

LDAP + FreeRADIUS + LAM-Testumgebung

1. Aufbau der Testumgebung

Komponente	Funktion	IP-Adresse
VM1	DHCP, Router, FreeRADIUS	192.168.100.1
VM2	OpenLDAP + LAM	192.168.100.10

2. Grundinstallation der Server

Voraussetzungen

- Debian 12 (Bookworm) Minimalinstallation pro VM
- Netzwerkverbindung zur Kommunikation zwischen den VMs

Softwarequellen aktualisieren

```
bash
```

```
sudo apt update && sudo apt upgrade -y
```

Netplan installieren (falls nicht vorhanden)

```
bash
```

```
sudo apt install netplan.io
```

Netzwerkadapter anpassen und umbenennen

- Debian verwendet standardmäßig „Predictable Network Interface Names“. Um die Netzwerkkarten sinnvoll umzubenennen:
- Datei `/etc/systemd/network/99-custom-names.link` erstellen:

```
bash
```

```
sudo nano /etc/systemd/network/99-custom-names.link
```

- Beispielinhalt:

```
/etc/systemd/network/99-custom-names.link
```

```
[Match]  
MACAddress=AA:BB:CC:DD:EE:01
```

```
[Link]
```

```
Name=wan0
```

```
[Match]
```

```
MACAddress=AA:BB:CC:DD:EE:02
```

```
[Link]
```

```
Name=lan0
```

- (MAC-Adressen der jeweiligen Netzwerkkarten anpassen!)
- Danach: `bashbash> sudo update-initramfs -u sudo reboot</code>`

Netplan-Konfiguration (für 2 Netzwerkkarten auf VM1)

- Datei anlegen/bearbeiten:

```
bash
```

```
sudo nano /etc/netplan/01-netcfg.yaml
```

- Beispiel für VM1 (Router):

```
/etc/netplan/01-netcfg.yaml
```

```
network:
  version: 2
  renderer: networkd
  ethernets:
    wan0:
      dhcp4: true
    lan0:
      addresses:
        - 192.168.100.1/24
```

- Anwenden:

```
bash
```

```
sudo netplan apply
```

3. Installierte Software

VM1 (RADIUS + NAT + DHCP)

```
bash
```

```
sudo apt install isc-dhcp-server iptables-persistent freeradius freeradius-ldap net-tools netplan.io curl sudo less vim
```

- NAT mit iptables (MASQUERADE)
- Freeradius + LDAP-Modul
- DHCP für das Subnetz 192.168.100.0/24
- Zusätzliche Tools: net-tools, vim, less, sudo, curl
- Beispiel DHCP-Konfiguration (/etc/dhcp/dhcpd.conf):

```
/etc/dhcp/dhcpd.conf
```

```
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.100.0 netmask 255.255.255.0 {
  range 192.168.100.100 192.168.100.200;
  option routers 192.168.100.1;
  option domain-name-servers 192.168.100.10;
}
```

- DHCP-Interface definieren in /etc/default/isc-dhcp-server:

```
/etc/default/isc-dhcp-server
```

```
INTERFACESv4="lan0"
```

VM2 (LDAP-Server + Webverwaltung)

```
bash
```

```
sudo apt install slapd ldap-utils ldap-account-manager net-tools netplan.io
curl sudo less vim
```

- Während der slapd-Installation:
 - Domäne: zkm.local
 - Admin-Passwort setzen (z. B. zkmadminpass)
 - Standardmäßig wird nur ldap:// aktiviert (kein TLS)
- Zusätzliche Pakete wie curl, vim, less und sudo empfohlen zur Systempflege.

