

M159 - Directory Services

Thema 2

Arbeitsblatt 2

1 Lernziele

Im AB 2 verfolgen wir folgende Lernziele:

- Installation und Konfiguration des LDAP Access Managers (LAM)
- Übersicht der Objekte eines AD mit der LDAP-Brille
- Anlegen eines Users und Hinzufügen in eine Gruppe
- TGT für neu erstellten User beziehen und Testverbindung herstellen

2 Installation und Konfiguration LAM

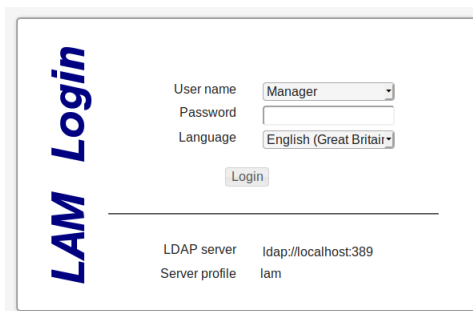


Abbildung 1: LAM Login Fenster

Im letzten Arbeitsblatt haben wir vmLS1 als DC konfiguriert. Im folgenden testen wir nun den LDAP-Dienst und verwenden dazu den LAM. Installieren Sie dazu zuerst die ldap-tools und den LAM (LDAP-Account-Manager):

```
sudo apt-get install smbldap-tools
```

```
sudo apt install ldap-account-manager
```

Danach werden wir eine Verbindung mit dem Browser von vm1p1 auf <http://192.168.220.10/lam/> herstellen. Die Konfiguration des LAM ist im Buch *Samba 4 - Das Praxisbuch für Administratoren* auf den Seiten 110ff im Detail beschrieben (siehe Modulordner). Sie können sich auch an diese Anleitung halten. Diese ist etwas kürzer und berücksichtigt unsere Laborumgebung.

2.1 LAM-Profil erstellen

Klicken sie oben rechts auf **LAM configuration/Edit server profiles/Manage Server Profiles**. Das LAM-Masterpasswort ist lam. Legen Sie ein neues Profil an mit folgenden Angaben:

Profile name: sam159Domain

ProfilePassword: sml12345

Template: windows_samba4

Klicken sie **ADD**. Danach werden sie nach dem Masterpasswort gefragt. Geben sie lam ein. Anschliessend gelangen sie automatisch in das neu erstellte Profil.

Abbildung 2: LAM-Profil erstellen

2.2 LAM-General Settings definieren

Hier definieren sie unter General Settings folgende Werte:

Server address: ldap://vmls1.sam159.iet-gibb.ch

Tree suffix: dc=sam159,dc=iet-gibb,dc=ch

Default Language: Deutsch

Time zone: Europe/Zurich

List of valid user: cn=Administrator,cn=users,dc=sam159,dc=iet-gibb,dc=ch

Abbildung 3: LAM General Settings

2.3 LAM-Account Types definieren

Unter *Account Types*, *Users*, *Groups* und *Hosts* jeweils:

LDAP suffix:: `dc=sam159,dc=iet-gibb,dc=ch`

und unter *Module settings*:

Windows Domains: `sam159.iet-gibb.ch`

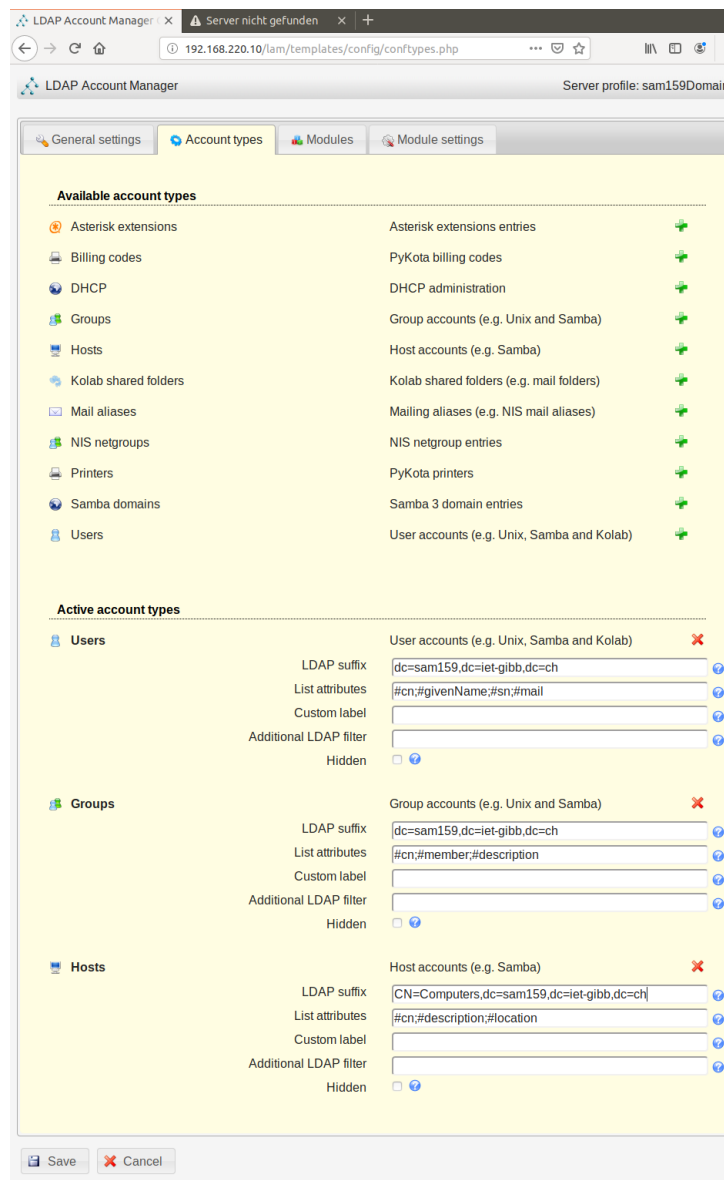
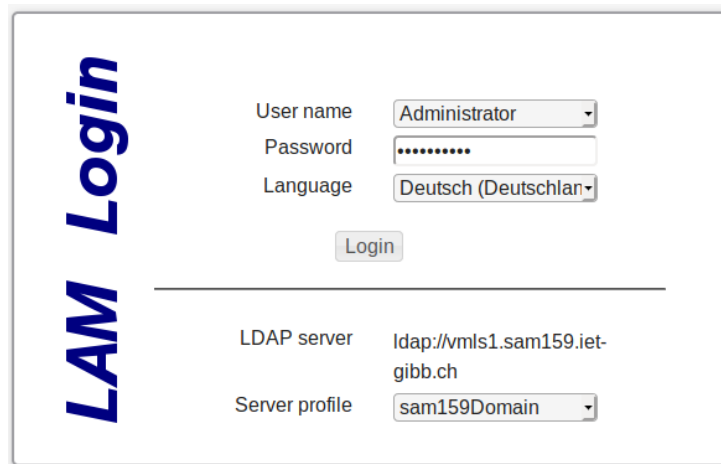


Abbildung 4: LAM Account Types

Am Ende alles abspeichern. Jetzt können sie sich am LAM mit dem Domainadministrator anmelden. Wir sind nun damit in der Lage, User und Gruppen anzulegen.

WICHTIG: damit die Verbindung klappt, muss in der `smb.conf`-Datei in der `[global]`-Section folgender Eintrag stehen:

`ldap server require strong auth = no`



The image shows the LAM Login interface. On the left, the text "LAM Login" is written vertically in a large, blue, stylized font. To the right, there is a login form with the following fields: "User name" with a dropdown menu showing "Administrator", "Password" with a masked input field (dots), and "Language" with a dropdown menu showing "Deutsch (Deutschland)". Below these fields is a "Login" button. Further down, there are two more fields: "LDAP server" with the value "ldap://vmls1.sam159.iet-gibb.ch" and "Server profile" with a dropdown menu showing "sam159Domain".

