Homework 4
LDAP Service and Integration

changhoy, tcyuan

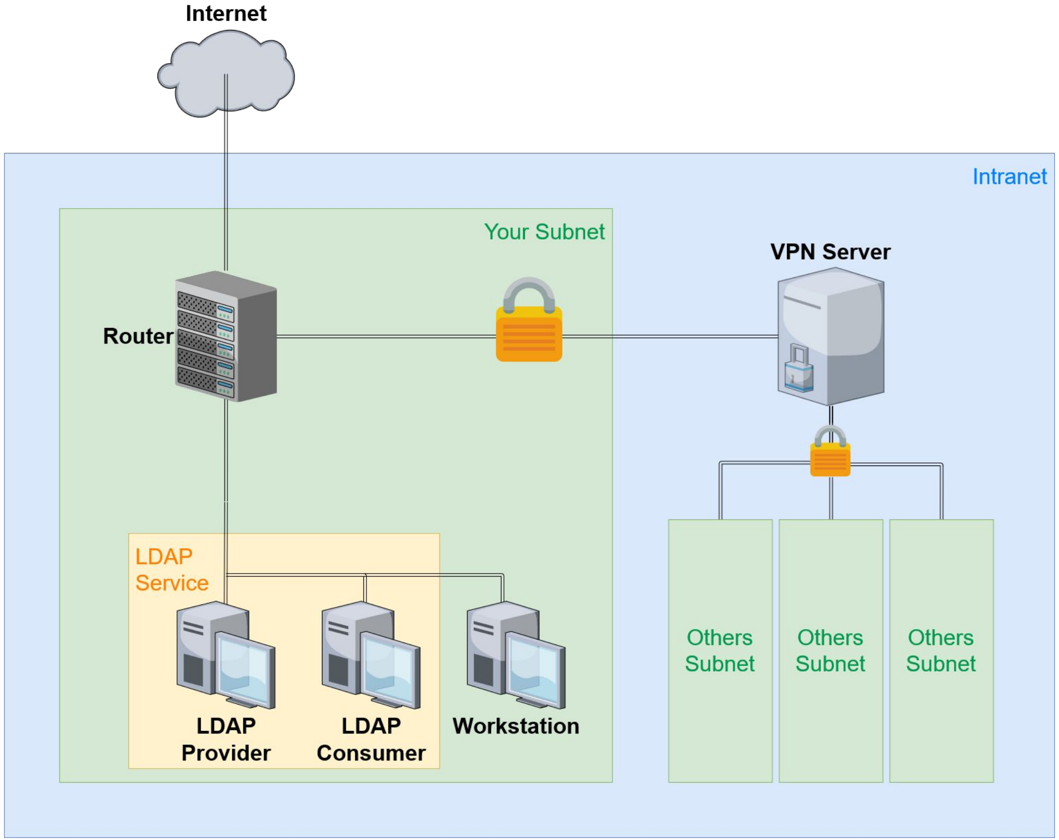
國立陽明交通大學資工系資訊中心

Computer Center of Department of Computer Science, NYCU

Purposes

- Build a basic LDAP service
- Understand how to…
  - configure LDAP provider-consumer replication
  - manage LDAP data using LDIF
  - authenticate an Unix client with LDAP server
  - integrate other service or applications with LDAP

Overview


Internet
Intranet
Your Subnet
VPN Server
Router
LDAP
Service
LDAP
Provider
LDAP
Consumer
Workstation
Others
Subnet
Others
Subnet
Others
Subnet

Overview (cont.)

- A simple LDAP Provider (Master) server
  - Providing LDAP service
  - LDAP client, NFS client
- A simple LDAP Consumer (Slave) server
  - Providing LDAP service
  - Sync LDAP data from LDAP provider
  - LDAP client, NFS client
- One or more Workstations
  - LDAP client, NFS client

Requirements (1/9)

- LDAP Provider
  - IP: 10.113.ID.y/24 with static DHCP, where y is arbitary
  - Hostname: ldapprovider.{ID}.nasa.
  - Base DN: dc=<ID>,dc=nasa
  - LDAP over TLS (StartTLS) and force TLS search
    - Not LDAPS
    - Use self-signed certificate
    - Add your CA certificate to DNS TXT Record
      - cert => `base64 cacert.pem`

Requirements (2/9)

