Lehrerinnenfortbildung
Baden-Württemberg

ZSL

Gruppenrichtlinien

Eine Einführung

Netzwerke/Linux

Peter Schmidt und Mathias Rettich

6. Oktober 2021

Inhaltsverzeichnis

1. Todo

Msitools installieren.

2. Worum geht's?

In diesem AK wird die Anwendung von Gruppenrichtlinien an Hand der folgenden Beispiele gezeigt:

1. Raumbasiertes Installieren von Software über Gruppenrichtlinien.
2. Einrichten von Druckern über Gruppenrichtlinien.
   Drucker werden nicht mehr auf dem Client, sondern bei der Anmeldung am Client über Gruppenrichtlinien zur Verfügung gestellt und bei Bedarf installiert.
   Es wird möglich sein, dass Lehrer sich zusätzlich Drucker freischalten können. So etwas findet auf Laptops Anwendung, wenn beispielsweise der Physiklehrer sich den Physikdrucker freischaltet. Ein anderer Kollege wird sich den Informatikdrucker im zweiten Stock freischalten.
3. Raum- oder Klassenbasierte Bildschirmhintergründe.

3. Gruppenrichtlinien-Management-Tool installieren

Um mit Gruppenrichtlinien zu arbeiten brauchen wir das Gruppenrichtlinien-Management-Tool.

Ab Version 1809 sind die RSAT ein optionales Feature. Die Installation erfolgt über *Start → Einstellungen → Apps → optionale Features -> Feature hinzufügen -> RSAT: Tools zur Gruppenrichtlinienverwaltung*.

4. Druckerverteilung über Gruppenrichtlinien

4.1. mmc.exe Rechte einräumen

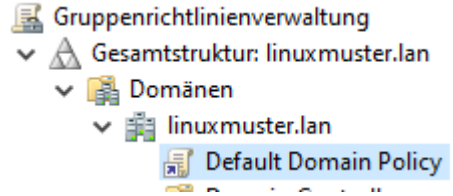
Bevor es losgehen kann, müssen wir dem global-admin noch die nötigen Rechte auf dem Server einräumen. Melden Sie sich dazu als root auf dem Server an und führen Sie die folgenden Befehle aus:

```
net rpc rights grant "LINUXMUSTER\Domain Admins"
SePrintOperatorPrivilege -U "LINUXMUSTER\global-admin"

chgrp -R "LINUXMUSTER\Domain Admins" /var/lib/samba/printers/

chmod -R 2775 /var/lib/samba/printers/
```

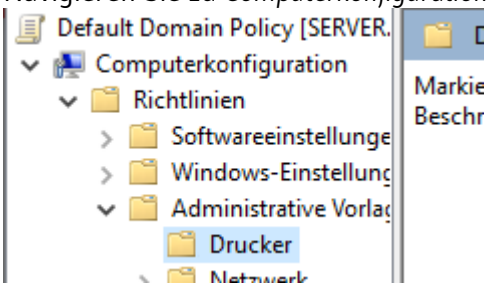
4.2. Über Gruppenrichtlinien dem server als printserver vertrauen

Seit Juli 2016 hat Windows10 ein neues Sicherheitsfeature. Es muss über GPOs festgelegt werden, dass die Windows-Clients unserem Server vertrauen. Dazu gehen wir wie folgt vor:

1. Melden Sie sich als *global-admin* an, starten Sie die Gruppenrichtlinienverwaltung und navigieren zur *Default Domain Policy* von *linuxmuster.lan*.

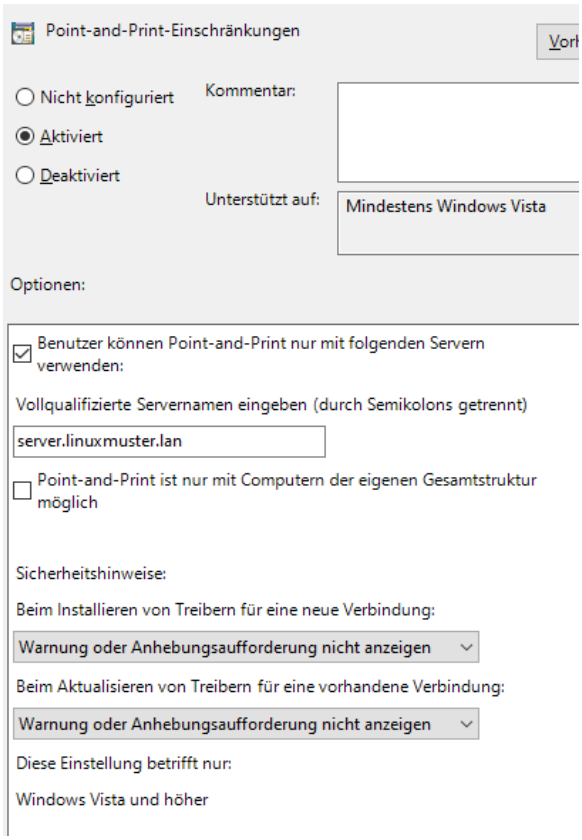


2. Wählen Sie mit einem Rechtsklick *Bearbeiten*. Es öffnet sich der Gruppenrichtlinien-Editor.
3. Navigieren Sie zu *Computerkonfiguration* → *Richtlinien* → *Administrative Vorlagen* → *Drucker*.



