Netzwerke und Kommunikation
B-LS-MI 004
Basisdienste
LDAP/ActiveDirectory Verzeichnisdienst

rolf.schmutz@fhnw.ch

FHNW

27. Oktober 2020

n|w

Ziele

- Sie kennen die Aufgaben von LDAP
- Sie können gezielt LDAP-Server abfragen

LDAP: DNS für Personen und Inventar

LDAP steht für "Lightweight Directory Access Protocol" [1]

LDAP ist ein flexibler Verzeichnisdienst und z.B. verwendet für

- Personenverzeichnis innerhalb einer Organisation ("Telefonbuch")
- Computer-Inventar

LDAP bietet im Gegensatz zu DNS auch eine Authentisierung[2] und wird für Autorisierung[3] verwendet

[1] wie immer bei IETF wenn etwas "simple" oder "lightweight" heisst, ist es das nicht...

[2] gesicherte Identifizierung

[3] Berechtigungen

LDAP: Factlets

- LDAP basiert auf dem ISO/OSI X.500 Standard
- LDAP wird meistens über TCP[4] implementiert
- LDAP bietet ein Objektmodell wobei jeder Eintrag von mehreren Klassen "erben" kann – damit werden die vorhandenen Felder[5] bestimmt
- anders als DNS wird LDAP nicht global/verteilt betrieben[6], d.h. die einzelnen Verzeichnisdienste müssen dem Anfrager bekannt sein
- es sind "Federations" möglich – eine Verlinkung auf andere Verzeichnisse (z.B. FHNW und Switch/AAI)
- die Einträge sind hierarchisch[7] geordnet, meistens nach Unternehmensstruktur
- es sind Beziehungen zwischen Objekten möglich, das wird vorallem für Gruppenzugehörigkeit[8] benutzt

[4] Port 389

[5] z.B. objectClass=person → sn=Familienname, givenName=Vorname, mail, ...

[6] obschon das in X.500 so vorgesehen war

[7] über Attribute `dc` (domain-component), `ou` (organisational-unit), `l` (location), etc

[8] memberOf

Implementierungen

LDAP ist wie DNS auch ein eher "verborgener" Dienst, der von Endbenutzer nicht direkt verwendet wird.

Serverseitig gibt es zwei wesentliche Implementierungen

- **openLDAP**
- **AD**/ActiveDirectory von Microsoft

Clientseitig wird meistens durch eine Benutzeranwendung[9] (Mail, Anmeldung, etc) und/oder spezielle Bibliotheken kommuiziert. Einige

spezielle LDAP-Clients (GUI, command-line) sind ebenfalls vorhanden, wir benutzen die ldap-utils von OpenLDAP

[9] d.h. ähnlich wie eine URL/Hostnamen im Browser über DNS aufgelöst wird

Recordformat (1/2)

Das verwendete (externe) Datenformat ist LDIF

- einzelne "Records"[10] werden durch Leerzeile oder "–" getrennt
- einzelne Attribute werden mit: `Attribut-Typ: Wert` aufgeführt
- ein Wert kann über mehrere Zeilen gehen, die Folgezeilen müssen dann eingerückt werden
- Werte können base64 codiert sein: `sn:: S8O8dHRuZXI=`[11] ("Küttner")
- mindestens werden die Attribute `objectClass`[12], `dn` "distingushed name"/Pfad und `cn` "common name"/Name erwartet

[10] anders als bei DNS sind das komplette Einträge/Nodes mit mehreren Attributen – die im DNS den Resource-Records/RR entsprechen

[11] wird mit "::" anstatt ":" als Attribut-Trenner signalisiert, vorallem für "lange" Werte wie Benutzerbild, Zertifikate, Namen mit Umlauten, etc

[12] kann mehrfach vorkommen

Recordformat (2/2)

```
dn: cn=1000002, ou=Payroll, dc=willeke, dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: 1000002
cn: KayC
sn: Kay
description: This is Chicky Kay's description
l: Alameda
ou: Payroll
postalAddress: Payroll$Alameda
telephoneNumber: +1 213 993-9665
title: Elite Payroll Assistant
uid: KayC
givenName: Chicky
mail: KayC@ns-mail4.com
departmentNumber: 8982
employeeType: Contract
roomNumber: 9562
secretary: cn=100135, ou=Human Resources, dc=willeke, dc=com
manager: cn=100474, ou=Administrative, dc=willeke, dc=com
```

Abfragen

LDAP bietet eine flexible textbasierte Abfragesprache nach einem funktionalen Ansatz:

- Suche nach einem Namen: `(givenName=Fritz)`
- Suchen können mit "&" (and), "|" (or) und "!" (not) verknüpft werden[13] – mit zwei oder mehr Argumenten
- Suche nach mehreren Argumenten:
  konjunktiv: `(& (givenName=Fritz) (sn=Knob) )`
  disjunktiv: `(| (objectClass=person) (objectClass=top) )`
- Suche mit Platzhalter: `(sn=K*)`
- "unscharfe"[14] (approximate) Suche: `(givenName~=Franz)`
- . . . und alles kann noch "verschachtelt" werden :)

[13] dabei wird eine super-coole (LISP-like) Präfixnotation verwendet: `(& (a) (b) (c))`

[14] wird nicht von allen Server unterstützt

Exercises

- Verwenden sie die Shell/Terminal auf https://fhnw.netlabs.ch/
- benutzen sie einen der Public LDAP Server[15]
- Beispiel: `ldapsearch -x -H ldap://x500.bund.de '(sn=K*)'`
- mit `ldapsearch -LLL -x...` wird die Ausgabe ein wenig besser lesbar

Suchen Sie:

- alle Einträge mit Vorname "Fritz" (`x500.bund.de`)
- Eintrge mit einem Nachname beginnend mit "K" und Vorname beginnend mit "M" (`x.500.bund.de`)
- Einträge mit einem `userCertificate` Attribut (`x500.bund.de`)
- Einträge mit einem `collectiveOrganizationalUnitName` Attribut (`x500.bund.de`)

[15] bitte nicht "bombardieren" sonst werden wir gesperrt