

M159 - Directory Services

Thema 2

Arbeitsblatt 7

1 Lernziele

Im AB 7 verfolgen wir folgende Lernziele:

- Sie können allgemeine Freigaben auf dem Linux-Samba-Fileserver mit Gruppenrichtlinien verwalten

2 Zuweisung der Shares über Group Policies - GPOs

Bis zu diesem Zeitpunkt müssen sich Benutzer die Freigaben immer noch selbst über den Dateimanager verbinden. Das ist nicht das, was Sie auf die Dauer wollen. Besser ist es, wenn die Freigaben beim Anmelden eines Benutzers automatisch verbunden werden.

Das können Sie auf die alte Art machen, indem Sie Logon-Skripte erstellen und diese dann den Benutzern zuweisen, oder Sie machen es über Gruppenrichtlinien.

Der Weg über Gruppenrichtlinien ist auf jeden Fall der bessere Weg, da Sie hier die Zuordnung nicht bei jedem einzelnen Benutzer erstellen müssen, sondern Sie können diesen Vorgang über Gruppen steuern.

So ist es einfach, einem Benutzer bei einem Abteilungswechsel schnell neue Freigaben bereitzustellen.

2.1 Anlegen der GPOs

Als Erstes müssen Sie eine leere Gruppenrichtlinie anlegen. Dazu öffnen Sie die *Gruppenrichtlinienverwaltung*, die zu den RSAT gehört. Hier erstellen Sie in dem Container GRUPPENRICHTLINIENOBJEKTE ein neues leeres Gruppenrichtlinienobjekt.

Da alle Gruppenrichtlinienobjekte immer in diesem Container erzeugt werden, sollten Sie sich einen Namensstandard überlegen. Die Objekte werden hier alphabetisch sortiert angezeigt.

Wenn Sie alle Laufwerkzuordnungen zum Beispiel immer mit »LW-« beginnen, werden Sie die entsprechenden Gruppenrichtlinienobjekte auch immer schnell finden.

Dokumentieren Sie alle Gruppenrichtlinien, damit Sie die Übersicht über Ihre Gruppenrichtlinien und deren Inhalt behalten.

Das leere Gruppenrichtlinienobjekt taucht jetzt in der Liste aller Gruppenrichtlinien auf und kann mit dem *Gruppenrichtlinieneditor* bearbeitet werden. Klicken Sie dafür mit der rechten Maustaste auf das Objekt und dann auf BEARBEITEN .

Öffnen Sie die Einstellung BENUTZERKONFIGURATION • EINSTELLUNGEN • WINDOWS-EINSTELLUNGEN. Dort finden Sie den Unterpunkt LAUFWERKSZUORDNUNGEN. Klicken Sie auf die LAUFWERKSZUORDNUNGEN. Auf der rechten Seite erscheint dann das Fenster aus Abbildung 1.

Mit Rechtsklick kann eine neue Laufwerkzuordnung erstellt werden. Daraufhin öffnet sich ein Fenster wie in Abbildung 2.

