M159 - Directory Services

Thema 2

Arbeitsblatt 1

1 Lernziele

Im gesamten 2. Teil verfolgen wir folgende Lernziele:

- Verwaltung eines integrierten ADDS mit Samba
- Praktisches Fallbeispiel ist die Basis für eine realitätsnahe Konfiguration
- Verständnis für LDAP als Teil eines Active Directory Service
- Kenntnis wie Windows und Linux Rechner in einer Domain eingebunden werden
- Berechtigungen definieren und in der Domain umsetzen unter Berücksichtigung der Windows/Linux - Integrationsproblematik

2 Arbeitsumgebung

Wir betrachten hier die Implementierung eines Directory Services mit dem OpenSource-Produkt:

Samba in der Version ab 4.x kann als Implementierung des Microsoft ADDS unter Linux/Unix verstanden werden und ist daher eine echte Alternative zum kommerziellen Produkt von Microsoft. Sehr oft wird Samba auch in kommerziellen Network Attached Storages - NAS verwendet.
Es gibt zwei Arten, wie ein Samba Rechner implementiert werden kann:

Samba als Domain Controller:

- Ab Version 4 kann Samba als Active Directory (AD) domain controller (DC) eingesetzt werden
- LDAP als AD backend ist integriert
- Heimdahl Kerberos wird vom KDC für die Authentisierung verwendet.

Samba als Domain Member:

- bezeichnet einen Linux Rechner, welcher Teil einer Domain ist.
- stellt File- und Printservices zur Verfügung
- Domain Users werden gegenüber dem DC beim Login authentifiziert.

2.1 Laborumgebung mit smartlearn.ssd

Die aufzubauende Laborumgebung besteht aus der Realm

SAM159.IET-GIBB.CH

Folgende Rechner werden dafür verwendet:

- vmLS1 als Domain Controller / KDC, DNS Server und LDAP-Server
- vmLS2 als Domain Member Server
- vmLP1 als Domain Member Client

3 Vorbereitung des Domain Controllers / KDC

3.1 Samba Domain Controller vmLS1 installieren

Führen Sie folgende Schritte durch

1. Netzwerk konfigurieren

   (a) passen sie das `*.yaml`-File in `/etc/netplan/` an. Die IP-Adresse lautet: `192.168.220.10/24`. Die DNS Domain setzen wir bereits auf `sam159.iet-gibb.ch`. Die Aktivierung der Settings erfolgt mit `netplan apply`.

```
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      dhcp4: no
      addresses: [ 192.168.220.10/24 ]
      gateway4: 192.168.220.1
      nameservers:
        search: [sam159.iet-gibb.ch]
        addresses: [192.168.220.10,192.168.220.1, 8.8.8.8]
```

Listing 1: `/etc/netplan/00-eth0.yaml` von vmLS1

   (b) Anpassen von `/etc/hosts`

```
127.0.0.1 localhost
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.220.10  vmls1.sam159.iet-gibb.ch
```

Listing 2: `/etc/hosts` von vmLS1

   (c) Anpassen von `/etc/hostname`

```
vmls1.sam159.iet-gibb.ch
```

Listing 3: `/etc/hostname` von vmLS1

2. Rechner updaten mit `sudo apt update && sudo apt upgrade`
3. Samba und diverse Packages installieren

(a) `apt install samba smbclient heimdal-clients`
Bei der Installation wird der Kerberos- und der Administrative-Server abgefragt. Geben Sie dort jeweils `vmls1.sam159.iet-gibb.ch` ein. Installieren Sie ebenfalls:

```
apt install acl attr build-essential libacl1-dev libattr1-dev
apt install libblkid-dev libgnutls28-dev libreadline-dev python-dev
apt install python-dnspython gdb pkg-config libpopt-dev libldap2-dev
apt install libbsd-dev attr krb5-user docbook-xsl libcups2-dev acl ntp ntpdate
apt install net-tools git winbind libpam0g-dev dnsutils lsof
```

(b) Sichern sie das originale Samba-conf-File: `mv /etc/samba/smb.conf /etc/samba/smb.conf.orig`