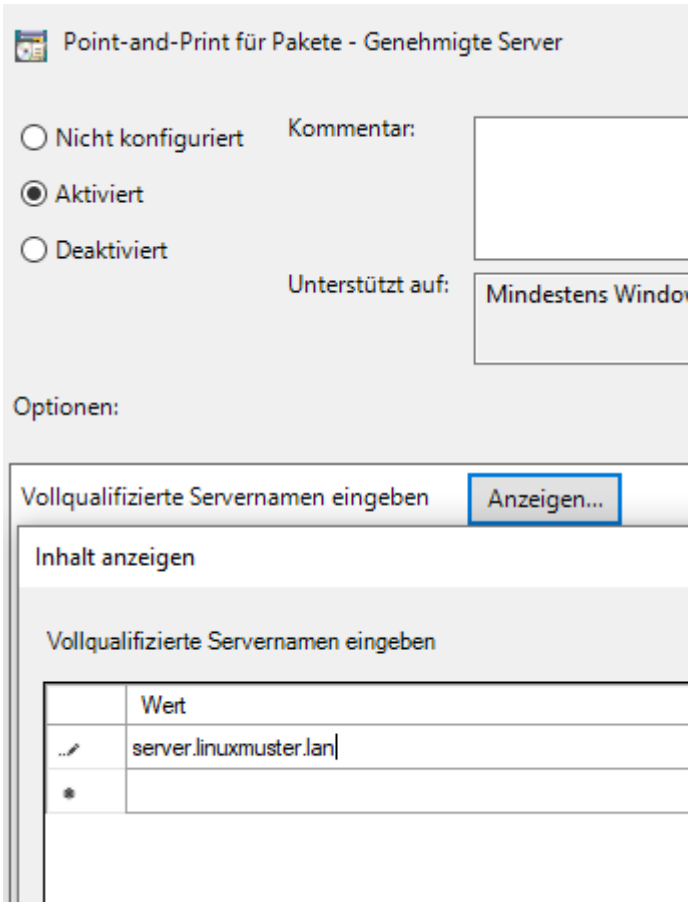
4. Doppelklicken Sie auf *Point and Print Einschränkungen*.

   Aktivieren Sie die Richtlinie und setzen folgende Einstellungen:



- Setzen Sie einen Haken bei *Benutzer können Point and Print für Pakete – Genehmigte Server verwenden*.
- Geben Sie *server.linuxmuster.lan* als FQDN ein.
- Wählen Sie bei *Beim Installieren von Treibern für eine neue Verbindung* und bei *Beim Aktualisieren von Treibern für eine vorhandene Verbindung* die Einstellung *Warnung oder Anhebungsaufforderung nicht anzeigen*.

5. Bestätigen Sie mit *OK*.
6. Doppelklicken Sie auf *Point and Print für Pakete – Genehmigte Server* und aktivieren Sie auch diese Richtlinie

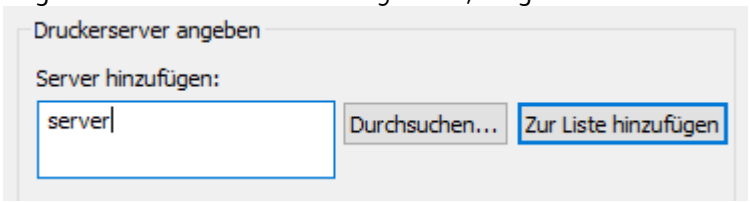


7. Klicken Sie auf *Anzeigen…* , geben den FQDN des Servers ein und bestätigen Sie zwei mal mit *OK*.
8. Schließen Sie den Gruppenrichtlinien-Editor und die Gruppenrichtlinien-Verwaltung
9. Starten Sie den Rechner neu.

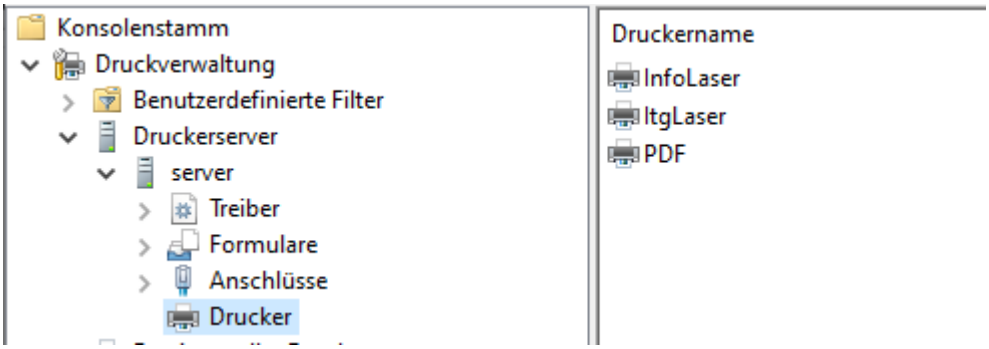
4.3. Druckertreiber auf dem Server installieren

Jetzt können wir die Druckertreiber auf dem Server installieren.

1. Öffnen Sie als global-admin das Programm *mmc.exe und* wählen Sie *Datei → snapin hinzufügen/entfernen.*
2. Fügen Sie die *Druckerverwaltung* hinzu, tragen den Server ein und klicken auf *zur Liste hinzufügen*.



3. Klicken Sie anschließend auf *Fertigstellen* und *OK*.
4. Wie man sieht, sind die Drucker des Systems bekannt. Sie müssen nur noch die Druckertreiber installieren.

