserver über Windows verwalten
- Sie kennen den Trick, um mit einem administrativen Share, weitere Shares mit entsprechenden Berechtigungen anzulegen
- Sie verwenden *Regedit*, um Parameter für Shares zu definieren
- Sie verstehen den Parameter `hide unreadable = yes` und können diesen im Rahmen einer praktischen Aufgabe anwenden
- Sie können einer 9-seitigen Anleitung folgen und halten stets die Übersicht, worum es hier geht

2 Allgemeine Shares auf vmLS2 einrichten

Sie werden immer mehr als nur die Freigaben für das Heimatverzeichnis der Benutzer als Freigabe bereitstellen wollen.

Ziel dieses ABs ist es, nachdem Sie eine administrative Freigabe erzeugt haben, die gesamte Konfiguration der Freigaben für Ihre Benutzer komplett über Windows zu steuern.

Natürlich können Sie Ihre Freigaben auch weiterhin direkt auf Ihrem Samba-Server erstellen und verwalten, aber denken Sie beim Anlegen von Verzeichnissen daran, dass Windows eine etwas komplexere Rechtevergabe bestehend aus ACLs und erweiterten Dateisystemattributen verwendet.

Wenn Sie wollen, dass Ihre Benutzer ihre Rechte in ihren Verzeichnissen selbst verwalten können, dann sollten Sie Berechtigungen für Freigaben immer unter Windows setzen.

2.1 Administrativer Share einrichten

Um später die Freigaben auch von Windows über den Registryeditor einrichten zu können, soll jetzt als Erstes eine administrative Freigabe angelegt werden. Das Verzeichnis für diese Freigabe müssen Sie auf jeden Fall noch unter Linux anlegen. Bei der Freigabe können Sie sowohl den Weg über Linux als auch über Windows gehen. Im folgenden Listing sehen Sie, wie Sie die administrative Freigabe einrichten und mit Rechten versehen:

```
root@vmls2:~# mkdir -m 775 /admin-share
root@vmls2:~#
root@vmls2:~# chgrp 'SAM159\Domain Admins' /admin-share/
root@vmls2:~#
root@vmls2:~# net conf addshare admin-share /admin-share writeable=y guest_ok=n "Admin-
share"
root@vmls2:~#
root@vmls2:~# net conf setparm admin-share "browsable" "yes"
root@vmls2:~#
```

Listing 1: Einrichtung eines Administrativ-Shares auf vmLS2

Bevor Sie jetzt die erste Freigabe für Ihre Benutzer unter Windows anlegen, müssen Sie erst noch ein Privileg an die Gruppe der *domain admins* vergeben. Nur so können die Mitglieder der Gruppe der *domain admins* überhaupt Freigaben auf dem Server einrichten. Das Privileg, das Sie hier benötigen, ist das Privileg *SeDiskOperatorPrivilege*. Das Privileg setzt man so:

```
root@vmls2:~# net rpc rights grant 'SAM159\domain admins' SeDiskOperatorPrivilege -U
administrator -S vmls2
Enter administrator's password:
Successfully granted rights.
root@vmls2:~#
```

Listing 2: Vergabe des *SeDiskOperatorPrivilege*-Privileges auf vmls2

Das Privileg kann auch abgefragt werden mit:

```
root@vmls2:~# net rpc rights list 'SAM159\domain admins' -U administrator -S vmls2
Enter administrator's password:
SeDiskOperatorPrivilege
```

Listing 3: Abfrage des *SeDiskOperatorPrivilege*-Privileges auf vmls2

WICHTIG:

Privilegien können nur von einem Mitglied der Gruppe *domain admins* gesetzt werden. Deshalb muss bei diesem Kommando immer eine Authentifizierung verwendet werden.

2.2 Aufgabe 1


Informieren sie sich über das Privileg *SeDiskOperatorPrivilege*! Was bedeutet dieses?

3 Erstellen eines Shares unter Windows

Jetzt soll eine Freigabe unter Windows angelegt werden. Die Daten in dieser Freigabe sollen später für alle Mitarbeiter komplett zur Verfügung stehen. Melden Sie sich dafür an einem Windows-Client als Administrator an, und verbinden Sie sich mit der vorher erstellten administrativen Freigabe *admin-share*.

