Assignment 3 - LDAP client

Security

Sébastien Vaucher
sebastien.vaucher@unine.ch

25 October 2017

1 Introduction

LDAP stands for Lightweight Directory Access Protocol. As its name suggests, this protocol provides access to directories and is widely used, for example as address book repositories or authentication directories. Each object stored in the directory is created on the basis of a schema, which defines its attributes. The directory is hierarchical, similar to conventional file systems.

2 Assignment instructions

The goal of this assignment is to program a rudimentary LDAP client that can connect to an LDAP server, display the directory contents, and add/remove/modify entries from it.

For the duration of this assignment, an LDAP server will be available in order for you to test your application. Here are all the relevant connection information:

Host	clusterinfo.unineuchatel.ch
Port for LDAP protocol	10389
DN (username)	cn=admin,dc=security,dc=ch
Password	security2017

You also have access to a web interface where you can operate on the LDAP database using a graphical interface. It is available at this address:
`https://clusterinfo.unineuchatel.ch:10400/lam`
The password is also `security2017`

Warning: you are given *admin* rights to the LDAP server. Please do not remove or modify any existing data.

3 The LDAP protocol

Each entity in an LDAP directory is identified by its Distinguished Name (*dn*). It serves as a unique identifier that also identifies where the object belongs in the hierarchy. The *dn* is formed by concatenating the path of the element from leaf to root.

LDAP uses the LDIF format to print objects in plain text. For instance, an entity could be defined as:

```
dn: cn=Sébastien Vaucher,ou=tutor,dc=security,dc=ch
objectclass: person
cn: Sébastien Vaucher
sn: sv
description: Assistant for the Security lecture
```

The root *dn* of our server is:

```
dn: dc=security,dc=ch
```

This means that the *dn* of any object contained within the server always ends with this sequence.

For this assignment, you will be working with the `students` organizational unit (*ou*). It can be located using the following *dn*:

```
dn: ou=students,dc=security,dc=ch
```

Each entity is defined by a particular schema, which references the list of attributes that can be set on a given object. An attribute can be required or optional. In the LDAP vocabulary, a type of object is called an `objectclass`. You can query the server for the list of accepted `objectclass`es, including the list of their required and optional attributes.

4 Hand-in

The time allotted for this assignment is 1 week. The deadline is on 2017-11-01T13:59:59 local time. Late submissions are not accepted.

- To be submitted to Ilias[1]:
  - Source code of **your** assignment
  - Readme file briefly mentioning how to compile and run your program, which dependencies it requires, etc.
  - All the files have to be packed in an archive in a standard format[2], named following this exact pattern (in lowercase letters only):
    `security17-as<assignment number>-<your family name>.<extension>`.
    For example, if your name were to be *Homer J. Simpson*, you would use the following filename for this assignment: `security17-as3-simpson.tar.gz`
  - Please use the "Upload File" button when handing-in your assignment in Ilias. Do **not** use "Upload Multiple Files as Zip-Archive".
- You have to present a demonstration of the program in class (to the TA).
  - It is **mandatory** for each student to demonstrate his or her submission!
  - The sooner you present your assignment, the better (even before the deadline).

Your grade will depend on both the presentation and the code.

5 Notes

You can use your favorite programming language for the assignments of this course, so long as it is a programming language readily available on the GNU/Linux operating system[3]. The suggested language for this assignment is Python using the `ldap3`[4] library.

Should you have additional questions, please direct them to the TA at sebastien.vaucher@unine.ch.

[1] Or sent by e-mail for external students

[2] `.tar`, `.tar.gz`, `.tar.bz2`, `.tar.xz`, `.zip`

[3] You can use any of the languages in the following list. If you want to use another language, please check with the TA first. List in alphabetical order: Bash, C, C++, Go, Java, Kotlin, Perl, PHP, Python, Ruby, Rust, Scala

[4] `https://ldap3.readthedocs.io/`