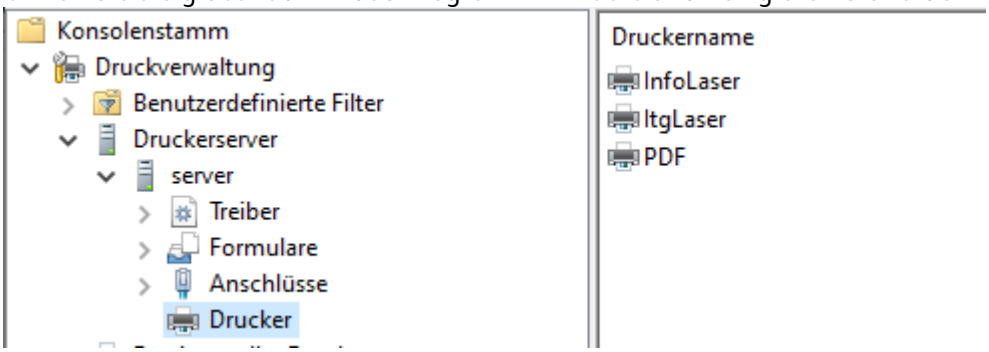


5. Machen Sie einen Rechtsklick auf *Treiber* und wählen *Treiber hinzufügen*.
6. Weiter → Weiter → Datenträger… Durchsuchen → Ok
7. Wählen Sie den richtigen Druckertreiber. Es werden nur Microsoft zertifizierte Treiber akzeptiert. Falls Sie mit Ihrem Treiber Probleme haben, versuchen Sie es eventuell mit einem etwas älteren Treiber. Die werden sehr oft akzeptiert.
8. Klicken Sie abschließend auf *Fertigstellen*.

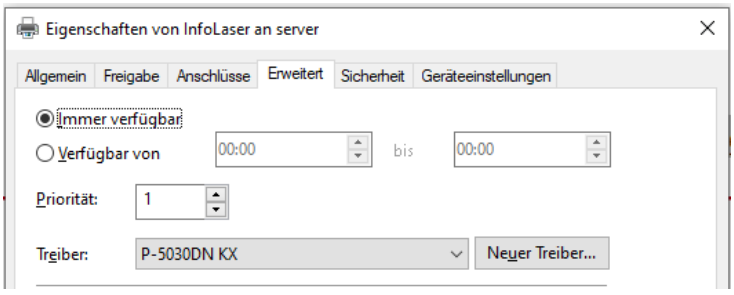
4.4. Druckertreiber einem Druckern zuweisen

Jetzt müssen wir nur noch den Druckern die Druckertreiber zuweisen.

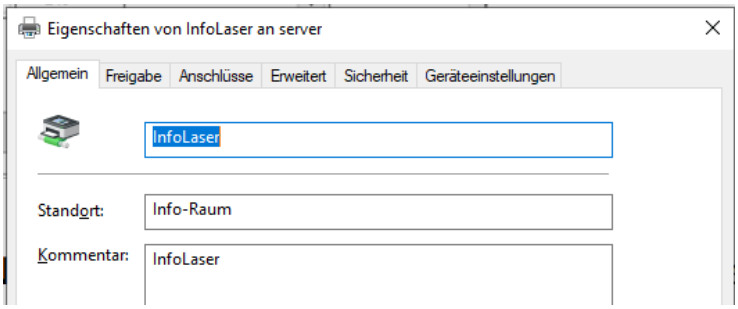
1. Öffnen Sie als global-admin das Programm *mmc.exe* und navigieren Sie zu den Druckern.



2. Machen Sie einen Rechtsklick auf den Drucker, dem Sie einen Druckertreiber zuweisen wollen und wählen *Eigenschaften…*
   Falls Sie gefragt werden, ob Sie einen Druckertreiber lokal installieren möchten, antworten Sie mit *Nein*.
3. Klicken Sie auf den Reiter *Erweitert*, wählen bei *Treiber* den passenden Treiber für den Drucker und bestätigen Sie abschließend mit OK.



4. Leider ändert Windows den Namen des Drucker in den Namen des Druckertreibers. Um wieder den richtigen Namen zu setzen, rechtsklicken Sie in mmc.exe den Drucker und wählen Eigenschaften...
5. Ändern Sie unter dem Reiter Allgemein den Namen, den er in CUPS hat und bestätigen Sie mit OK.



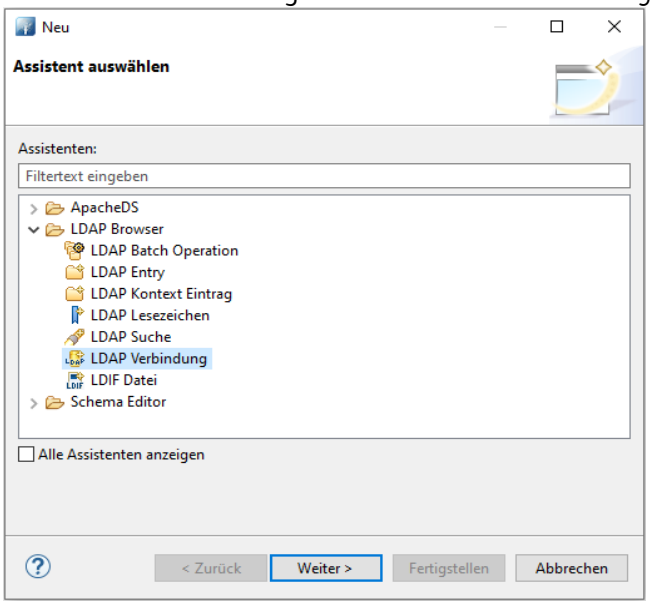
4.5. Drucker einzelnen Räumen zuweisen

Für die Raumzuweisung von Druckern eignet sich am besten das *Apache Directory Studio*. *Apache Direktory Studio* braucht *Java Development Kit*. Laden Sie dafür von https://www.oracle.com/de/java/technologies/javase-downloads.html die Installationsdatei und installieren Sie sie.

Laden Sie anschließend von https://directory.apache.org/studio/ die aktuelle Version von *Apache Direktory Studio* herunter und installieren Sie sie.