- LDAP Consumer
  - IP: 10.113.ID.y/24 with static DHCP, where y is arbitary
  - Hostname: ldapconsumer.{ID}.nasa.
  - Base DN: dc=<ID>,dc=nasa
  - LDAP over TLS (StartTLS) and force TLS search
    - (Refer to previous page)
  - Sync data from LDAP provider

Requirements (3/9)

- Workstation
  - IP: 10.113.ID.y/24 with static DHCP, where y is arbitary
  - Hostname: workstation.{ID}.nasa.
  - Allow TA login to your machine
    - See next slide for credentials
  - We will judge your work on this machine
    - Allow ssh connections from intranet (10.113.0.0/16) solely on this machine
    - Make sure your work can be examined with this host

Requirements (4/9)

- Add an user with DN “**uid=ta,ou=People,<Base DN>**”
  - Allow this user to connect via SSH with both ssh key and password
    - uid: ta
    - uid number: 3000
    - public key: <ta’s public key>
    - user password: <your WG_PRIVATE_KEY>
  - TA's public key: https://nasa.cs.nctu.edu.tw/na/2021/id_rsa.pub
    - Fingerprint:

```
$ ssh-keygen -l -f id_rsa.pub
3072 SHA256:T0q/ihuk0gSHKXZQDLftzRVMBb9zxq6aNsNQNqHzOms 2021-na-hw4 (RSA)
```

Requirements (5/9)

- Add another user with DN “**uid=stu<ID>,ou=People,<Base DN>**”
  - Allow this user to connect via SSH with both ssh key and password
    - uid: stu<ID>
      - e.g. stu1, stu55
    - uid number: 3000 + <ID>
      - e.g. 3001, 3055
    - user password: <your WG_PRIVATE_KEY>

Requirements (6/9)

- Add a simple authentication user with DN “**cn=syncuser,<Base DN>**”
    - LDAP consumer will bind as this entry using simple authentication
    - **cn=syncuser** should exist only on LDAP provider
        - i.e., this entry would not be syncronized from provider to consumer

Requirements (7/9)

- Set proper LDAP Access Control
  - Provider
    - Allow users to modify their own user data
    - Allow users to search all user data except other users’ password
      - i.e., users can only search their own password
  - Consumer
    - Allow users to modify their own user data except password
    - Allow users to search all user data except password
      - i.e., users cannot search anyone’s password, even their own password

Requirements (8/9)

- Configure LDAP Client on every machine
  - Configure LDAP for login authentication
  - Query to LDAP consumer first. If failed, then query provider
- Configure NFS Client on every machine
  - Configure LDAP and Autofs for home directory mapping
    - Mount users' home directories on 10.113.0.254
    - Map local directories ***/u/nasa*** to NFS server ***/vol/<ID>/home***
      - Each user's home directory is ***/u/nasa/{user_id}*** including "**uid=ta**"

Requirements (9/9)

- Custom shell script “addnasauser”
    - This script is used to create LDAP users so that users can login to all of your machines using LDAP
    - This script must...
        - create user data on LDAP server
        - create home directory ***/u/nasa/{new_user_id}*** for new user

Submission - Online Judge

- ❑ Your work will be tested by our online judge system
  - Submit a judge request when you are ready.
  - You can submit request multiple times. However, **the score of the last submission instead of the submission with the highest score**, will be taken.
  - **Late submissions are not accepted**.
  - Please check your score at OJ after judge completed.
- ❑ Scoring starts at : 2021/5/17 (Mon.) 00:00
  - The cool-down time is 30 minutes
- ❑ Deadline: 2021/6/3 (Thur.) 23:59

Submission - Online Demo

- ❑ Scoring Structure
  - Online Judge 75% + Demo 25%
- ❑ Failed to complete Demo + Q&A will results in a loss of 20% credit
- ❑ We will release a bonus problems one day before Demo time
  - At most 10 points
  - No partial credits
- ❑ Online Demo time: 18:30 ~ 21:30 on June 10th online
  - Demo time table and link will be announced later on e3

Help

- Due to the pandemic, NO TA office hours
  - Please ask your questions online
- Questions about this homework.
  1. Make sure you have studied through lecture slides and the HW spec.
  2. Clarify your problems and search it to find out solutions first.
  3. Ask them on https://groups.google.com/g/nctunasa .
     - Be sure to include all the information you think others would need.