(c) Jetzt erfolgt das Setup von Samba als KDC für den Realm `SAM159.IET-GIBB.CH` und die Domain `SAM159` mit folgender Anweisung:
`samba-tool domain provision`
Übernehmen Sie jeweils die Default-Werte, ausser bei der Auswahl des DNS Backends – geben Sie dort SAMBA_INTERNAL ein. Als `DNS forwarder IP address`: `8.8.8.8`. Setzen Sie als `Administrator`-Passwort: `SmL12345**`. Das Passwort muss hier der eingestellten Passwortkomplexität genügen. Am Ende sollten Sie folgenden Output erhalten:

```
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/
    samba/private/krb5.conf
Once the above files are installed, your Samba AD server will be ready to use
Server Role:           active directory domain controller
Hostname:              vmls1
NetBIOS Domain:        SAM159
DNS Domain:            sam159.iet-gibb.ch
DOMAIN SID:            S-1-5-21-4113420325-2841194728-3666662892
```

Listing 4: Output von `samba-tool domain provision`

(d) Da jetzt der DNS-Dienst von Samba zur Verfügung gestellt wird, müssen wir den DNS-Resolver deaktivieren mit

```
sudo systemctl disable systemd-resolved
sudo systemctl stop systemd-resolved
```

Listing 5: Resolver deaktivieren

(e) Inhalt von `/etc/samba/smb.conf` kontrollieren:

```
# Global parameters
[global]
  dns forwarder = 8.8.8.8
  netbios name = VMLS1
  realm = SAM159.IET-GIBB.CH
  server role = active directory domain controller
  workgroup = SAM159

[netlogon]
  path = /var/lib/samba/sysvol/sam159.iet-gibb.ch/scripts
  read only = No

[sysvol]
  path = /var/lib/samba/sysvol
  read only = No
```

Listing 6: /etc/samba/smb.conf

(f) Samba automatisch starten bei Systemboot. Aktivieren mit:

```
systemctl unmask samba-ad-dc
systemctl enable samba-ad-dc
systemctl start samba-ad-dc
reboot
systemctl status samba-ad-dc
```

```
```

Listing 7: Samba automatisch starten bei boot

(g) Jetzt konfigurieren wir Samba für die Verwendung des Kerberos-Authentifizierungsdiensts

```
mv /etc/krb5.conf /etc/krb5.conf.orig
ln -sf /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Listing 8: Softlink des `krb5.conf` nach `/etc`

(h) Ergänzen Sie die Datei `/etc/krb5.conf` mit den folgenden Angaben:

```
[libdefaults]
  default_realm = SAM159.IET-GIBB.CH
  dns_lookup_realm = false
  dns_lookup_kdc = true

[realms]
  SAM159.IET-GIBB.CH = {
    kdc = vmls1.sam159.iet-gibb.ch
    default_domain = sam159.iet-gibb.ch
  }
```

Listing 9: Inhalt von `/etc/krb5.conf`

4. Netzwerk testen

(a) Ports sind listening? `netstat -tlpn`. Das Resultat sollte aussehen wie in der Abbildung.

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
    PID/Program name
tcp        0      0 0.0.0.0:49152           0.0.0.0:*               LISTEN
    513/samba
tcp        0      0 0.0.0.0:49153           0.0.0.0:*               LISTEN
    513/samba
tcp        0      0 0.0.0.0:49154           0.0.0.0:*               LISTEN
    513/samba
tcp        0      0 0.0.0.0:3268            0.0.0.0:*               LISTEN
    517/samba
tcp        0      0 0.0.0.0:3269            0.0.0.0:*               LISTEN
    517/samba
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN
    517/samba
tcp        0      0 0.0.0.0:135             0.0.0.0:*               LISTEN
    513/samba
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
    519/smbd
tcp        0      0 0.0.0.0:464             0.0.0.0:*               LISTEN
    521/samba
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN
    532/samba
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
    494/sshd
tcp        0      0 0.0.0.0:88              0.0.0.0:*               LISTEN
    521/samba
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN
    517/samba
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
    519/smbd
```

Listing 10: Output von `netstat -tlpn`

(b) Den internen DNS-Service aktualisieren mit `samba_dnsupdate --verbose`. Es dürfen keine Fehler angezeigt werden.

