UCS LDAP

Dank an Moritz Bunkus für seinen klärenden Beitrag, dem diese Informationen entstammen.

Auf einem Univention-System mit Samba4 laufen gleich zwei LDAP-Server: OpenLDAP und das Samba4-LDAP. Zwischen beiden werden Einträge synchronisiert, sodass Benutzer in beiden existieren. Allerdings verwenden beide eine leicht unterschiedliche DNs für die Benutzer:

Server	DN	auslesen
Samba	CN=[username],CN=Users,DC=[domain],DC=[tld]	`univention-s4search cn=mosu dn`
Openldap	uid=[username],cn=users,dc=[domain],dc=[tld]	`univention-ldapsearch uid=mosu dn`

Beides ist derselbe User-Eintrag. Man muss daher wissen, an welchem LDAP man sich anmeldet, um den richtigen Anmeldenamen nutzen zu können.

Folgende Ports werden verwendet:

Server	Port (START-TLS)	SSL
Samba	389	636
OpenLdap	7389	7636

Weiterhin muss man bei Verschlüsselung auf die üblichen zwei Dinge achten:

1. Der verbindende Client muss der CA vertrauen, die das Zertifikat ausgestellt hat. Daher ist es oft nötig, die UCS-CA in der Client-Anwendung oder dem Client-Betriebssystem zu importieren. Die CA liegt auf dem DC Master in /etc/univention/ssl/ucsCA/CAcert.pem.
2. Der Hostname, den der Client zum Verbinden nutzt, muss im Zertifikat als subjectAlternativeName mit angegeben sein. Andernfalls wird die Verbindung als unsicher abgelehnt. Man kann also nicht einfach die IP-Adresse oder den kurzen Hostnamen nehmen, man muss den FQDN des LDAP-Servers nutzen.

Das Samba4-LDAP akzeptiert drei Varianten für die Angabe des Loginnamens:

- Den vollständige DN des Users
- Die Variante user@domain.dld
- Die Variante NetBIOSDomain\user

OpenLDAP akzeptiert ausschließlich die DN-Syntax. Siehe oben, Tabelle: Server/DN

Große Unterschiede zwischen beiden LDAP-Varianten sind:

- Samba4 speichert Gruppenmitgliedschaften im Userobjekt direkt mittels des Attributs memberOf.
- OpenLDAP speichert die Mitgliedschaft hingegen im Gruppenobjekt mittels des Attributs uniqueMember.

Wenn man in seiner Anwendung nur einen LDAP-Filter angeben kann, so ist daher die Samba4-Variante einfacher. Achtung: man kann das in OpenLDAP mit Hilfe des »memberOf-Overlays« nachrüsten. Das wird ab UCS 4.3 übrigens standardmäßig aktiv sein. (Siehe unten.)

Diverse für Unix/Linux relevante Attribute wie z.B. das Home-Verzeichnis oder die Login-Shell stehen ausschließlich im OpenLDAP zur Verfügung. Die von Univention bereitgestellten, beliebig zu vergebenden Free Attributes stehen ebenfalls nur im OpenLDAP zur Verfügung.

memberOf

Seit dem UCS 4.3 gibt es ein sog. Overlay, welches „memberOf“ für den OpenLDAP aktivert. Dazu muss das Paket installiert sein und die Funktion aktiviert werden, denn per Default ist sie deaktiviert:

```
apt install univention-ldap-overlay-memberof
ucr set ldap/overlay/memberof=true
```

Quelle

Jetzt muss man noch wissen, dass der Filter erst bei neuen Gruppen funktioniert. Um „memberOf“ für bestehende Gruppen zu aktivieren müssen die Benutzer aus der Gruppe entfernt, die Gruppe gespeichert und dann die Benutzer der Gruppe wieder hinzugefügt werden.

TLS bei samba4 ausschalten

Laut dieser Quelle ist bei samba4 zwingend eine TLS-Verschlüsselung notwendig

```
ucr set samba/ldap/server/require/strong/auth=no
service samba restart
```

Quellen:

- https://help.univention.com/t/ldap-auth-fur-externe-systeme/7991/2

From:
https://wiki.da-checka.de/ - **PSwiki**

Permanent link:
https://wiki.da-checka.de/doku.php/wiki/basteleien/active_directory/ldap

Last update: **2019/01/13 22:36**