Da Sie für diese Aufgabe nur Standardwerkzeuge eines Windows-Clients benötigen, müssen auf dem Client, von dem aus Sie die Freigabe einrichten, die RSAT nicht installiert sein. Der Client muss nur Mitglied der Domäne sein. Mit anderen Worten: wir werden mit diesem Trick Shares einrichten können, ohne die RSAT-Tools verwenden zu müssen.

Erstellen Sie nun in der Freigabe einen Ordner PUBLIC, der anschliessend als Share *sh-public* für die User verwendet werden soll:

←  Netzlaufwerk verbinden

Welcher Netzwerkordner soll zugeordnet werden?

Bestimmen Sie den Laufwerksbuchstaben für die Verbindung und den Ordner, mit dem die Verbindung hergestellt werden soll:

Laufwerk:

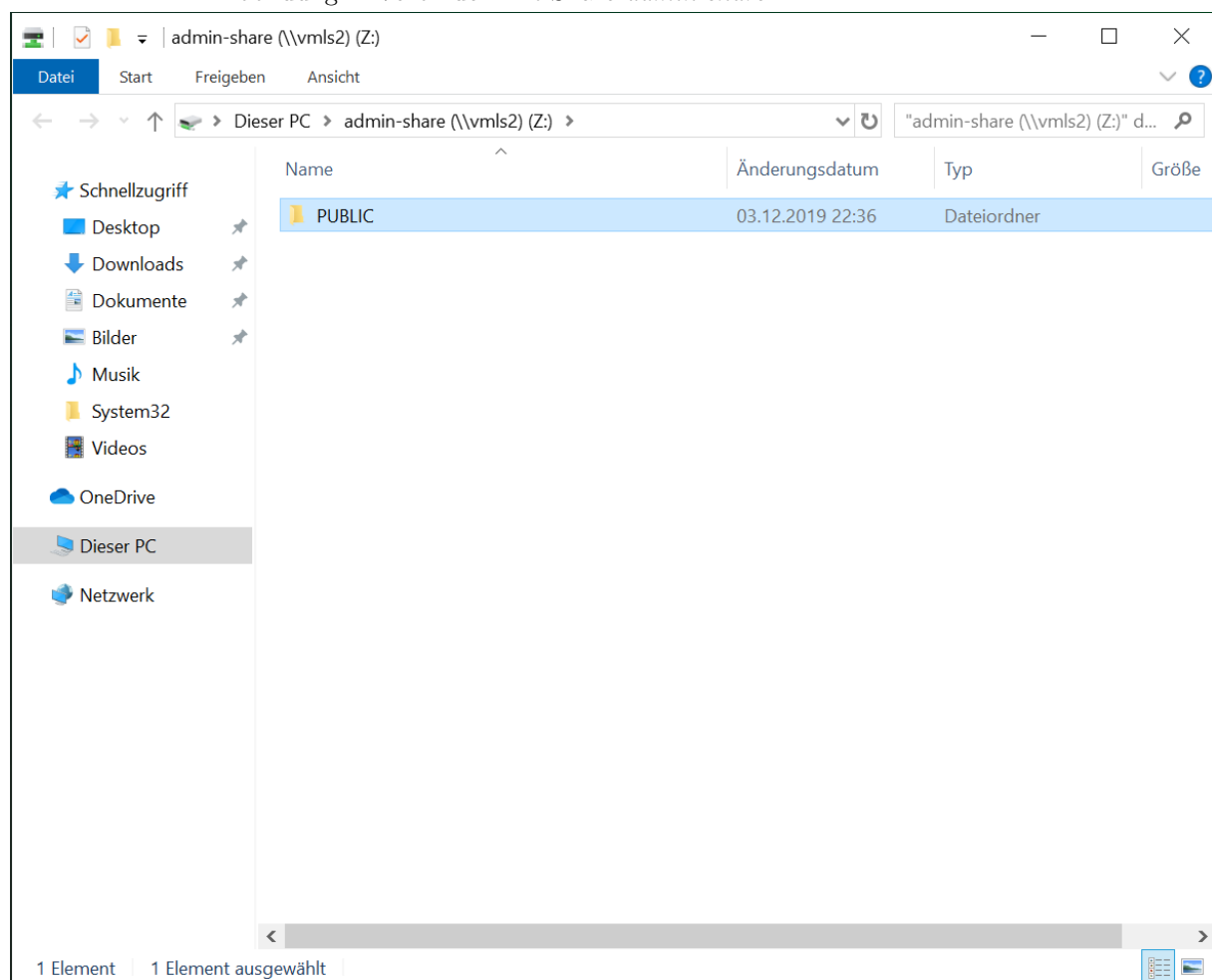
Ordner:

Beispiel: \\Server\Freigabe

☒ Verbindung bei Anmeldung wiederherstellen

☐ Verbindung mit anderen Anmeldeinformationen herstellen

[Verbindung mit einer Website herstellen, auf der Sie Dokumente und Bilder speichern können](#)

Abbildung 1: Verbinden mit Share *admin-share*Abbildung 2: Erstellung Ordner *PUBLIC* für neuen Share *sh-public*

Um die Rechte an dem Ordner anpassen zu können, öffnen Sie anschliessend die Eigenschaften des Ordners und klicken auf SICHERHEIT. Jetzt sollen komplett neue Rechte für diesen Ordner unter Windows gesetzt werden. Dafür klicken Sie

auf ERWEITERT.

Es erscheint ein neues Fenster mit allen momentan gesetzten Rechten, so wie Sie es in folgender Abbildung sehen.

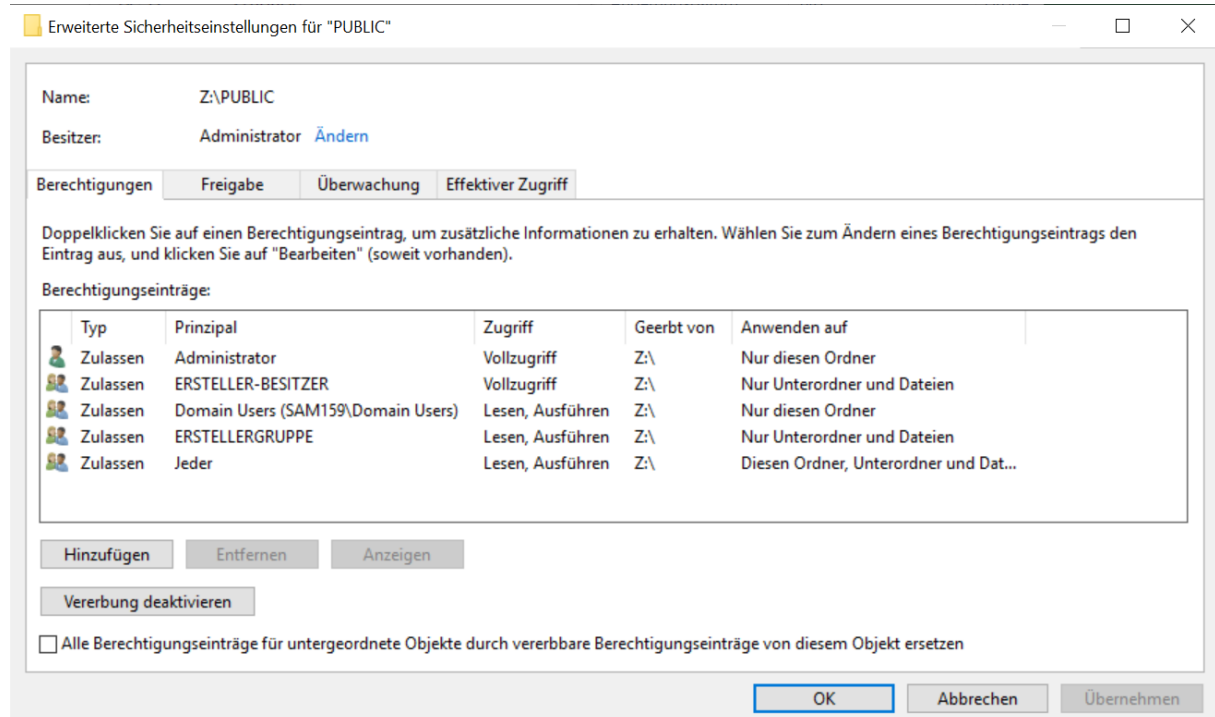


Abbildung 3: aktuelle Rechte am neuen Ordner *PUBLIC*

Klicken Sie jetzt auf VERERBUNG DEAKTIVIEREN. Es erscheint ein Fenster, in dem Sie die Wahl haben, die vererbten Rechte zu übernehmen oder diese zu entfernen. Da hier eine komplett neue Rechtestruktur entstehen soll, entfernen Sie alle Rechte. Anschliessend sehen Sie, dass die ACL leer ist. Klicken Sie jetzt auf HINZUFÜGEN, um einen neuen Eintrag in der ACL zu erstellen. In dem neuen Fenster klicken Sie auf PRINZIPAL AUSWÄHLEN. Entweder können Sie jetzt direkt eine Gruppe eintragen oder über die Schaltfläche ERWEITERT Ihr Active Directory nach einer Gruppe durchsuchen.