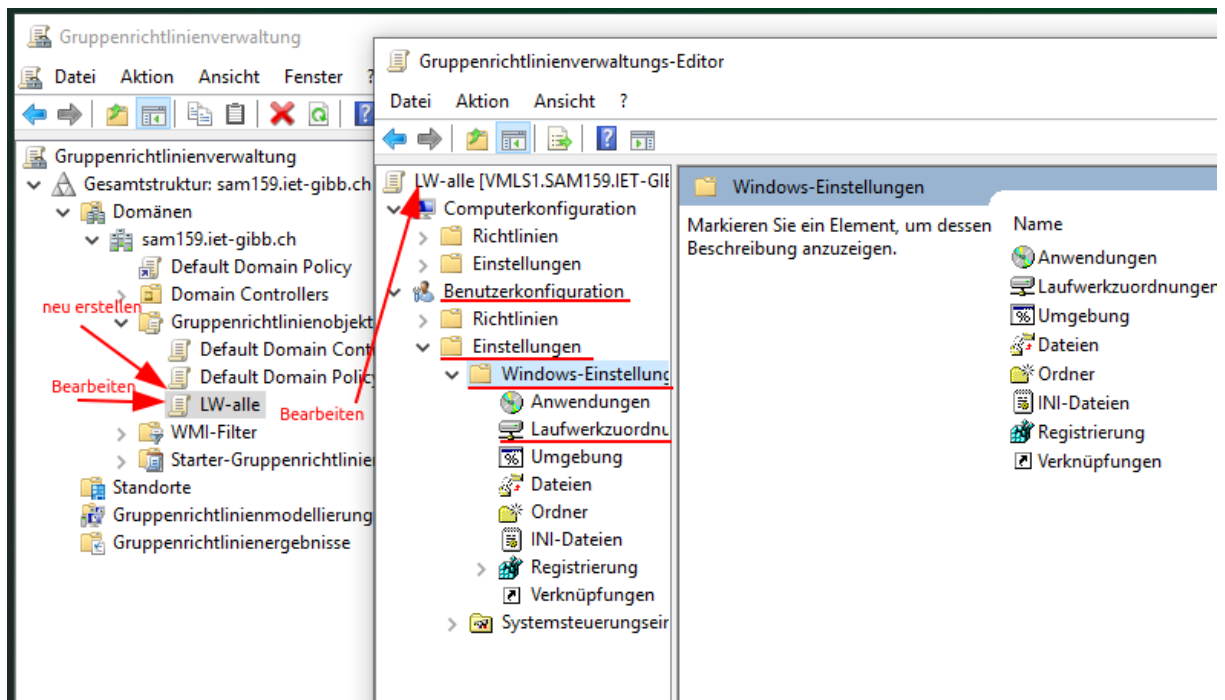


Abbildung 1: neues GPO erstellen

Unter dem Punkt AKTION können Sie verschiedene Möglichkeiten auswählen, wie die Zuordnung beim Client behandelt werden soll.

