M159 - Directory Services

Thema 2

Arbeitsblatt 3

1 Lernziele

Im AB 3 verfolgen wir folgende Lernziele:

- Einrichtung des Fileservers `vmls2` in den Realm `SAM159.IET-GIBB.CH`
- Funktion des ID-Mappings Windows <–> Linux verstehen
- Behehle kennen, um von Linux aus AD User und AD Gruppen aufzulisten

2 Einrichtung des Linux-Fileservers `vmls2`

Jetzt geht es darum einen Fileserver in der Domain einzurichten. Daten in einer Domain sollten nie auf dem Domain-Controller liegen sondern immer auf einem dedizierten Fileserver. Bei uns ist das `vmLS2`.

Ein Domaincontroller hat immer ein eigenes ID-Mapping. Selbst bei mehreren Domain-Controllern in einer Domain ist das ID-Mapping auf jedem Controller verschieden. Ein Fileserver garantiert, dass das ID-Mapping für die Datei-Dienste immer gleich ist. Auch Microsoft rät davon ab, Fileservices auf einem Domaincontroller anzubieten.

Unter Linux und Windows gibt es unterschiedliche Arten der ID-Zuweisung (vgl. AB02, Thema SID). Wie bereits in AB02 beschrieben, verwenden wir für das Mapping auf dem Fileserver die *rid*-Methode. Dabei wird die RID des Users oder der Gruppe verwendet. Die RID wird beim Anlegen der Gruppe oder des Users vom controller automatisch vergeben und ist immer eindeutig. Wir müssen nur darauf achten, dass der Bereich für das ID-Mapping auf allen Mitgliedern der Domain einheitlich verwendet wird. Das wird kein Problem sein, da wir hier nur mit einem Fileserver arbeiten werden.

2.1 Netzwerk konfigurieren und Samba auf `vmLs2` installieren

- Kontrollieren sie zuerst auf `vmLS2` die Netzwerkkonfiguration. Als DNS Server muss `vmLS1 - 192.168.220.10` und als search-Domain `sam159.iet-gibb.ch` verwendet werden. Kontrollieren Sie diese Angaben mit dem Befehl
  `systemd-resolve --status`
  Korrekturen führen sie bitte mit `netplan` aus. Passen sie dazu das `.yaml`-File in `/etc/netplan` an und aktivieren sie die Konfiguration mit `netplan apply`.

```
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      addresses: [ 192.168.220.11/24 ]
      gateway4: 192.168.220.1
      nameservers:
        search: [ sam159.iet-gibb.ch ]
        addresses: [ 192.168.220.10 ]
```

Listing 1: `/etc/netplan/00-eth0.yaml` von `vmLS2`

- Installieren Sie Samba auf `vmLS2` mit:
  `apt install samba samba-common-bin smbclient heimdal-clients libpam-heimdal`
  Geben sie währen der Installation als Realm `SAM159.IET-GIBB.CH` und als Kerberos Server `vmLS1.sam159.iet-gibb.ch`.
  Installieren Sie auch:
  `apt install libnss-winbind libpam-winbind`

2.2 Grundkonfiguration des Fileservers

Dazu müssen folgende Einträge in `/etc/samba/smb.conf` gemacht werden:

```
[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
   client ipc signing = auto
   vfs objects = acl_xattr
```

Listing 2: Einträge in der Datei `/etc/samba/smb.conf` von `vmLS2`

Die Parameter haben die folgenden Bedeutungen:

- **workgroup = sam159** Hier wird der NetBIOS-Name der Domäne angegeben. Auch als Mitglied im AD heisst der Parameter workgroup.
- **realm = SAM159.IET-GIBB.CH** Bei dem realm handelt es sich um die Information für die Kerberos-Domäne. Für diesen Realm wird sich der Samba-Server einen KDC suchen. Beim Key Distribution Center (KDC) handelt es sich um die Zentral Vergabestelle der Kerberos-Tickets für Authentifizierung.
- **security = ADS** Damit legen Sie fest, dass Ihr Server ein Mitglied in einer AD-Domäne ist.
- **winbind enum users = yes** Ohne diesen Parameter würden die Benutzer auf dem lokalen Linux-System nicht angezeigt, wenn Sie die Benutzer mit getent passwd abfragen. Nur einzelne Benutzer könnten über das Kommando getent passwd username abgefragt werden. In Domänen mit vielen Benutzern sollten Sie diesen Parameter immer auf der Standardeinstellung no belassen, da der Aufwand der Umrechnung des RIDs auf die IDs sehr aufwendig ist und das System stark belasten kann.
- **winbind enum groups = yes** Dieser Parameter hat die gleiche Aufgabe wie vorher schon der Parameter für die Benutzer. Auch hier gilt: In grösseren Umgebungen sollte der Wert dieses Parameters immer auf no gesetzt sein.
- **winbind use default domain = yes** Haben Sie nur eine Domäne, können Sie mit diesem Parameter dafür sorgen, dass nur die Benutzernamen von winbind übergeben werden, ohne die Domäne vor den Namen zu stellen. ***Wenn Sie aber Vertrauensstellungen zu anderen Domänen herstellen wollen, dürfen Sie diesen Parameter auf gar keinen Fall setzen.***
- **winbind refresh tickets = yes** Mit diesem Parameter werden Kerberos-Tickets automatisch erneuert, wenn der Benutzer angemeldet ist und das Ticket abläuft.
- **template shell = /bin/bash** Diesen Parameter dürfen Sie auf gar keinen Fall vergessen. Ohne ihn kann sich ein Benutzer aus dem Active Directory zwar über ssh anmelden, aber er wird sofort wieder abgemeldet, da der Benutzer im Active Directory keine Shell zugewiesen bekommt, diese

aber für eine erfolgreiche Anmeldung benötigt wird. Nur wenn Sie das rfc-2307-Schema verwenden und eine Shell bei den Benutzern eingetragen haben, können Sie diesen Parameter ignorieren. Setzen Sie diesen Parameter nicht, ist die Standardshell /bin/false; damit können Sie verhindern, dass sich ein Benutzer auf dem Server über ssh oder die lokale Konsole anmeldet.

- **idmap config * : range = 10000 - 19999** Neben den Gruppen und Benutzern, die Sie als Administrator anlegen, gibt es noch die Built-in-Groups. Diese Gruppen haben eine eigene verkürzte SID. Für diese Gruppen müssen Sie auch das ID-Mapping konfigurieren. Die Konfiguration der Built-in-Groups erfolgt über den Stern in idmap config * : range = 10000 - 19999. Eigentlich müssten Sie auch noch den Parameter idmap config * : backend = tdb konfigurieren, aber dieser Parameter wird von Samba4 automatisch gesetzt. Testen können Sie das mit dem Kommando testparm.
- **idmap config SAM159 : backend = rid** Die IDs der Benutzer werden aus dem RID der AD-Benutzer generiert.
- **idmap config SAM159 : = 1000000 - 1999999** Hier legen Sie den Bereich fest, in dem sich die UIDs der Benutzer befinden sollen.

2.3 `vmLS2` als Mitglied zur Domäne hinzufügen

Machen Sie ein Reboot. Dann führen sie den join mit folgendem Befehl aus:
`net ads join -Uadministrator`
Das `administrator`-Passwort ist `SmL12345**`. Sie sollten folgende Meldung kriegen:

```
Enter administrator's password:
Using short domain name -- SAM159
Joined 'VMLS2' to dns domain 'sam159.iet-gibb.ch'
DNS Update for vmls2.sam159.iet-gibb.ch failed: ERROR_DNS_UPDATE_FAILED
DNS update failed: NT_STATUS_UNSUCCESSFUL
```

Der DNS-Fehler entsteht, weil wir `vmLS2` bereits im DNS eingetragen haben. Wenn sie keine Erfolgsmeldung für ein *join* erhalten, kontrollieren sie das `/etc/krb5.conf`-File. Dieses sollte gleich sein wie das auf `vmLS1`.