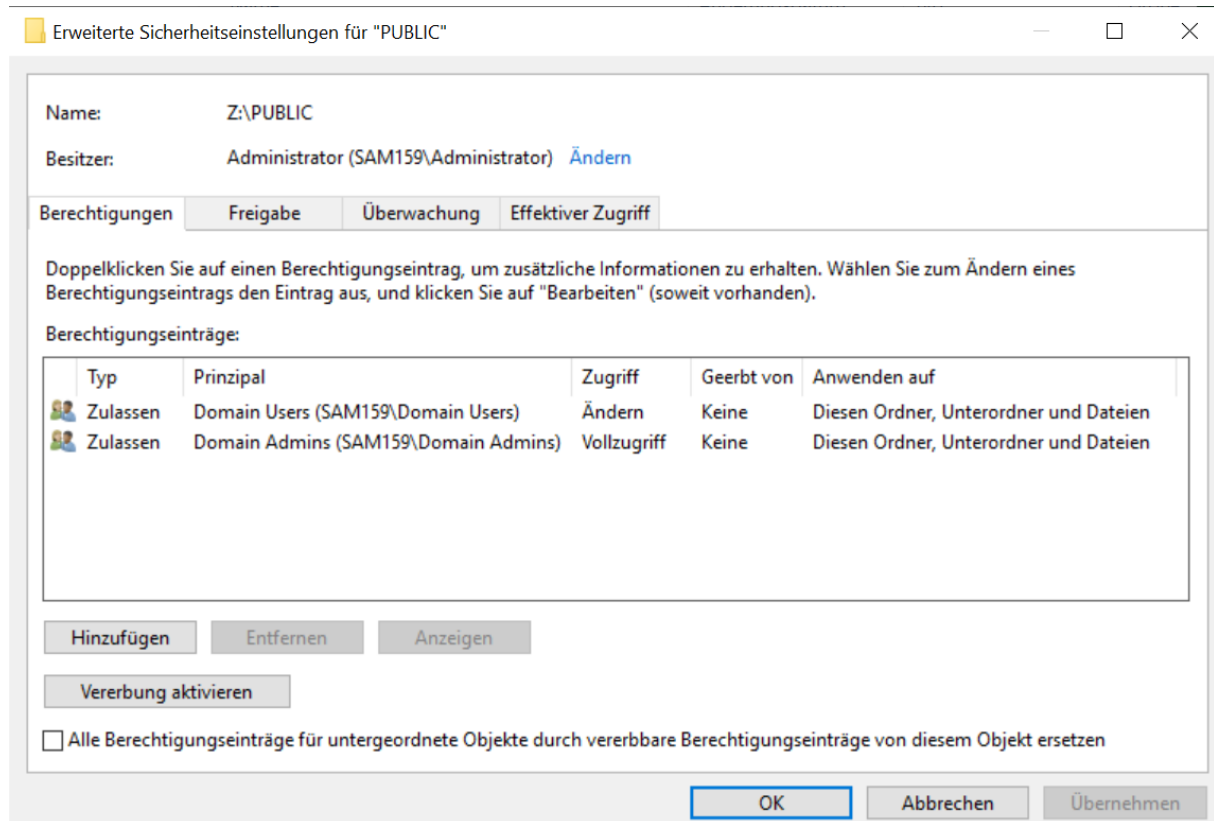
Da auf diese Freigabe später alle Mitglieder der Domäne Zugriff haben sollen, wird hier am einfachsten die Gruppe der *domain users* hinzugefügt. Geben Sie der Gruppe das Recht ÄNDERN. Dieses Recht reicht aus, damit dort alle Benutzer Dateien und Verzeichnisse erstellen, löschen, kopieren und umbenennen können.