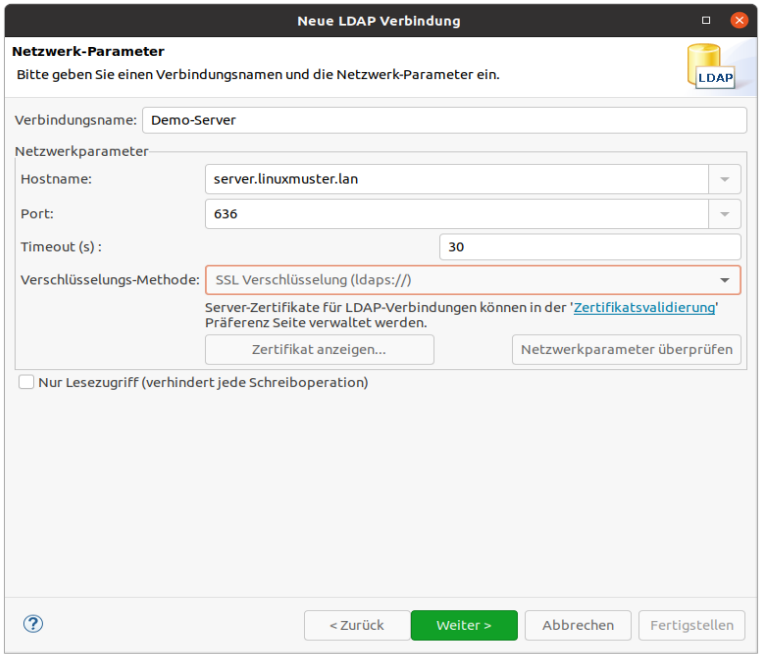
Schauen wir uns mit dem *Apache Directory Studio* die AD-Struktur etwas genauer an.

1. Starten Sie *Apache Directory Studio*.
2. Gehen Sie in der Menü-Leiste auf *Datei → Neu*.
3. Es öffnet sich ein Dialog. Wählen Sie *LDAP-Verbindung* und klicken auf weiter.



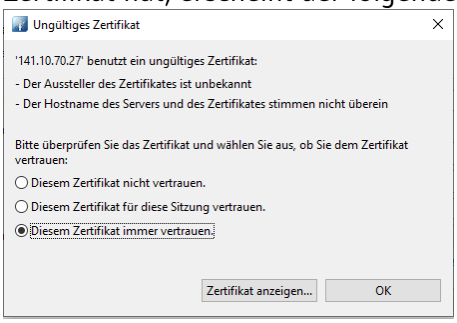
4. Geben Sie der Verbindung einen Namen und tragen Sie die Verbindungsdaten des

Musterlösungsservers ein.



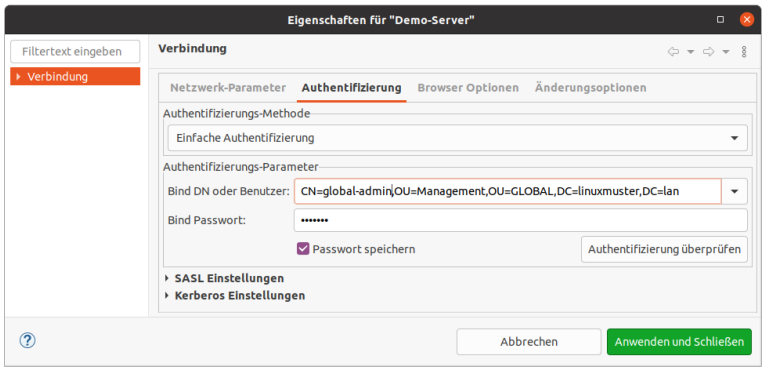
Unser Demoserver hat die URL *server.linuxmuster.lan*. Falls Sie die AD-Struktur des Servers Ihrer Schule anschauen wollen, geben Sie die IP-Adresse oder die URL ihres Schulservers ein. Beispiel: server.meineschule.de
In diesem Fall ist Voraussetzung, dass für den ldaps-Port 636 eine Portweiterleitung eingerichtet wurde.

5. Klicken Sie auf *Netzwerkparameter überprüfen*. Da unser Demo-Server nur ein selbst signiertes Zertifikat hat, erscheint der folgende Dialog:



Wählen Sie *Diesem Zertifikat für immer vertrauen* und klicken auf ok.
Wenn Sie jetzt auf *Netzwerkparameter überprüfen* klicken, sollte die Verbindung erfolgreich aufgebaut werden.

Klicken Sie auf *weiter*.



Als Bind DN tragen Sie *CN=global-admin,OU=Management,OU=GLOBAL,* gefolgt von Ihrer DN ein. Bei unserem Demo-Server ist das *CN=global-admin,OU=Management,OU=GLOBAL,DC=linuxmuster,DC=lan*

Wir wählen den global-admin, weil er Schreibrechte hat. Auf einem Produktiv-System sollte man sicherheitshalber einen Snapshot des Servers machen.

6. Klicken Sie auf *Fertigstellen*.

Der Baum des AD wird geladen.

Schreiben Sie sich in der Schulkonsole bei den Druckern ein.

Im AD-Baum sieht das dann so aus:

memberOf	CN=11a,OU=11a,OU=Students,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=infolaser,OU=printer-groups,OU=Devices,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=internet,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=intranet,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=itglaser,OU=printer-groups,OU=Devices,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=printing,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=role-teacher,OU=Groups,OU=GLOBAL,DC=linuxmuster,DC=lan
memberOf	CN=teachers,OU=Teachers,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=webfilter,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=wifi,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan

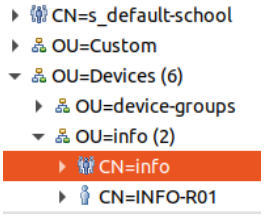
Im Eintrag des Benutzers sind die Drucker als memberOf eingetragen.