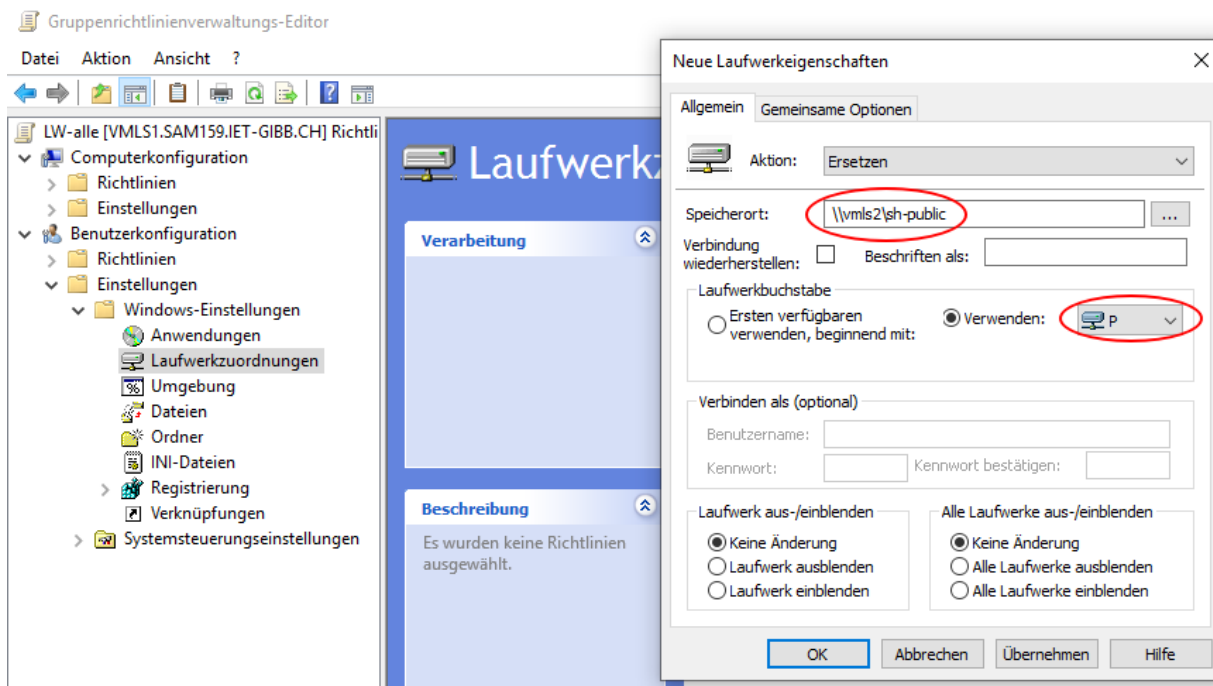


Abbildung 2: hier werden Laufwerkzuordnungen definiert

- **ERSTELLEN**
Die Zuordnung wird eingerichtet, wenn die entsprechende Freigabe noch nicht verbunden wurde. Ist die Freigabe schon verbunden, passiert nichts.
- **ERSETZEN**
Hierbei werden alle bestehenden Verbindungen zur Freigabe gelöscht, und die Zuordnung wird mit

den aktuellen Einstellungen hergestellt. Ist die Freigabe bis jetzt noch nicht verbunden gewesen, wird die Verbindung jetzt hergestellt.

- **AKTUALISIEREN**

Verwenden Sie diesen Punkt, dann wird eine bestehende Verbindung nur verändert. Besteht noch keine Verbindung zu der Freigabe, wird die Freigabe erzeugt.

- **LÖSCHEN**

Löscht eine Freigabe. Diese Option ist nur sinnvoll, wenn Sie sichergehen wollen, dass eine Freigabe dauerhaft von allen Clients verschwindet.

In den meisten Fällen ist es sinnvoll, den Punkt ERSETZEN zu wählen, denn dann werden auch die eventuell vom Benutzer selbst erstellten Zuordnungen immer wieder neu aufgebaut. Auch die von Ihnen vorgenommenen Änderungen werden bei einer Neuansmeldung eines Benutzers sofort übernommen. Tragen Sie neben der Option SPEICHERORT den Pfad, bestehend aus Servername und Freigabename, zur Freigabe ein. In unserem Beispiel wäre das \\vmLS2\sh-public. In Abbildung 2 sehen Sie die kompletten Einstellungen für die Zuordnung.

Wenn Sie möchten, dass die Verbindung mit einer Freigabe entfernt wird, sobald Sie die Kriterien für die Zuordnung geändert haben, dann müssen Sie ERSETZEN wählen.

Die Einstellungen lassen sich noch weiter verfeinern. So können Sie zum Beispiel die Richtlinie auch noch auf bestimmte Gruppen beschränken. Sie sehen hier, wie Sie die Zuordnungen erstellen.

Wenn Sie über Gruppenrichtlinien Laufwerke zuordnen, können Sie jedes Laufwerk über eine eigene Gruppenrichtlinie verwalten, Sie können aber auch mehrere Laufwerke über eine Gruppenrichtlinie zuordnen.

Jetzt können Sie den *Gruppenrichtlinieneditor* einfach schliessen und gelangen dann zurück in die *Gruppenrichtlinienverwaltung*. Sie müssen Änderungen an dieser Stelle nicht extra speichern.

Klicken Sie jetzt bei dem gerade erstellten Gruppenrichtlinienobjekte auf den Karteireiter EINSTELLUNGEN und dort auf SHOW ALL. Dort sehen Sie dann, so wie in Abbildung 3, die Einstellungen, die Sie mit dem Gruppenrichtlinieneditor erstellt haben.