Nie das Recht VOLLZUGRIFF vergeben

Das Recht Vollzugriff sollten Sie nie an alle vergeben, da dieses Recht es auch allen Mitgliedern der Gruppe erlaubt, die Berechtigungen an diesem Ordner zu verändern.

Wenn Sie hier der Gruppe der *domain admins* keine Rechte zuweisen, können ihre Mitglieder nicht auf die Freigabe zugreifen. Da der Administrator nur in der Gruppe *domain admins* ist und nicht Mitglied der Gruppe *domain users*, gilt das auch für ihn. Im Gegensatz zu Linux hat der *Administrator* nicht immer automatisch vollen Zugriff auf alle Daten.

Geben Sie daher der Gruppe *domain admins* den VOLLZUGRIFF. Speichern Sie Ihre Änderung der Rechte, und schliessen Sie alle Fenster, die zu den Eigenschaften des Ordners gehören. Anschliessend öffnen Sie die Eigenschafteneigenschaften erneut, klicken wieder auf SICHERHEIT und schauen sich die neuen Rechte an. Somit sehen die Rechte wie folgt aus:

Abbildung 4: neue Rechte am Ordner *PUBLIC*

3.1 Aufgabe 2

Wie sehen die gesetzten ACLs für den Ordner *PUBLIC* direkt auf dem Samba-Server aus? Verwenden Sie den Befehl `getfacl` und dokumentieren sie das im Arbeitsjournal.

3.2 Share mit *Regedit* anlegen

Das war der erste Schritt auf dem Weg hin zu einer ersten Freigabe. Jetzt soll der Ordner *PUBLIC* noch von Windows aus über den Registryeditor *Regedit* als Freigabe *sh-public* eingerichtet werden.

Das Einrichten der Freigabe ist nur für ein Mitglied der Gruppe der *domain admins* möglich. Stellen Sie sicher, dass der Benutzer, mit dem Sie momentan angemeldet sind, Mitglied dieser Gruppe ist.

Starten Sie hierfür den *Regedit*, und verbinden Sie sich mit Ihrem Fileserver. Öffnen Sie den Baum so wie Sie es in der folgenden Abbildung sehen:

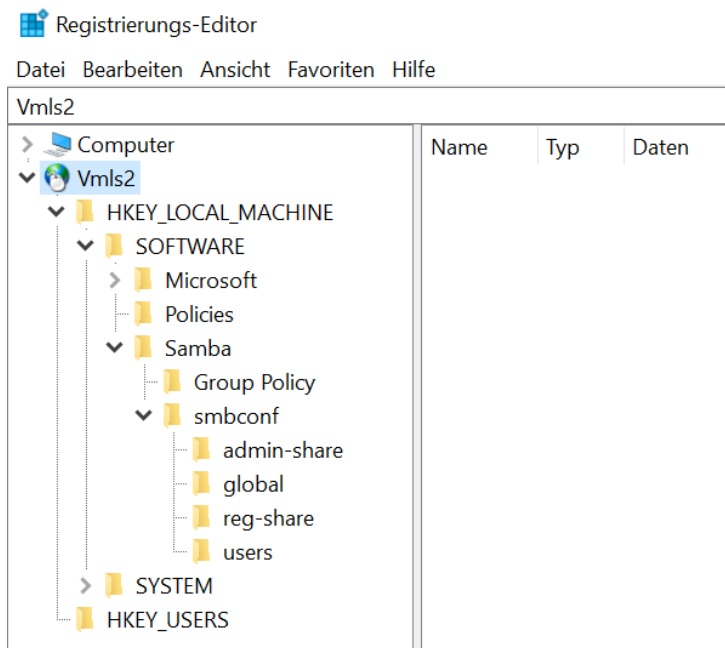


Abbildung 5: Öffnen der Registry

Klicken Sie mit der rechten Maustaste auf der linken Seite auf SMBCONF, und erstellen Sie einen neuen Schlüssel.

Der Schlüssel soll den Namen der zukünftigen Freigabe erhalten: *sh-public*

Beim Umbenennen des Schlüssels erhalten Sie eine Fehlermeldung, dass der Schlüssel nicht umbenannt werden kann, so wie Sie es in der folgenden Abbildung sehen.