Abbildung 5: LAM Administrator-login

Das Passwort des **Administrators** lautet: SmL12345**
Melden sie sich an und klicken Sie auf **Tree View**

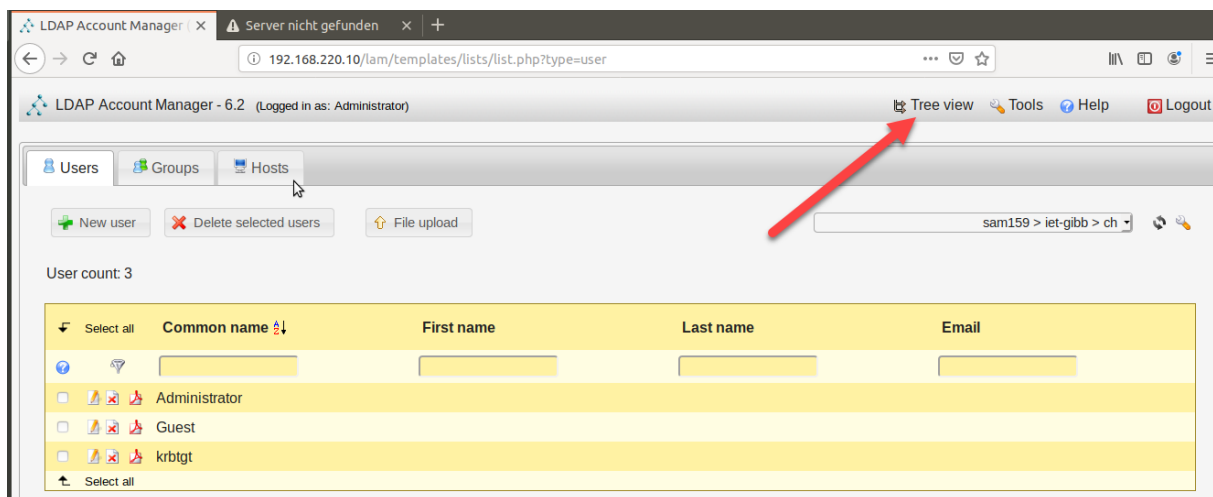


Abbildung 6: Tree View

Damit erhalten sie eine Übersicht aller Objekte im Active Directory:

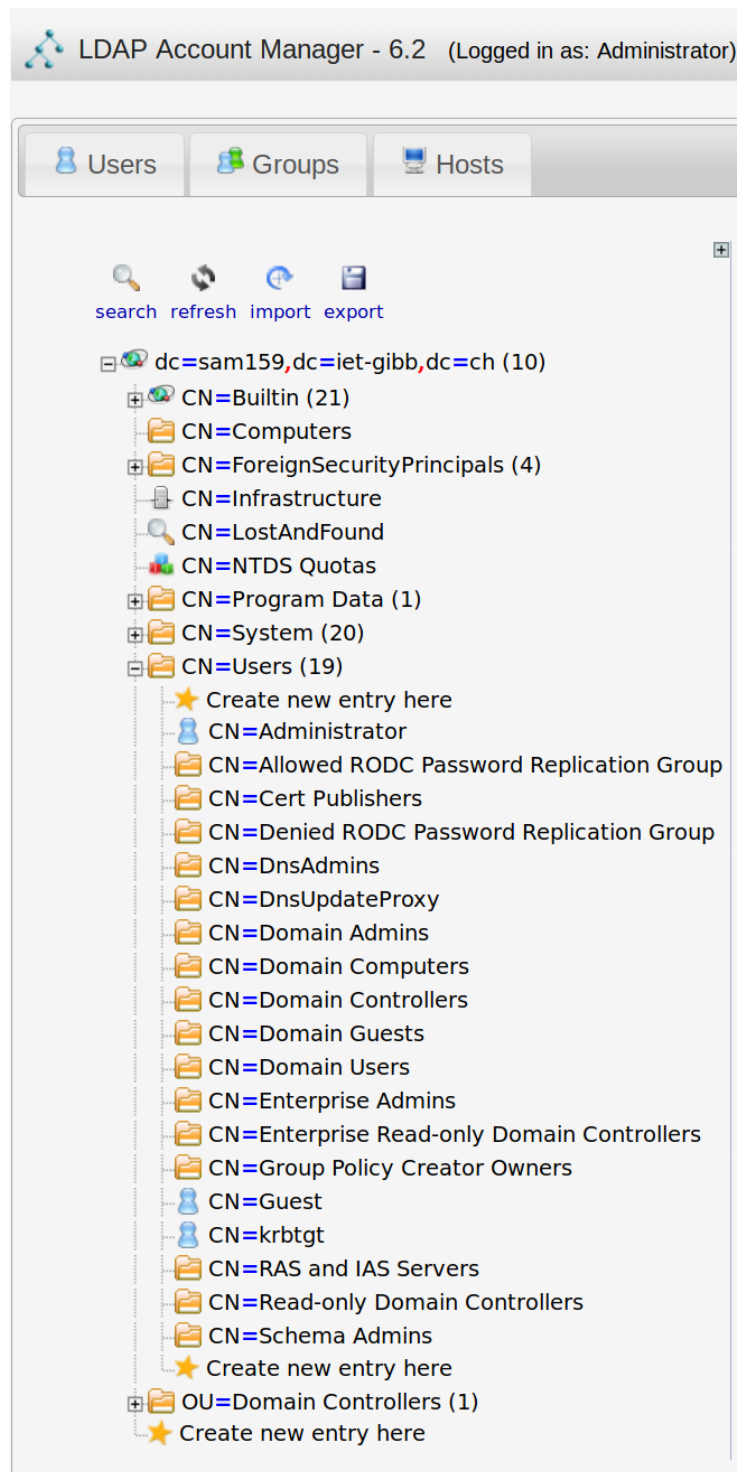


Abbildung 7: Objekte des Active Directory

3 Aufgaben

3.1 Neuen User im LDAP anlegen und TGT lösen

To Do:

- Legen sie einen Benutzer an. Als Name verwenden sie ihren Vornamen. Passwort SmL12345**
- Fügen sie den Benutzer in die Gruppe der Domain Admins

- Wie lautet der *distinguishedName* (DN:) dieses Benutzers? Wo können sie das herauslesen?
- Wie lautet der DN: der Gruppe Domain Admins ?
- Gehen sie ins Terminal der vmLS1 und lösen sie ein TGT für den erstellten User.
- Erstellen sie mit dem neuen User eine *kerberisierte* Testverbindung. Verwenden sie dazu den Befehl `smbclient` . Wie lautet der ganze Befehl und was sehen sie?
- Finden Sie im AD die SID vom Administrator und von der Gruppe *Domain Admins*. Vergleichen Sie die Nummern und konsultieren sie die Tabelle des nachfolgenden Kapitels.

3.2 User, Gruppen und DNS mit RSAT Tools verwalten

RSAT steht für *Remote Server Administration Tools*. Dies sind Werkzeuge, welche für die Verwaltung einer AD-Domäne verwendet werden können. RSAT-Tools stammen von Microsoft und sind für Windows-Client Rechner vorgesehen. Wir sind damit in der Lage, den SAMBA-AD-DC von einem Windows-Rechner aus zu verwalten. Lösen sie folgende Aufgaben:

To Do:

- Fügen Sie vmWP1 in die Domain `sam159.iet-gibb.ch` ein. Was müssen Sie beim Client netzwerkseitig unbedingt beachten, damit das klappt?
- Melden Sie sich nach dem Neustart mit dem Domain-Administrator auf vmWP1 an
- Installieren Sie die RSAT-Tools. Vergewissern sie sich vorher, welche Windows 10-Version bei Ihnen installiert ist (1709, 1803 oder 1809 oder ?. Der Befehl `winver` hilft ihnen dabei die Version zu finden) und laden sie das entsprechende RSAT-Package herunter: <https://www.microsoft.com/en-US/download/details.aspx?id=45520>. Anschliessend installieren sie dieses. RSAT wird von Windows wie ein Update behandelt.
- Welche Domain-Admin Tools stehen ihnen jetzt auf vmWP1 zur Verfügung?
- Legen Sie mit RSAT einen User an und vergleichen Sie die Angaben durch die LAM-Brille.
- Kontrollieren sie die DNS-Einträge auf dem DNS-Server mit RSAT-Tools. Alles ok?

3.3 Active Directory mit ldapsearch abfragen

Das AD kann auch mit `ldapsearch` abgefragt werden. Dazu müssen die `ldap-utils` installiert sein. Installieren sie diese auf vmLP1. Eine Abfrage könnte dann so aussehen:

```
ldapsearch -x -LLL -H ldap://vmLS1.sam159.iet-gibb.ch -b dc=sam159,dc=iet-gibb,dc=ch -D CN=administrator,CN=Users,DC=sam159,DC=iet-gibb,DC=ch -w SmL12345** '(cn=administrator)'
```

Lassen Sie ihre neu erstellten User so anzeigen! Was erhalten sie, wenn sie `'(cn=*)'` schreiben ?