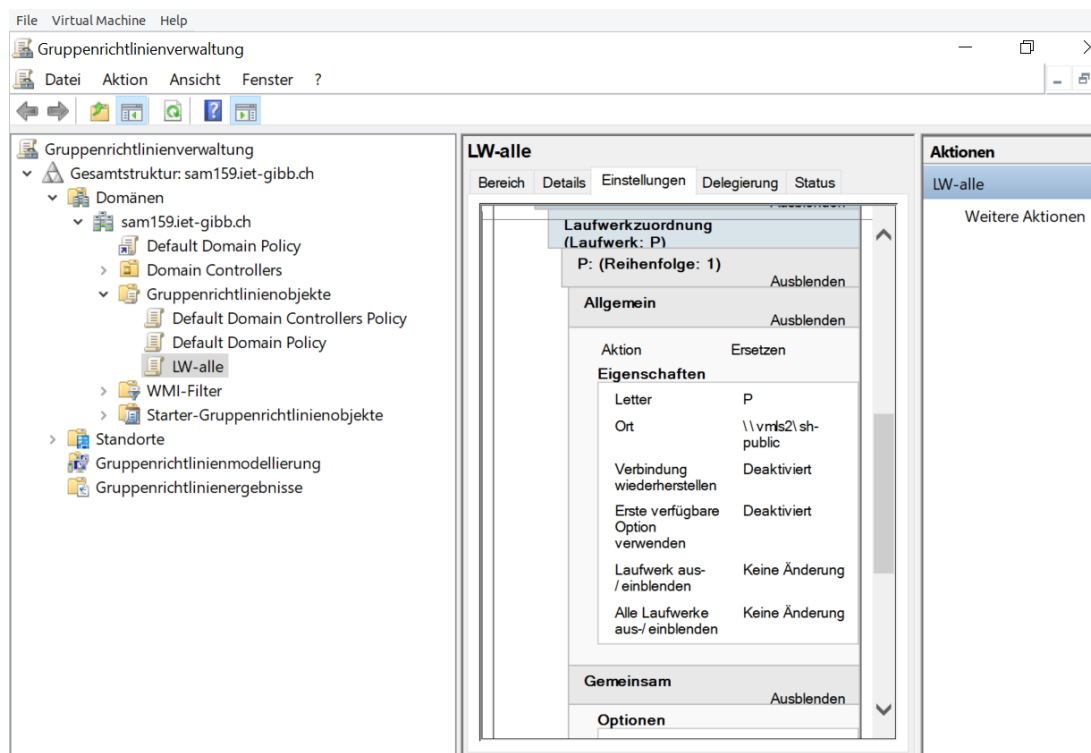


Abbildung 3: Einstellung der GPO

Damit haben Sie die Gruppenrichtlinie erstellt und können im nächsten Schritt die Gruppenrichtlinie zuordnen.

2.2 Zuordnung der GPO

Bevor Sie Ihre Gruppenrichtlinien zuordnen können, müssen Sie sich jetzt erst eine Baumstruktur für Ihr Active Directory überlegen und anlegen. Anschliessend müssen Sie alle Ihre Gruppen und Benutzer, denen Sie über die Gruppenrichtlinie ein Laufwerk zuordnen wollen, in einem OU außerhalb des Containers cn=Users verschieben.

Dem Container cn=Users können Sie keine Gruppenrichtlinie zuordnen.

2.2.1 Anlegen der Struktur

Um Gruppen und Benutzer übersichtlich verwalten zu können, sollten Sie sich eine Struktur überlegen, in der Sie Ihre Benutzer und Gruppen organisieren. Bauen Sie hierfür eine Struktur auf, die zur Organisation Ihres Unternehmens passt. Hier werden wir auf die drei Abteilungen zurückgreifen, die wir schon vorher für die Freigabe verwendet haben. In Abbildung 4 sehen Sie die Struktur, die wir für alle anderen Beispiele unterhalb der OU ou=ORGANISATION anlegen wollen.