Beim Eintrag des Druckers ist der Benutzer als member eingetragen.

member	CN=rettich,OU=Teachers,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
name	infolaser

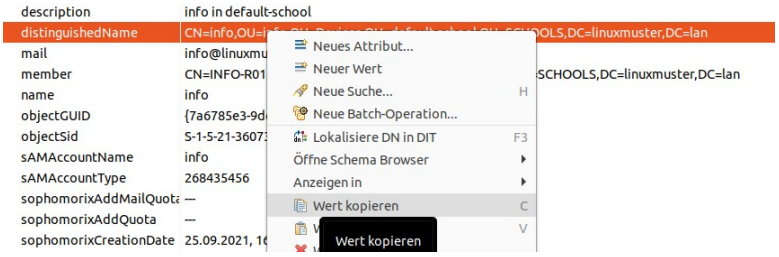
Genau so tragen wir die Gruppe des Informatik-Raums als Member in die Gruppe des InfoLasers ein:

1. Navigieren Sie zum Gruppeneintrag des Informatik-Raums.

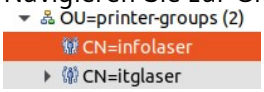


Im Mittleren Fenster werden die Einträge der Gruppe *info* angezeigt.

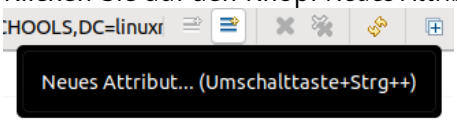
2. Kopieren Sie mit einem Rechtsklick den *distinguishedName*.



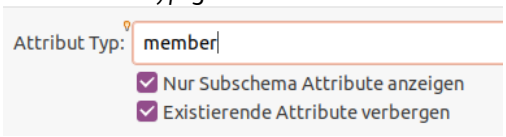
3. Navigieren Sie zur Gruppe des InfoLasers.



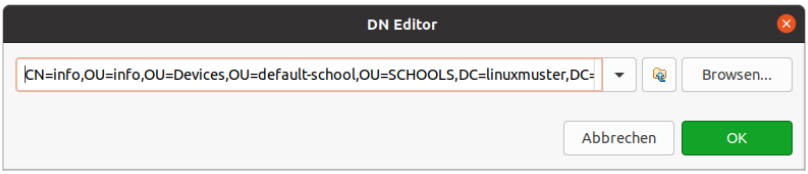
4. Klicken Sie auf den Knopf *Neues Attribut...*



5. Als *Attribut-Typ* geben Sie *member* ein und klicken anschließend auf *Fertigstellen*.



6. Fügen Sie jetzt mit *<Strg>+V* den vorher kopierten *distinguishedName* ein und klicken anschließend auf *OK*.



Alle Rechner die im Informatikraum stehen, werden ab „jetzt“ Zugriff auf den InfoLaser haben. Allerdings kann es eine ganze Weile dauern, bis sich dieser Eintrag auf die Druckerverteilung auswirkt.

4.6. Benutzern erlauben einen Druckertreiber zu installieren

Die Windows-Clients erlauben normalen Benutzern nicht, einen Druckertreiber zu installieren. Das müssen wir ändern, da sonst normale Benutzer nicht drucken können. Am einfachsten geht das mit folgendem Registry-Eintrag:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\
PointAndPrint
RestrictDriverInstallationToAdministrators=0 (DWORD)
```

Erzeugen Sie den Eintrag mit dem Registrierungs-Editor direkt in die Registry ein oder erzeugen Sie sich die datei win10.printer.reg mit folgendem Inhalt:

```
Windows Registry Editor Version 5.00
; linuxmuster.net 7 version
; notwendig, damit Druckertreiber installieret werden können
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\
PointAndPrint]
"RestrictDriverInstallationToAdministrators"=dword:00000000
```

Erzeugen Sie ein neues Image, damit die Firewall-Einstellungen und der Registry-Eintrag auf die Windows-Clients verteilt werden.

5. Firefox Proxy-Einstellungen über Gruppenrichtlinien festlegen

Wenn wir die Firefox Proxy-Einstellungen oder die eines anderen Browsers über Gruppenrichtlinien festlegen, kann sich Windows nicht mehr ungewollt updaten.
Ein weiterer Vorteil ist, dass die Benutzer ihre Proxy-Einstellungen nicht mehr selbst ändern können.
Allerdings sind hierfür noch einige Vorbereitungen nötig.

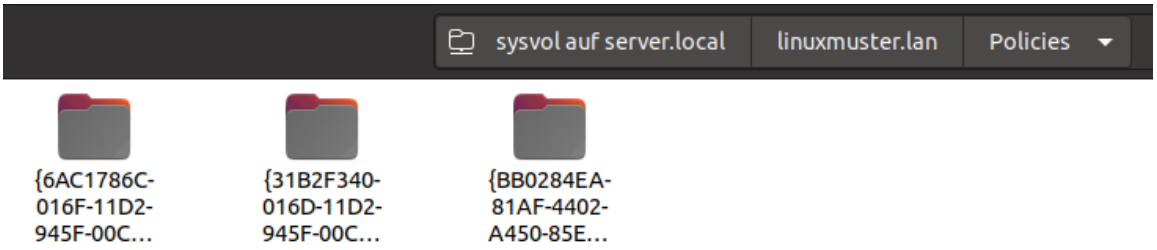
5.1. Template-Vorlagen auf den Server kopieren

Zunächst müssen wir die Mozilla-Firefox- und die Windows-GPO-Vorlagen auf den Server kopieren. Wir benötigen beide Vorlagen, da wir sonst nur noch die Mozilla-Firefox-GPO-Vorlagen bearbeiten können.

Die nächsten Schritte lassen sich auf einem Linux-Client besonders leicht ausführen, da Linux die benötigten Werkzeuge bereits mitbringt.

1. Laden Sie die Windows admx-Templates von https://www.microsoft.com/en-us/download/102157 herunter.
2. Öffnen Sie ein Terminal/Shell und entpacke mit msiextract Administrative\ Templates\ \ (.admx\)\ for\ Windows\ 10\ October\ 2020\ Update.msi die msi-Datei.
3. Öffnen das Verzeichnis Downloads das Verzeichnis

4. Öffnen Sie auf dem Server:

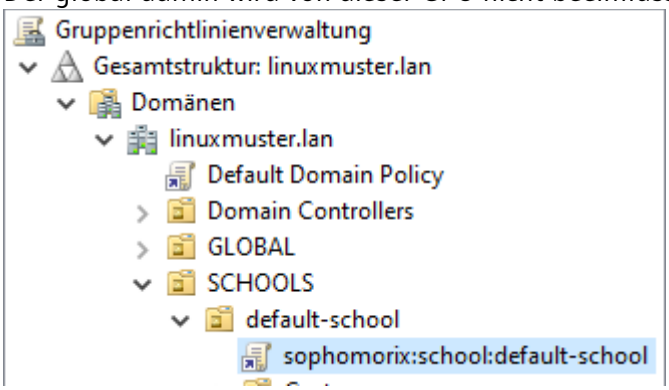


5. Und Kopieren PolicyDefinitions nach sysvol/linuxmuster.lan/Policies
6. Laden Sie die Mozilla-Firefox-Templates herunter und entpacken Sie sie:
   https://github.com/mozilla/policy-templates/releases
7. Kopieren Sie den Inhalt von Downloads/policy_template_v3.2/windows nach sysvol/linuxmuster.lan/Policies/PolicyDefinitions.

5.2. Die Gruppenrichtlinie erstellen

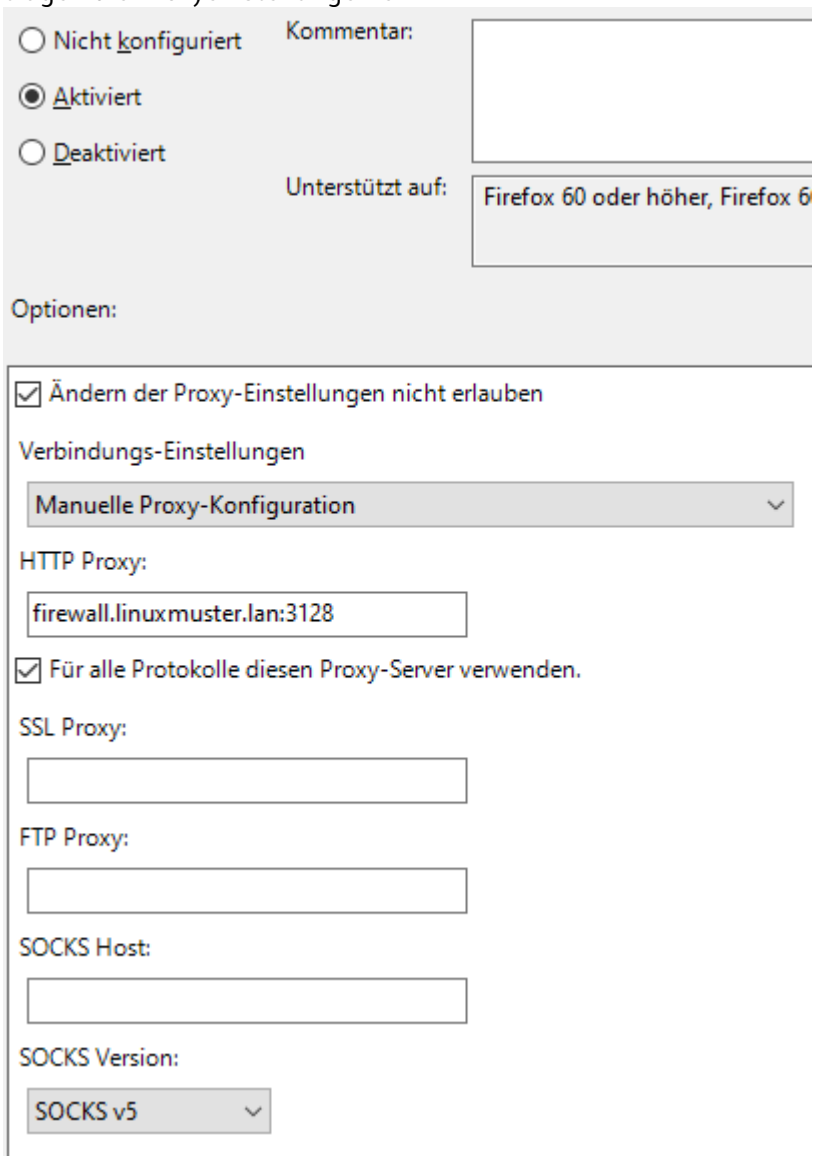
Da die neue Proxy-Einstellung für alle Rechner in unserem Netzwerk gelten soll, bearbeiten wir die GPO Default Domain Policy und definieren dort die Proxy-Einstellungen.

1. Solle die GPO nur für Lehrer und Schüler gelten, öffnen Sie die Gruppenrichtlinienverwaltung, navigieren zur GPO sophomorix:school:default-school und bearbeiten sie.
   Der global-admin wird von dieser GPO nicht beeinflusst, da er im LDAP-Baum weiter oben liegt.