Diese Meldung können Sie ignorieren. Klicken Sie hier einfach auf OK und anschliessend drücken Sie F5 um die Anzeige zu aktualisieren.

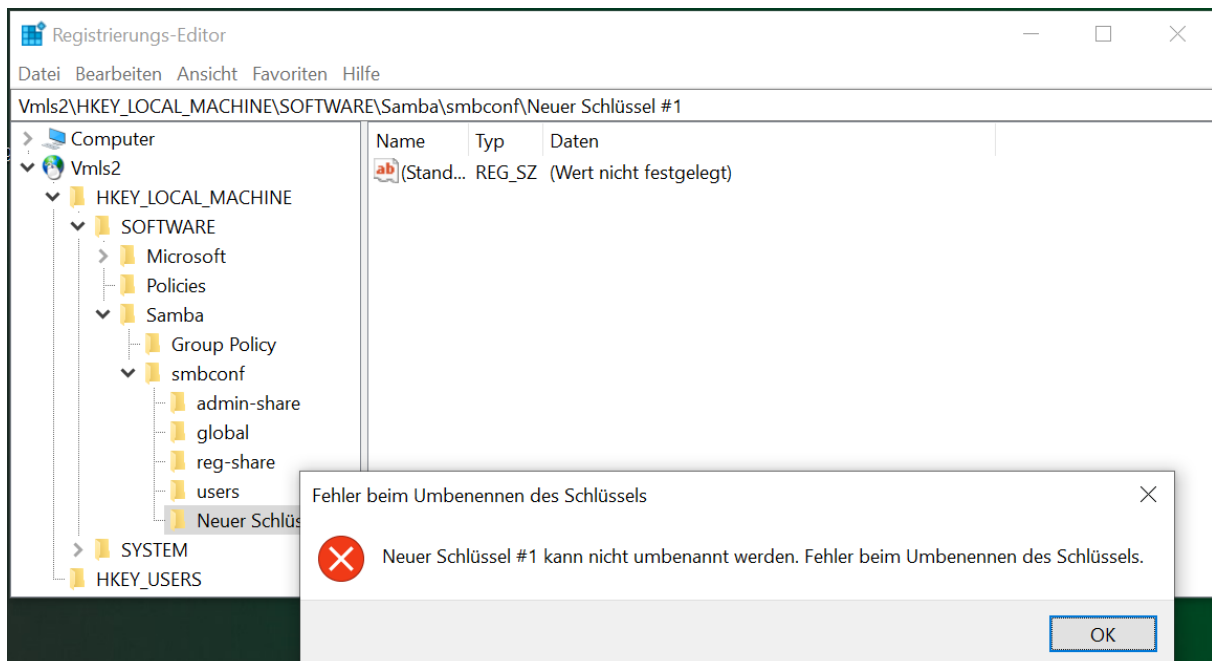


Abbildung 6: Fehler beim Umbenennenden des Schlüssels - IGNORIEREN!

Nachdem Sie die Ansicht aktualisiert haben, werden Sie feststellen, dass der Schlüssel *sh-public* aufgeführt wird, aber zusätzlich noch ein Schlüssel mit dem Namen *Neuer Schlüssel #1* erstellt wurde. Diesen

Schlüssel können Sie einfach löschen.


Bei jeder neuen Freigabe, die Sie mit dem *Regedit* erstellen, werden Sie den gleichen Fehler erhalten.

Klicken Sie jetzt auf den von Ihnen neu erstellten Schlüssel. Auf der rechten Seite des Fensters sehen Sie jetzt, dass ausser dem Eintrag Standard keine weiteren Einträge vorhanden sind. Hier tragen Sie jetzt nach und nach alle benötigten Parameter ein.

Klicken Sie dafür mit der rechten Maustaste auf die rechte Seite des Fensters, und erstellen Sie einen neuen Parameter vom Typ ZEICHENFOLGE. Geben Sie dem neuen Parameter den Name **path**.

Führen Sie einen Doppelklick auf den neuen Parameter aus, und tragen Sie bei Wert den absoluten Pfad im Linux-Dateisystem ein, so wie Sie es in folgender Abbildung sehen. Alle Einträge in der Samba-Registry sind immer vom Typ ZEICHENKETTE. Sie werden hier nie einen anderen Typ verwenden.