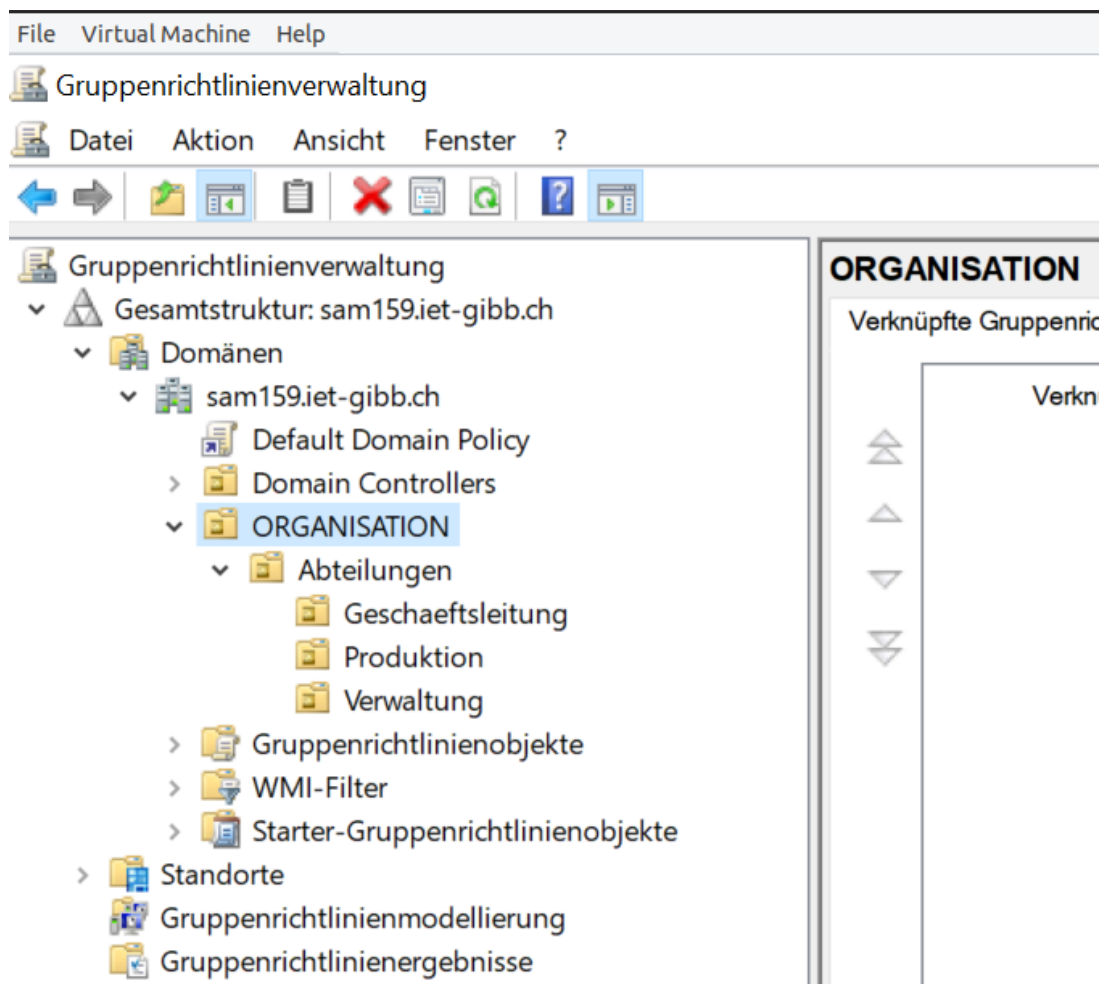


Abbildung 4: Struktur der GPOs

Damit die Gruppenrichtlinien für die Gruppen und Benutzer wirksam werden können, müssen Sie jetzt die entsprechenden Gruppen und die Mitglieder der Gruppen in die Container der einzelnen Abteilungen verschieben. Dazu verwenden Sie das Programm *Active Directory-Benutzer und -Computer* aus

den RSAT.

Ein Verschieben der Benutzer über das Kommando `samba-tool` ist nicht möglich. Wollen Sie sehr viele Benutzer über ein Skript verschieben, geht das nur mithilfe einer `.ldif`-Datei und des Kommandos `ldapmodify`.

2.2.2 Berechtigungen eintragen

Öffnen Sie jetzt wieder die *Gruppenrichtlinienverwaltung*, und klicken Sie auf Ihre Gruppenrichtlinie für die Verwaltung der Laufwerke und dort auf den Karteireiter **BEREICH**. Dort sehen Sie auf der rechten Seite des Fensters, dass die SICHERHEITSFILTERUNG im Moment noch *Authenticated Users* anzeigt. Das ist die Standardeinstellung bei allen neuen Gruppenrichtlinien. Da die Laufwerkzuordnung aber nur für die Gruppe *domain users* gelten soll, entfernen Sie diesen Eintrag aus der Liste, anschliessend klicken Sie auf Hinzufügen und fügen die Gruppe der *domain users* zur SICHERHEITSFILTERUNG hinzu. Jetzt steht nur noch die Gruppe der *domain users* in der Liste, so wie Sie es in Abbildung 5 sehen.