2. Navigieren Sie im Gruppenrichtlinienverwaltungs-Editor zu Computerkonfiguration → Richtlinien → Administrative Vorlagen → Mozilla → Firefox.

3. Doppelkilicken Sie dort die Richtlinienvorlage Proxy Einstellungen, aktivieren die GPO und tragen die Proxyeinstellungen ein.



4. Bestätigen Sie mit OK und schließen den Gruppenrichtlinienverwaltungseditor und die Gruppenrichtlinienverwaltung.

6. Softwareinstallation mittels Gruppenrichtlinien

Über GPOs können drei Arten von Paketen installiert werden: Windows-Installationspakete mit der Dateiendung .MSI, Transformationsdateien mit der Dateiendung .MST und Patch-Dateien, die auf .MSP enden.

6.1. Software bereitstellen

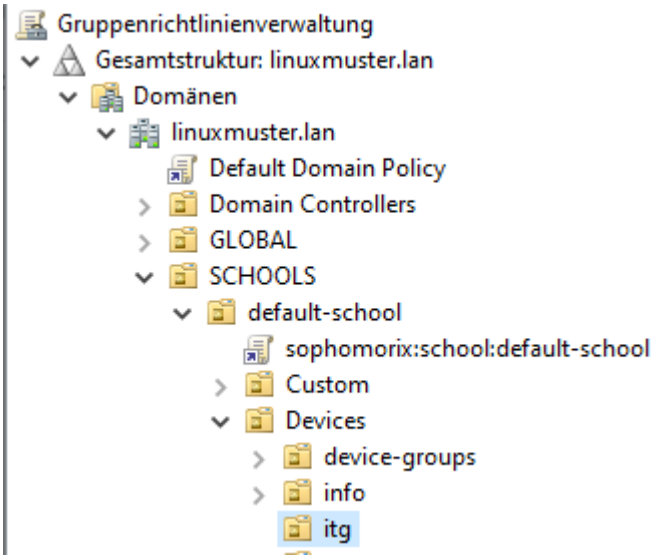
Zunächst sollte die Software auf einem Pfad abgelegt werden, von dem aus die Installation ausgeführt werden kann. Dieses Share sollte für die Clients erreichbar sein:
`\\server\sysvol\domänenname\`

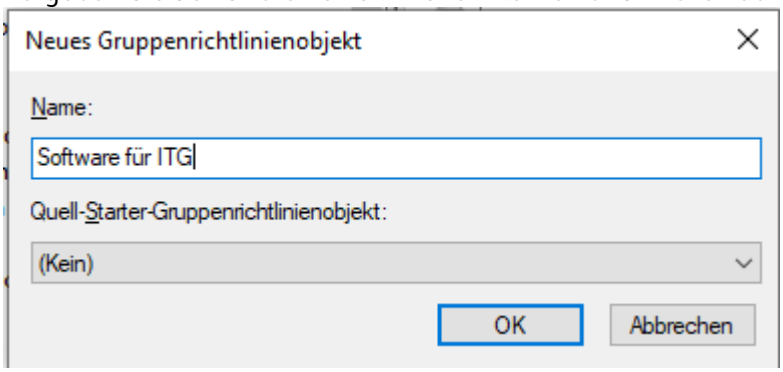
Legen Sie hier einen Unterordner `Software` an und legen Sie die MSI-Pakete dort ab.

Laden Sie die Installationspakete für Libreoffice herunter und legen Sie sie im eben angelegten Verzeichnis ab.

6.2. Neue Gruppenrichtlinie erzeugen

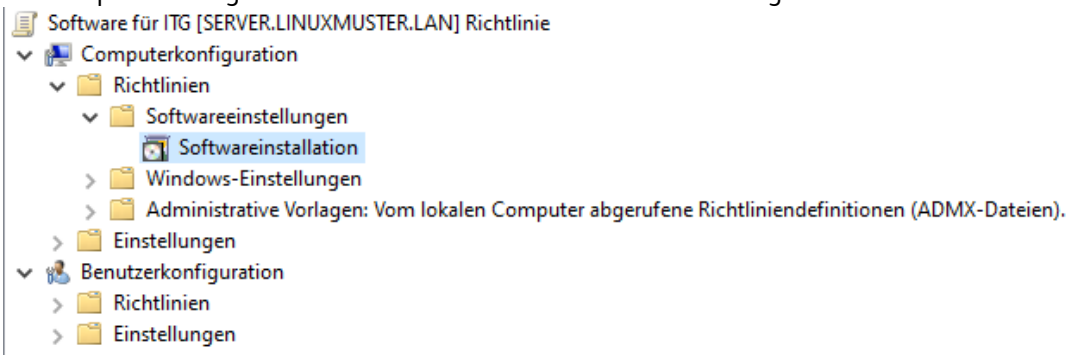
Um eine GPO, die LiberOffice im ITG-Raum installiert anzulegen, gehen Sie wie folgt vor:

1. Starten Sie als *global-admin* die Gruppenrichtlinienverwaltung und gehen Sie zu *Gesamtstruktur: linuxmuster.lan → Domänen → linuxmuster.lan → Schools → default-school → devices → itg*.


2. Wählen Sie nach einem Rechtsklick *Gruppenrichtlinienobjekt hier erstellen und verknüpfen*.
3. Vergeben Sie der GPO einen sinnvollen Namen und klicken auf ok.


4. Machen Sie einen Rechtsklick auf die neue GPO und wählen bearbeiten.
Der Gruppenrichtlinienverwaltungs-Editor öffnet sich.
5. Da wir die Software installieren wollen, wenn sich der Rechner im ITG-Raum befindet, gehen wir

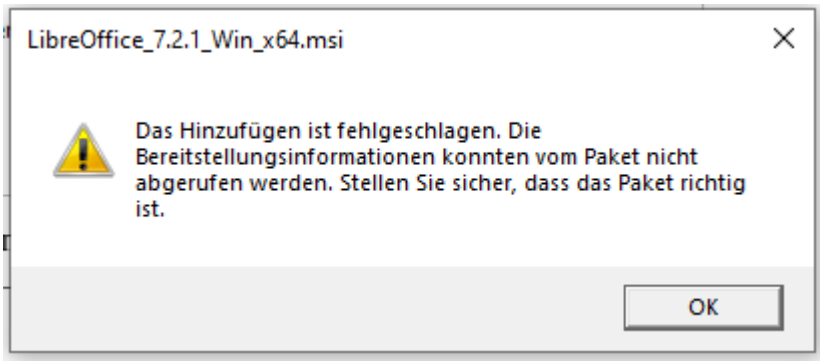
zu Computerkonfiguration → Richtlinien → Softwareeinstellungen → Softwareinstallation.



6. Machen Sie einen Rechtsklick auf *Softwareinstallation*, wählen *Neu* → *Paket* und geben den Pfad zum Paket ein.
7. Wählen Sie bei der Bereitstellungsmethode *Zugewiesen* aus und bestätigen mit *Ok*.

Damit die neue GPO am Ziel-PC greift, muss dieser neu gestartet werden.

Bei LibreOffice erscheint eine Fehlermeldung.



Das liegt wohl daran, dass im Installer mehr als eine Sprache verfügbar sind.