Ergänzen Sie die Freigabe um die Parameter **read only = no** und **browsable = yes**. Im Anschluss sieht Ihre Freigabe so aus wie in folgender Abbildung:

 Registrierungs-Editor

Datei Bearbeiten Ansicht Favoriten Hilfe

Vmls2\HKEY_LOCAL_MACHINE\SOFTWARE\Samba\smbconf\sh-public

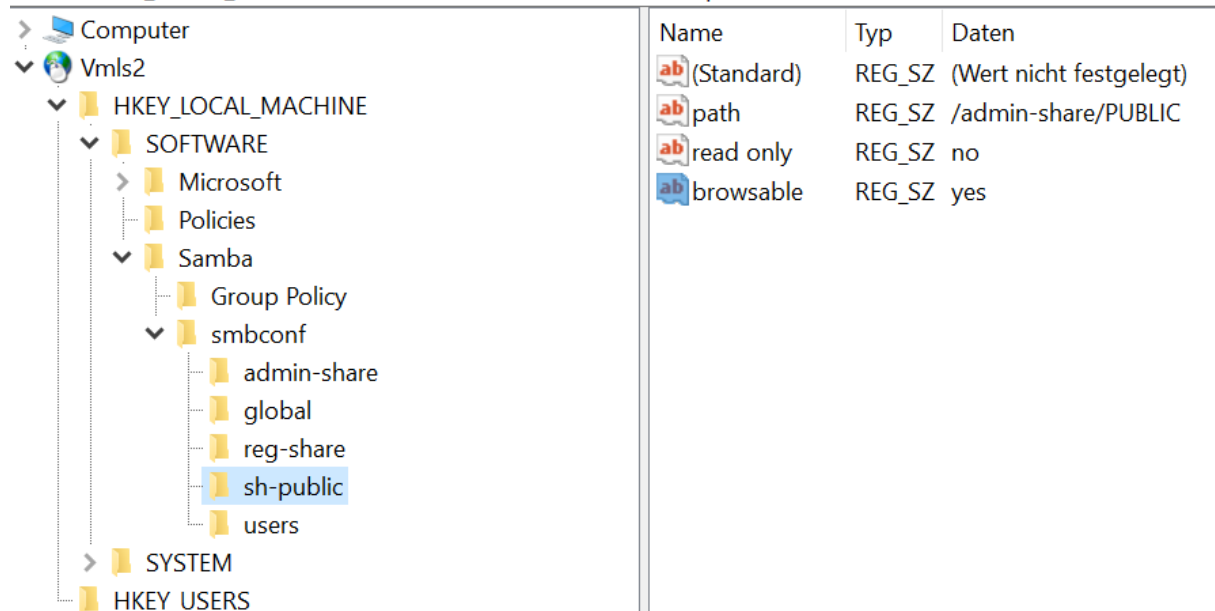


Abbildung 7: Parameter für Share *sh-public*

Damit ist die Einrichtung des Shares *sh-public* abgeschlossen. Lassen Sie sich jetzt die Registry auf der Konsole mit dem Kommando **net conf list** anzeigen. **net conf list** zeigt Ihnen alle Shares an, welche wir bis jetzt erstellt haben.

4 Aufgabe 3: Share mit `hide unreadable = yes`

Zuerst, was bewirkt der Parameter `hide unreadable = yes` ?

Dieser Parameter kann Ihnen dabei helfen, die Anzahl der Freigaben auf einem Server zu reduzieren. Sie geben nur noch eine übergeordnete Ebene der Verzeichnisse frei, die Sie Ihren Benutzern zur Verfügung stellen wollen.

Wenn Sie jetzt die Zugriffsrechte so setzen, dass nur noch bestimmte Gruppen Rechte an den Verzeichnissen haben, dann sehen Ihre Benutzer beim Zugriff auf die Freigabe nur noch die Verzeichnisse, an denen sie Leserechte besitzen. Alle anderen Verzeichnisse sind für sie unsichtbar. So ist es einfach, ei-

nem Benutzer durch den Wechsel in eine andere Gruppe andere Verzeichnisse der Freigabe bereitzustellen.

Bevor sie mit der Umsetzung der Aufgabe beginnen, lesen sie zuerst die Anforderungen und dann die Tipps für das Vorgehen genau durch.