(c) DNS testen auf folgende wichtige Einträge:
`host -t SRV _kerberos._tcp.sam159.iet-gibb.ch`

```
_kerberos._tcp.sam159.iet-gibb.ch has SRV record 0 100 88 vmls1.sam159.iet-gibb.
    ch.
```

Listing 11: Output:Kerberos Eintrag im DNS

```
host -t SRV _gc._tcp.sam159.iet-gibb.ch
```

```
_gc._tcp.sam159.iet-gibb.ch has SRV record 0 100 3268 vmls1.sam159.iet-gibb.ch.
```

Listing 12: Output: Global Catalog

```
host -t SRV _ldap._tcp.sam159.iet-gibb.ch
```

```
_ldap._tcp.sam159.iet-gibb.ch has SRV record 0 100 389 vmls1.sam159.iet-gibb.ch.
```

Listing 13: Output: LDAP

```
host -t A vmls1.sam159.iet-gibb.ch
```

```
vmls1.sam159.iet-gibb.ch has address 192.168.220.10
```

Listing 14: Output: `vmls1` wird aufgelöst

5. Reverse-Lookup-Zone einrichten

   (a) Die Verwaltung von DNS wird mit dem Befehl `samba-tool` gemacht. Die Reverse-Lookup-Zone richten sie wie folgt ein:
   `samba-tool dns zonecreate vmls1 220.168.192.in-addr.arpa -Uadministrator`
   Danach müssen Sie das Passwort eingeben: `SmL12345**`

   (b) Reverse-Zone für `vmLS1` eintragen: (alles auf eine Zeile!)
   `samba-tool dns add 192.168.220.10 220.168.192.in-addr.arpa 10 PTR vmls1.sam159.iet-gibb.ch -Uadministrator`

6. A-Records eintragen

   (a) A-Record für `vmls2` eintragen:
   `samba-tool dns add 192.168.220.10 sam159.iet-gibb.ch vmls2 A 192.168.220.11 -Uadministrator`

7. Testen der Verbindung

   (a) Der Test des Verbindungsaufbaus wird mit dem Befehl `smbclient` gemacht:

```
smbclient -L localhost -Uadministrator
Enter SAM159\administrator's password: SmL12345**

  Sharename       Type      Comment
  ---------       ----      -------
  netlogon        Disk
  sysvol          Disk
  IPC$            IPC       IPC Service (Samba 4.7.6-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

  Server               Comment
  ---------            -------

  Workgroup            Master
  ---------            -------
  WORKGROUP            VMLS1
```

Listing 15: Test des Verbindungsaufbaus

Im Listing sehen sie, dass bereits zwei Freigaben auf dem Domaincontroller bereitgestellt werden: `sysvol` und `netlogon`. Diese beiden Shares werden auf einem Domaincontroller immer benötigt und somit bei der Erstkonfiguration auch immer angelegt.

Auf einem Domaincontroller sollten keine weiteren Freigaben eingerichtet werden. Alle Daten sollten auf einem Fileserver gespeichert werden. Der Grund dafür ist das unterschiedliche ID-Mapping der UIDs und GIDs der Linux-Benutzer.

4 Aufgaben

4.1 Lösen Sie ein Ticket für den User `administrator`

4.2 Verbindung testen mit `smbclient -L vmls1 -k`

Was bewirkt der Parameter `-k`?

4.3 Wie sieht der Credential Cache aus?

4.4 Warum funktioniert der Verbindungsaufbau mit `localhost` nicht?

Versuchen Sie es mit: `smbclient -L localhost -k`
`localhost` entspricht doch `vmls1`?
warum hat es mit `localhost` bei 7(a)-Testen der Verbindung geklappt bzw. warum klappt es hier nicht mit `-k`?

4.5 Passwort-Komplexität deaktivieren mit `samba-tool`

Studieren Sie den Befehl `samba-tool` und deaktivieren sie die Passwort-Komplexität auf Ebene Domain. Für Hilfe verwenden sie `samba-tool`. Setzen sie folgende Einstellungen:

1. Password complexity = deactivated
2. Password history length = 0
3. Minimum password age = 0
4. Maximum password age = 0
5. Expiration Time für den User administrator ausschalten

4.6 Anlegen eines DNS A Records mit samba-tool

Legen sie vmls2 und vmls3 als A-Record im DNS an. Verwenden Sie dazu den Befehl samba-tool. Für Hilfe verwenden sie samba-tool -h oder finden sie Beispiele im Internet.

4.7 Anlegen der PTR Records für vmls2 und vmls3

Legen Sie für beide Rechner die PTR Record an mit dem Befehl samba-tool.

4.8 Was zeigt `samba-tool fsmo show` ?

Erklären Sie die Bedeutung von jedem Eintrag und notieren Sie das im Arbeitsjournal.