Nach dieser Anleitung kann die Installationsdatei bearbeitet werden:

1. Laden Sie *SuperOrca* von hier.
2. Installieren Sie *SuperOrca* und starten es.
3. Laden Sie mit *File* → *Open* den Installer.
4. Klicken Sie auf *Tools* → *Summary Information…*
5. Löschen Sie im Feld *Languages* alle Einträge bis auf 1033.
6. Klicken Sie auf *Apply* und anschließend auf *Close*.
7. Speichern Sie die Datei unter einem anderen Namen ab.

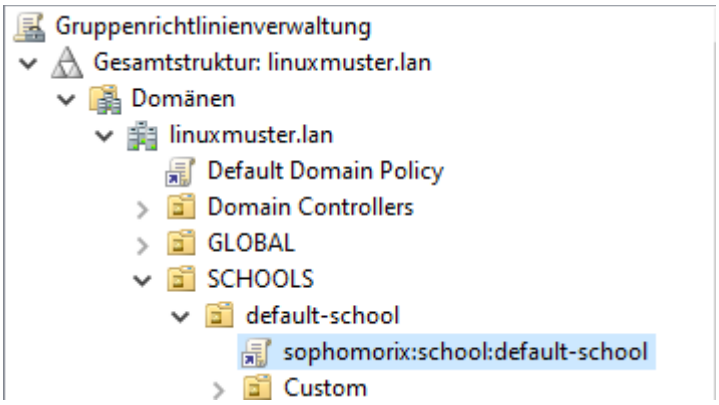
Jetzt lässt sich auch der Installer von LibreOffice in die GPO einfügen.

6.3. Beim Start des Clients auf die Netzwerkverbindung warten

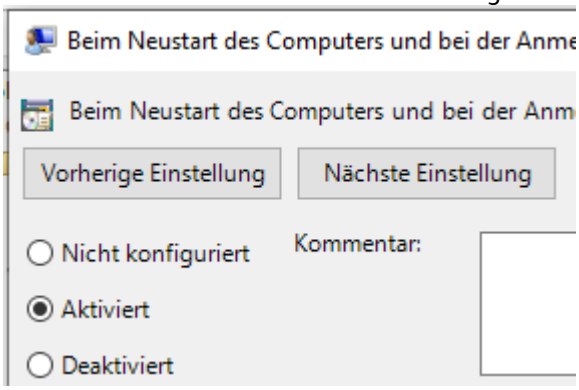
Es kann vorkommen, dass die GPO nicht übernommen wird, weil das Share, auf dem sich die Installationsdateien befinden, noch nicht verfügbar ist.

In diesem Fall müssen Sie für die Client-Rechner der gesamten Schule mittels der Gruppenrichtlinienverwaltung die lokale GPO *Beim Neustarten des Computers und bei der Anmeldung immer auf das Netzwerk warten* aktivieren:

1. Starten Sie als *global-admin* die Gruppenrichtlinienverwaltung.
2. Gehen Sie zu *sophomorix:school:default-school* und wählen Sie mit einem Rechtsklick *Bearbeiten*.



3. Doppelklicken Sie im Gruppenrichtlinienverwaltungs-Editor *Computerkonfiguration → Richtlinien → Administrative Vorlagen → System→ Anmelden -> Beim Neustarten des Computers und bei der Anmeldung immer auf das Netzwerk warten*.
4. Aktivieren Sie die Richtlinie und bestätigen Sie mit *OK*.



Wenn jetzt ein Rechner gestartet wird, wartet er beim Bootvorgang, bis die Netzwerkverbindungen stehen. So ist sicher gestellt, dass die Software auch installiert werden kann.

6.4. MAC-Adressen

server	00:0c:29:64:ba:aa	000c2964baaa
firewall	00:0C:29:6B:8F:01	000C296B8F01
info-r01 (linux)	00:0C:29:59:27:F3	000C295927F3
itg-r01 (win)	00:0C:29:73:0A:FA	000C29730AFA

7. Quellen

- Linuxmuster.net – Dokumentation: https://docs.linuxmuster.net/de/latest/
- Samba-Wiki: https://wiki.samba.org/index.php/Main_Page
- HelgeSverre – LibreOffice MSI Package GPO Error: https://helgesverre.com/blog/libreoffice-msi-gpo-error/
- Apache License 2.0: https://www.apache.org/licenses/LICENSE-2.0
- CC BY 4.0: https://creativecommons.org/licenses/by/4.0/
- CC BY-SA 4.0: https://creativecommons.org/licenses/by-sa/4.0/

8. Informationen zum Dokument

Titel	Gruppenrichtlinien
Untertitel	Eine Einführung
Bereich	Netzwerke/Linux
Autor	Peter Schmidt und Mathias Rettich
Datum	6. Oktober 2021
Lizenz	CC BY-SA 4.0