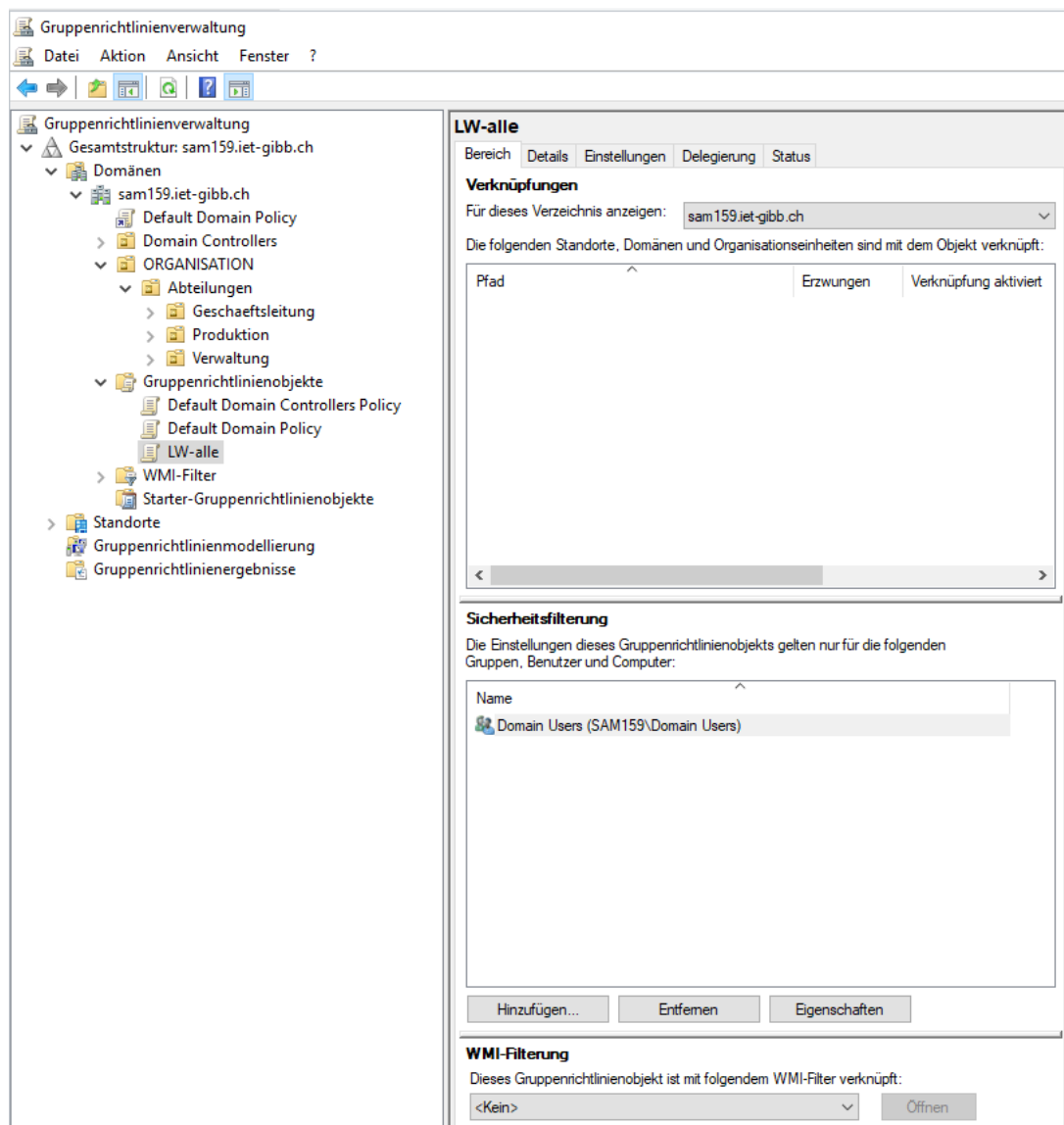


Abbildung 5: GPO Berechtigung

In der Abbildung sehen Sie auch, dass noch keine Verknüpfung mit der Richtlinie existiert. Da diese Laufwerkzuordnung für alle Benutzer gelten soll, wird diese Gruppenrichtlinie jetzt mit der OU `ou=ORGANISATION` verknüpft. Klicken Sie hierfür mit der rechten Maustaste auf die OU `ou=ORGANISATION`

und dann auf VORHANDENES GRUPPENRICHTLINIENOBJEKT verknüpfen und wählen Sie die Gruppenrichtlinie für das Laufwerk aus. Wenn Sie jetzt wieder auf das Gruppenrichtlinienobjekt klicken, sehen Sie, dass das Objekt der OU zugeordnet wurde. Abbildung 6 zeigt dieses.

