HW1-3 - LDAP

2026 NAP
ymlai

Objectives

- Build a basic LDAP service
- Understand how to...
  - Configure an LDAP server
  - Manage LDAP data using LDIF
  - Perform authentication and permission control on a Unix client with an LDAP server
  - Customize your own object classes and use OLC (online configuration)

Outline & Grading

- Basic Configuration (0%)
- Organizational Unit Naming (0%)
- PosixGroup (4%)
- People (5%)
- Access control (8%)
- Password policy (7%)
- TOTP (6%)
- Fortune (4%)

Basic Configuration

- DNS Records
  - LDAP server (private zone): `ldap.${STUID}.nasa`
  - workstation1 (DMZ): `workstation1.${STUID}.nasa`
  - workstation2 (DMZ): `workstation2.${STUID}.nasa`
  - The `{STUID}` is same as the ID you use in HW1-1
- Base DN: dc=<STUID>, dc=nasa
- LDAPS and force TLS search
  - Not LDAP over TLS (StartTLS)
  - Generate your key and certificate by yourselves

Organizational Unit Naming

- People
- Group (posixGroup)
- Ppolicy
- SUDOers
- Fortune (HW customize objectClass)

PosixGroup

We need two posix groups in LDAP:

- **`ta`** group (GID=10000)
  - Can login (ssh) into all workstations
  - Can use sudo to execute **all commands**
    - ex. `` `sudo adduser` ``
- **`stu`** group (GID=20000)
  - Can login (ssh) into workstation1 only
  - Only allow sudo to execute `` `ls` `` command
- Please **use LDAP** to implement the requirements above.
  - Including sudo rules and ssh key!

People (1/3)

Add a user with DN “`uid=generalta,ou=People,<Base DN>`”

- This user under **`ta`** group
- Allow this user to connect via SSH with both ssh public key and password
  - uid: generalta
  - uid number: 10000
  - homeDirectory: `/u/ta/generalta`
  - public key: `ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMUa1AsYerXm5/QVrTZ7QxtkcCUfuXopO04xu2hOBxNY 2026 NAP`
  - user password: `<TA_PASSWORD>`
    - user’s password must be hashed
  - mail: `generalta@{STUID}.nasa`

People (2/3)

Add a user with DN “`uid=mailta,ou=People,<Base DN>`”

- This user under **`ta`** group
- Allow this user to connect via SSH with both ssh public key and password
  - uid: mailta
  - uid number: 10001
  - homeDirectory: `/u/ta/mailta`
  - public key: `ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMUa1AsYerXm5/QVrTZ7QxtkcCUfuXopO04xu2hOBxNY 2026 NAP`
  - user password: `<TA_PASSWORD>`
    - user’s password must be hashed
  - mail: `mailta@{STUID}.nasa`

People (3/3)

Add a user with DN “`uid=stu,ou=People,<Base DN>`”

- This user under **`stu`** group
- Allow this user to connect via SSH with both ssh public key and password
  - uid: stu
  - uid number: 20000
  - homeDirectory: `/u/stu/stu`
  - public key: `ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMUa1AsYerXm5/QVrTZ7QxtkcCUfuXopO04xu2hOBxNY 2026 NAP`
  - user password: `<TA_PASSWORD>`
    - user’s password must be hashed
  - mail: `stu@{STUID}.nasa`

Access Control (1/2)

- Allow **`generalta`** and **`mailta`** to manage LDAP users and groups
- Allow all users to modify their own
  - `userPassword`, `loginShell` and `sshPublicKey`
  - Set all other attributes as **read-only**
- Allow users to search all user attributes, except for other users' password
  - i.e., users can only read their own password
  - **`generalta`** can write passwords but must not be allowed to read them!!

Access Control (2/2)

- Mount the home directory on each LDAP clients
  - Path: `/u/ta`, Permission: 755, Owner: `root:root`
  - Path: `/u/ta/{ta_name}`, Permission: 711, Owner: `{ta_name}:ta`
  - Path: `/u/stu`, Permission: 755, Owner: `root:root`
  - Path: `/u/stu/{stu_name}`, Permission: 711, Owner: `{stu_name}:stu`

- Note:
  - Home directory files for both students (`stu`) and teaching assistants (`ta`) must be **consistently synchronized** across all machines

Password policy

- The new password cannot be the same as the previous password
  - You need to implement this in LDAP
- Password requires **at least 8** characters long
- Password must contain **at least 3** different classes of characters:
  - Upper-case characters
  - Lower-case characters
  - Digits
  - Special characters

Time-based one-time passwords (TOTP)

- Apply TOTP feature on **`generalta`** and **`stu`** account
  - TOTP authentication is required **only for** password-based authentication
  - Logins using SSH public key authentication are exempt from TOTP authentication
  - The OJ will test authentication by using the password followed by the TOTP code
    - For example: `secret123456`
- Add the TOTP schema to the LDAP server
  - oathOTPLength: 6
  - oathTOTPTimeStepPeriod: 60
  - oathHMACAlgorithm: SHA-1
  - oathSecret: `<TOTP_secret>`

Fortune (1/2)

Add an ObjectClass fortune with on-line configuration(OLC)

- **schema**
  - ObjectClass's oid should be under the UUID branch
  - Extend from **top**, add **author** field (Directory String), and **id** field (integer)
  - **author's** matching, substring and order should be "**case insensitive**, **space insensitive**"
  - Use existing **description** (RFC 4519) attribute for sentences
- You need to check whether this objectClass is in database (`cn=config`)

Fortune (2/2)

- Import fortunes
  - From given yaml file (link)
  - 3 fields
    - ID
    - Author
    - Description
- Enable features
  - Server side sorting
  - Pagination
  - Hint: slapo-sssvlv

```
-
  ID: 106
  Author: Richard Feynman
  Description: 'I don''t know what''s the matter with people: they don''t learn by understandin
-
```

```
dn: cn=fortune-1,ou=Fortune,dc=254,dc=nasa
objectClass: fortune
objectClass: top
cn: fortune-1
author: Richard Feynman
id: 1
description: The first principle is that
you must not fool yourself -- and you are
the easiest person to fool.
```

LDAP Client

- Configure LDAP Client on `workstation1`, `workstation2`
- Configure LDAP for login (ssh) authentication
  - LDAP users can use password or public key to login
  - The detailed permissions is in PosixGroup page

Note

- You need to generate the **`TA_PASSWORD`** and **`TOTP_secret`** in
  - OJ → Tools → “Generate TA password & TOTP secret”
- OJ will use the **`generalta`** account to test all requirements in hw1-3
  - The **`mailta`** account will be used to test requirements related to LDAP in hw1–2

- **Always backup** your system before submission, as we may perform malicious actions during testing
- Make sure everything works correctly after **reboot**

Good Luck!