4 Fileserver in der Domäne

Bis jetzt haben wir nur einen Domaincontroller. Auf den Domaincontrollern sollten keine Daten gespeichert werden; diese sollen immer auf einem Fileserver liegen. Grund: Nur Fileserver sind in der Lage, bei einer Domäne mit Linux- und Windows-Clients ein einheitliches ID-Mapping (UIDs und GIDs) zu garantieren. Auch Microsoft rät davon ab, Daten auf einem Domaincontroller zu speichern.

Sie lernen hier auch, wie Konfigurationen des Fileservers in die Registry ausgelagert werden können.

4.1 Das Problem des ID-Mappings

Linux und Windows verwenden unterschiedliche Arten der ID-Zuweisung für User und Gruppen. Die im AD gespeicherten SIDs der Gruppen und Benutzer müssen auf irgendeine Art und Weise auf GIDs und UIDs umgesetzt werden. Wer ist für diese Umsetzung zuständig? Es ist der Dienst

Winbind

Winbind unterstützt verschiedene Arten. Die zu verwendende Art wird in der Datei `smb.conf` definiert.

Wir werden die *rid-Methode* verwenden:

Bei dieser Methode wird die RID eines AD-Benutzers oder einer AD-Gruppe für das ID-Mapping verwendet. Die RID wird beim Anlegen des Users oder der Gruppe automatisch vergeben und ist daher immer eindeutig. Mit dieser Methode schafft man es auch für Linux-Benutzer einer Domain ein einheitliches Mapping herzustellen.

4.1.1 Repetition: Was ist eine SID?

SIDs (Security Identifier) gehören zu den sogenannten *Security Principals* in einer Domäne. Die Security Principals erhalten mit der SID ihre Kennung (Eindeutigkeit). Eine SID besteht aus 2 Teilen:

- eindeutige **Domänenkennung**
- eindeutige **Objektkennung** (Relative Identifier **RID**)

Anhand der SIDs eines Objektes einer Active Directory-Domäne ist es möglich, den Zugriff auf Ressourcen zu vergeben oder zu verweigern. SID's in unserem AD:

- (1) 1-5-21-3770624505-2901393275-1935834510-500
- (2) 1-5-21-3770624505-2901393275-1935834510-512

- (1) Administrator
- (2) Domain Admins Gruppe

SIDs bestehen aus folgenden Bestandteilen

S- Kennzeichen für SID

1- Revisionsebene

5- Identifizierungsautorität

21-3770624505-2901393275-1935834510- Domäne/Computer

500/512 - Relativer Identifier (RID)

In einem AD gelten bestimmte Regeln wie SIDs vergeben werden. Ein bei der Installation eingerichtetes Administrations-Objekt hat immer die gleich Endung.

Folgende Sicherheitskennungen sind in einem ADDS vordefiniert:

SID	Zuordnung
S-1-5-<Domäne>-500	Administrator-Benutzerkonto
S-1-5-<Domäne>-501	Gast-Benutzerkonto
S-1-5-<Domäne>-502	KRBTGT-Servicekonto
S-1-5-<Domäne>-512	Domain Admins
S-1-5-<Domäne>-513	Domain User Group
S-1-5-<Domäne>-514	Domain Guest Group
S-1-5-<Domäne>-515	Domain Computer Group
S-1-5-<Domäne>-516	Domain Controller Group
S-1-5-<Domäne>-519	Organisations-Admins
S-1-5-<Domäne>-520	Richtlinien-Ersteller-Besitzer Gruppe
S-1-5-32-544	Administratoren-Gruppe
S-1-5-32-545	Benutzer-Gruppe

To Do:

- Wie lauten ihre SIDs des Administrators, der Domain Users und des neu erstellten Users? Wie findet man diese im LAM? Wie findet man diese aus Windows? Die Nummern entsprechen den vordefinierten Werten von obiger Tabelle?