Beachten Sie auch, dass das GPO-Objekt unterhalb der OU `ou=ORGANISATION` nun sichtbar ist.

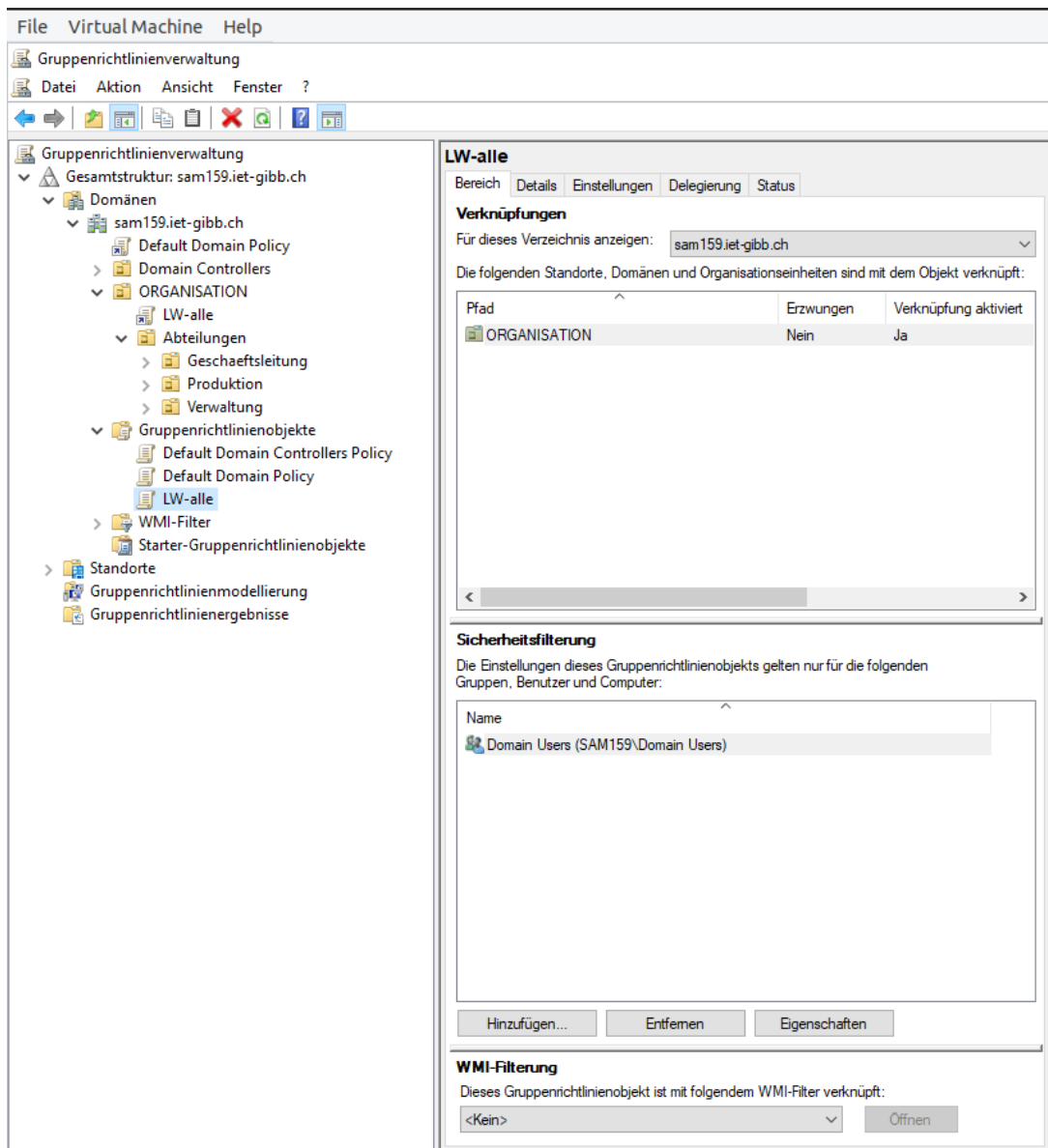


Abbildung 6: Zuordnung GPO → OU

2.3 Aufgabe 1

Erstellen Sie jetzt eine zweite Gruppenrichtlinie für die Abteilungslaufwerke und weisen diese der OU `ou=Abteilungen` zu. Sie können in der Liste der SICHERHEITSFILTERUNG auch mehrere Gruppen eintragen. Sie können jetzt auch jede einzelne Abteilung in die Liste eintragen. So können Sie sehr schnell eine Abteilung aus der Zuweisung der Laufwerke entfernen.

2.4 Aufgabe 2

Mit dem Befehl `samba-tool gpo list username` können Sie sich die Gruppenrichtlinien für einen bestimmten `username` anzeigen lassen. Führen Sie diesen Befehl auf dem Domaincontroller aus und lassen Sie sich die Gruppenrichtlinien der User `user1-gl`, `user1-verw` und `user1-prod` anzeigen. Verwenden Sie den Befehl aus folgendem Listing:

```
root@vmls1:~# samba-tool gpo list user1-gl
GPOs for user user1-gl
  Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
```

Listing 1: GPO's für User *user1-gl*

Die User sollten aber das GPO *LW-alle* zugewiesen haben. Was müssen sie tun, damit die User das GPO *LW-alle* erhalten? Oder anders gefragt: Welche Voraussetzungen müssen erfüllt sein, damit die User das GPO *LW-alle* zugewiesen haben? Sehen Sie folgendes Listing:

```
root@vmls1:~# samba-tool gpo list user1-prod
GPOs for user user1-prod
  LW-alle {963B0FA0-4BE3-45C8-9367-166EFAC1F30F}
  Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
root@vmls1:~# samba-tool gpo list user1-verw
GPOs for user user1-verw
  LW-alle {963B0FA0-4BE3-45C8-9367-166EFAC1F30F}
  Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
root@vmls1:~# samba-tool gpo list user1-prod