Da wir bereits `winbind` installiert haben, können sie mit folgenden Befehlen überprüfen, ob die Benutzer und Gruppen aus dem Active Directory übernommen wurden:
`wbinfo -u` listet Benutzer und `wbinfo -g` listet die AD-Gruppen. Testen Sie das! Die Ausgaben sollten etwas so aussehen:

```
root@vmls2:~# wbinfo -u
administrator
krbtgt
thomas
guest
thomas2
root@vmls2:~# wbinfo -g
allowed rodc password replication group
enterprise read-only domain controllers
denied rodc password replication group
read-only domain controllers
group policy creator owners
ras and ias servers
domain controllers
enterprise admins
domain computers
cert publishers
dnsupdateproxy
domain admins
domain guests
schema admins
domain users
dnsadmins
```

mit `wbinfo -?` sehen sie, was mit diesem Befehl alles möglich. Die SID des `administrators` erhält man so: `wbinfo --name-to-sid=administrator`. Infos zur Domain mit `wbinfo --domain-info=SAM159` oder wenn man wissen möchte, welches der DC der Domain ist mit `wbinfo --dc-info=SAM159`.

Damit wir Rechte an die Benutzer im Dateisystem vergeben können, muss die Datei `/etc/nsswitch.conf` angepasst werden:

```
passwd:         compat systemd winbind
group:          compat systemd winbind
shadow:         compat winbind
```

Listing 3: Einstellung `/etc/nsswitch.conf`

Mit `getent passwd` und `getent group` können nun auch die gemappten Linux-User und Gruppen angezeigt werden. Sie sollten am Ende der Ausgaben die Domain-User bzw. Gruppen sehen. Beachten Sie dabei die ID's!
Hinweis: Sollte bei Ihnen beim `getent`-Befehl kein Output erfolgen, müssen sie die Packages `libnss-winbind` und `libpam-winbind` mit `apt install` installieren.

Hier sehen sie nun die lokalen User und Gruppen zusammen mit den Active Directory User und Gruppen. Beachten sie bei den AD Objekten die UIDs und GIDs. Diese sind nun so, wie wir es im `/etc/smb.conf` eingestellt haben.

```
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
vmadmin:x:1000:1000:vmadmin,,,:/home/vmadmin:/bin/bash
mysql:x:106:111:MySQL Server,,,:/nonexistent:/bin/false
lampuser:x:1001:1001::/var/www:/bin/false
proftpd:x:107:65534::/run/proftpd:/usr/sbin/nologin
ftp:x:108:65534::/srv/ftp:/usr/sbin/nologin
administrator:*:1000500:1000513::/home/SAM159/administrator:/bin/bash
krbtgt:*:1000502:1000513::/home/SAM159/krbtgt:/bin/bash
thomas:*:1001103:1000513::/home/SAM159/thomas:/bin/bash
guest:*:1000501:1000513::/home/SAM159/guest:/bin/bash
jtom:*:1001109:1000513::/home/SAM159/jtom:/bin/bash
thomas2:*:1001105:1000513::/home/SAM159/thomas2:/bin/bash
root@vmls2:~#
```

Abbildung 1: getent passwd

```
sambashare:x:110:vmadmin
mysql:x:111:
ssl-cert:x:112:
lampuser:x:1001:
rdma:x:113:
winbindd_priv:x:114:
allowed rodc password replication group:x:1000571:
enterprise read-only domain controllers:x:1000498:
denied rodc password replication group:x:1000572:
read-only domain controllers:x:1000521:
group policy creator owners:x:1000520:
ras and ias servers:x:1000553:
domain controllers:x:1000516:
enterprise admins:x:1000519:
domain computers:x:1000515:
cert publishers:x:1000517:
dnsupdateproxy:x:1001102:
domain admins:x:1000512:
domain guests:x:1000514:
schema admins:x:1000518:
domain users:x:1000513:
datengruppe:x:1001108:
dnsadmins:x:1001101:
```

Abbildung 2: getent group

3 AUFGABEN

3.1 Aufgabe 1

Wir haben nun die AD-Gruppen und AD-User auf `vmLS2` aktiviert. Können wir nun aus dem lokalen User `root` in einen AD-User switchen? Versuchen Sie das mit dem Befehl `su`. Zum Beispiel mit `su - administrator` oder `su - ihrname`. Warum geht das noch nicht ganz sauber? Prüfen sie auch die Linux-ID des AD-Users mit dem Befehl `id`. Was sehen sie?

3.2 Aufgabe 2

Legen Sie mit den RSAT-Tools einen neuen User und eine neue Gruppe an. Wie lauten die uid und die gid unter Linux? Wie lauten die SIDs der beiden Objekte im LDAP? Erklären sie den Zusammenhang dieser IDs am konkreten Beispiel in ihrem Arbeitsjournal.