LDAP/NAC-Dokumentation (Testumgebung ZKM)

Übersicht

Diese Dokumentation beschreibt die Einrichtung eines zentralen Authentifizierungs- und Netzwerkzugangskontrollsystems (NAC) mit folgenden Komponenten:

- **OpenLDAP** (Verzeichnisdienst)
- **FreeRADIUS** (Authentifizierungsserver)
- **LDAP Account Manager (LAM)** (Webinterface zur LDAP-Verwaltung)
- **Dynamische VLAN-Zuweisung** basierend auf MAC-Adressen
- **Testumgebung mit zwei VMs**

Netzwerkstruktur (Testsetup)

- **VM1** - `192.168.100.1`
  - DHCP
  - FreeRADIUS
  - NAT-Routing (Gateway)
- **VM2** - `192.168.100.10`
  - OpenLDAP-Server
  - LAM Webinterface

OpenLDAP Einrichtung

1. Installation

snippet.bash

```bash
apt install slapd ldap-utils
```

2. Schema-Import (freeradius.schema)

Konvertierung

snippet.bash

```
mkdir /etc/ldap/schema-converted
mkdir /tmp/ldap
cp /etc/freeradius/3.0/mods-config/ldap/schema/freeradius.schema
/tmp/ldap
cd /tmp/ldap
sudo mkdir -p /etc/ldap/schema/freeradius
sudo slaptest -f slapd.conf -F /etc/ldap/schema/freeradius
```

Hinweis: `slapd.conf` enthält:

snippet.conf

```
include /etc/ldap/schema/core.schema
include /tmp/ldap/freeradius.schema
```

Import in LDAP

snippet.bash

```
ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/ldap/schema/freeradius/cn\=config/cn\=schema/cn\=\{0\}freeradius.l
dif
```

Wichtig: Bei mehrfacen Versuchen kann es zu OID-Dubletten kommen. Lösung: Slapd komplett zurücksetzen (siehe unten).

--

OpenLDAP zurücksetzen (Neuaufbau)

snippet.bash

```
systemctl stop slapd
rm -rf /etc/ldap/slapd.d/*
rm -f /var/lib/ldap/*
dpkg-reconfigure slapd
```

Danach Schema erneut konvertieren und importieren.

LDAP Account Manager (LAM)

Installation

snippet.bash

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

Zugriff

- Webinterface: `https://<server-ip>/lam` - Standard-Login: Konfigurierbar Ã¼ber `/etc/ldap-account-manager/config.cfg`

Benutzerdefinierte Felder

- MAC-Adressen via `radiusCallingStationId` - VLANs via `radiusTunnelPrivateGroupId`, `radiusTunnelType`, `radiusTunnelMediumType`

FreeRADIUS Anbindung an LDAP

Installation

snippet.bash

```
apt install freeradius freeradius-ldap
```

LDAP-Modul konfigurieren

Pfad: `/etc/freeradius/3.0/mods-available/ldap`

snippet.text

```
server = '192.168.100.10'
identity = 'cn=admin,dc=zkm,dc=intern'
password = 'geheim'
```

```
base_dn = 'ou=macs,dc=zkm,dc=intern'
```

Symlink aktivieren:

snippet.bash

```
ln -s /etc/freeradius/3.0/mods-available/ldap /etc/freeradius/3.0/mods-enabled/
```

Benutzerabfrage testen

snippet.bash

```
freeradius -X
```

MAC-basierte VLAN-Zuweisung

Beispielobjekt in LDAP (LDIF)

snippet.ldif

```
dn: cn=AA:BB:CC:DD:EE:FF,ou=macs,dc=zkm,dc=intern
objectClass: radiusProfile
cn: AA:BB:CC:DD:EE:FF
radiusCallingStationId: AA:BB:CC:DD:EE:FF
radiusTunnelType: VLAN
radiusTunnelMediumType: IEEE-802
radiusTunnelPrivateGroupId: 30
```

Beschreibung der Attribute

- `radiusCallingStationId` = MAC-Adresse
- `radiusTunnelPrivateGroupId` = VLAN-ID
- `radiusTunnelType` = VLAN
- `radiusTunnelMediumType` = IEEE-802

WeiterfÃ¼hrende Planung

- Automatisierter Import aus CSV/SQL in LDAP
- NAC mit 802.1X-Authentifizierung (zunÃ¤chst MAC-Bypass)
- Integration von Extreme Networks-Switches mit RADIUS-basiertem Port-Auth
- Skripte zur Switch-MAC-Erfassung und Zuordnung

Troubleshooting

- **OID-Konflikte beim Schemaimport:** Slapd komplett neu aufsetzen
- **LAM zeigt Felder nicht an:** Felder manuell in der Konfiguration aktivieren
- **RADIUS antwortet nicht:** Auth-Log und `freeradius -X` prüfen

-

ToDo

- [ ] Dynamische Gruppen in LAM aktivieren
- [ ] CSV-Import vorbereiten
- [ ] Radius-Live-Tests mit Switches durchführen
- [ ] VLAN-Tagging validieren

Stand: Mai 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_nac&rev=1746257019

Last update: **03.05.2025 09:23**