GPOs for user user1-prod
  LW-alle {963B0FA0-4BE3-45C8-9367-166EFAC1F30F}
  Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
```

Listing 2: GPO's für Users - hier mit *LW-alle*

Wenn Sie Aufgabe 1 erledigt haben, sollte zusätzlich auch ihr GPO für die Laufwerke der Abteilungen sichtbar sein:

```
root@vmls1:~# samba-tool gpo list user1-gl
GPOs for user user1-gl
  LW-Abteilungen {D42A4AA9-0B59-4301-8D56-F31D5A21FE4B}
  LW-alle {963B0FA0-4BE3-45C8-9367-166EFAC1F30F}
  Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
root@vmls1:~# samba-tool gpo list user1-prod
GPOs for user user1-prod
  LW-Abteilungen {D42A4AA9-0B59-4301-8D56-F31D5A21FE4B}
  LW-alle {963B0FA0-4BE3-45C8-9367-166EFAC1F30F}
  Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
root@vmls1:~# samba-tool gpo list user1-verw
GPOs for user user1-verw
  LW-Abteilungen {D42A4AA9-0B59-4301-8D56-F31D5A21FE4B}
  LW-alle {963B0FA0-4BE3-45C8-9367-166EFAC1F30F}
  Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
```

Listing 3: GPO's für Users - hier mit *LW-alle* und *LW-Abteilungen*

Hinweis: Sollte es beim Auflisten der Gruppenrichtlinien zu Fehlermeldungen kommen, prüfen Sie die ACLs der Gruppenrichtlinien mit dem Kommando `samba-tool ntacl sysvolcheck`. Sollte dort ein Fehler auftreten, können Sie diesen mit dem Kommando `samba-tool ntacl sysvolreset` beheben. Diese Fehler tauchen bei der Verwendung der RSAT unter Windows 10 zusammen mit der Samba-Version 4.X auf. Der Fehler hat keine Auswirkung auf die Funktion der GPOs. Es wird hier nur geprüft, ob eine GPO auch im System propagiert werden kann.

2.5 Aufgabe 3

Melden Sie sich mit einem User an und kontrollieren Sie, ob das Laufwerk verbunden wird.