4. OpenLDAP - Basisstruktur

```
basisstruktur.ldif
```

```
dn: dc=zkm,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: ZKM
dc: zkm

dn: cn=admin,dc=zkm,dc=local
objectClass: organizationalRole
cn: admin
```

```
dn: ou=people,dc=zkm,dc=local
objectClass: organizationalUnit
ou: people
```

```
dn: ou=groups,dc=zkm,dc=local
objectClass: organizationalUnit
ou: groups
```

- Import per:

bash

```
sudo ldapadd -x -D "cn=admin,dc=zkm,dc=local" -W -f basisstruktur.ldif
```

5. Beispielbenutzer

- Beispielbenutzer anlegen mit Passwort-Hash: dn: uid=demo,ou=people,dc=zkm,dc=local objectClass: inetOrgPerson objectClass: posixAccount objectClass: shadowAccount cn: Demo Benutzer sn: Benutzer uid: demo uidNumber: 10001 gidNumber: 10001 homeDirectory: /home/demo loginShell: /bin/bash userPassword: {SSHA}<gehashtesPasswort> • *Passwort generieren mit: slappasswd 6. FreeRADIUS + LDAP-Anbindung • Freeradius LDAP-Modul aktivieren: sudo ln -s /etc/freeradius/3.0/mods-available/ldap /etc/freeradius/3.0/mods-enabled/ • Konfiguration anpassen: server = '192.168.100.10' identity = 'cn=radius,dc=zkm,dc=local' password = 'radiuspass' basedn = 'dc=zkm,dc=local' user { basedn = „\${..basedn}“ filter = „(uid=%{%{Stripped-User-Name}:-%{User-Name}})“ scope = 'sub' } update { control:Password-With-Header += 'userPassword' } • Zusätzlich in /etc/freeradius/3.0/sites-enabled/default: if ((ok || updated) && User-Password && !control:Auth-Type) { update { control:Auth-Type := ldap } } • Freeradius Debugmodus zum Testen: sudo freeradius -X 7. NAT und Routing (VM1) • NAT aktivieren: sudo iptables -t nat -A POSTROUTING -o wan0 -j MASQUERADE sudo iptables -P FORWARD ACCEPT • IP-Forwarding aktivieren: echo „net.ipv4.ipforward=1“ | sudo tee -a /etc/sysctl.conf sudo sysctl -p • iptables-Regeln dauerhaft speichern: sudo netfilter-persistent save 8. LDAP Account Manager (LAM) • LAM installieren: sudo apt install ldap-account-manager • Zugriff via Browser: <http://192.168.100.10/lam> • Login-Einstellungen: • Login-Methode: Direkter DN • Benutzername: cn=admin,dc=zkm,dc=local • Aktivierte Module: • inetOrgPerson • posixAccount • shadowAccount • posixGroup • Standard-Base-DNs: • Benutzer: ou=people,dc=zkm,dc=local • Gruppen: ou=groups,dc=zkm,dc=local 9. Fallstricke & Fehlerbehebung Fehler Ursache Lösung Benutzer nicht gefunden falscher Login-Filter Login-Methode auf „Direkter DN“ ändern Kein Internet auf VM2 NAT nicht aktiv iptables + IP-Forwarding überprüfen RADIUS kein Passwort Attribut nicht lesbar userPassword lesbar machen, Hash prüfen slapd lauscht nur lokal SLAPDSERVICES falsch in /etc/default/slapd prüfen LAM findet DN nicht falscher Filter oder OU fehlt Basisstruktur kontrollieren 10. Best Practices • Immer sichere {SSHA} Passwörter verwenden • UID/GID sorgfältig verwalten und dokumentieren • Strukturierte OUs anlegen (people, groups) • Freeradius im Debugmodus testen (freeradius -X) • Keine Klartext-Passwörter verwenden 11. Status • Authentifizierung von LDAP-Usern über FreeRADIUS NAT und Routing aktiv auf VM1 Benutzerverwaltung über LAM funktionsfähig__ • (Stand: April 2025)*

From:

<http://wiki.nctl.de/dokuwiki/> - `Veni. Vidi. sudo rm -rf / vici.`

Permanent link:

http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:projekt:dokumentation:ldap_freeradius_lam-testumgebung&rev=1746115401

Last update: **01.05.2025 18:03**