ANFORDERUNGEN:

1. Wir wollen einen Share mit dem Namen *sh-abteilungen* erstellen. Innerhalb dieses Shares gibt es 3 Verzeichnisse GL, PRODUKTION und VERWALTUNG. GL steht für Geschäftsleitung.
2. Wir erstellen 3 Gruppen mit je einem User. Die Gruppen heissen entsprechend den Abteilungen *verwaltung*, *produktion* und *gl*. Es werden 3 User erfasst. Die User heissen *user1-verw*, *user1-prod* und *user1-gl*. Jeder User ist Mitglied der entsprechenden Gruppe. *user1-verw* gehört in die Gruppe *verwaltung*, usw.
3. Im administrativen Share *admin-share* legen wir einen Ordner ABTEILUNGEN an. Dieser Ordner soll unter dem Share-Namen *sh-abteilungen* allen Mitarbeitern zur Verfügung stehen.
4. Für jede Gruppe besteht somit ein eigenes Verzeichnis innerhalb des Shares *sh-abteilungen*. Die Forderung ist, dass nur Mitglieder der Abteilung schreibend Zugriff auf das eigene Verzeichnis haben. Die Geschäftsleitung soll an den Verzeichnissen der Produktion und Verwaltung zusätzlich das Leserecht erhalten. Abteilungsübergreifende Berechtigungen gibt es sonst keine: Die Verwaltung hat keine Sicht in das Verzeichnis der Produktion und umgekehrt.
5. *domain admins* sollen an den Ordnern keine Rechte erhalten!
6. Sehen sie den Zusammenhang mit dem Parameter `hide unreadable = yes` ? Falls nicht, lassen sie sich das von der Lehrperson erklären.

TIPPS für das Vorgehen in 3 Schritten:

1. Gruppen und User anlegen

- (a) Erstellen Sie die 3 Gruppen GL, PRODUKTION und VERWALTUNG. Tool: RSAT oder der Befehl `samba-tool group add`
- (b) Erstellen Sie die 3 User *user1-verw*, *user1-prod* und *user1-gl*. Tool: RSAT oder der Befehl `samba-tool user create ...`
- (c) Fügen Sie die User der entsprechenden Gruppe hinzu. Tool: RSAT oder der Befehl `samba-tool group addmembers PRODUKTION user1-prod ...`

2. Verzeichnisse anlegen

- (a) Im *admin-share* Verzeichnis legen sie als Administrator ein Verzeichnis ABTEILUNGEN an. Dieses Verzeichnis machen wir später zum Share *sh-abteilungen*. Unterhalb von ABTEILUNGEN legen sie die 3 Verzeichnisse GL, PRODUKTION und VERWALTUNG an. Sorgen Sie dafür, dass nur *domain users* lesenden Zugriff auf das Verzeichnis ABTEILUNGEN haben. Tragen Sie hier nicht die *domain admins* ein. Diese sollen an dem Ordner keine Rechte erhalten.
- (b) Passen Sie jetzt die Berechtigungen der Unterordner an, so dass die Abteilungen selbst das Recht ÄNDERN haben und die Gruppe der Geschäftsleitung das Recht LESEN zusätzlich an den Ordnern VERWALTUNG und PRODUKTION hat. Gehen Sie entsprechend vor, wie wir es bei der Rechtevergabe des Ordners PUBLIC gemacht haben. Sie oben, Seiten 3 und 4.

3. Erstellen des Shares *sh-abteilungen*:

- (a) Erstellen Sie den Share mit *Regedit*, analog wie wir es oben mit dem Share *sh-public* gemacht haben. Folgende Parameter sind für den Share *sh-abteilungen* wichtig:
 - i. `path = /admin-share/ABTEILUNGEN`
 - ii. `writable = yes`

- iii. `guest_ok = no`
 - iv. `browsable = yes`
 - v. `hide unreadable = yes`
- (b) oder Alternativ, wenn Sie ein Command-Line-Crack sind, können sie den Share unter Linux mit `net conf addshare sh-abteilungen anlegen`.
4. Testen Sie die Berechtigungen, indem sie sich mit jedem der 3 User anmelden und auf *sh-abteilungen* zugreifen. Melden Sie sich, wenn sie dies geschafft haben und alle Anforderungen erfüllt sind. Die Lehrperson wird Ihnen einen Samba-Orden verleihen.. ;-)

Dokumentieren Sie ihr Vorgehen Schritt für Schritt im Arbeitsjournal!