Network Administration/System Administration (NTU CSIE, Spring 2024) Homework #8 - LDAP

B12902110 呂承諺

April 28, 2024

1 Server Setup

(a) LDIF files

`suffix.ldif`

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=nasa,dc=csie,dc=ntu
```

`root.ldif`

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=nasa,dc=csie,dc=ntu
-
replace: olcRootPW
# Password: admin
olcRootPW: {SSHA}1ojwc9fVLEYyrfJwo/0zc3HcsmqkPeRy
```

`records.ldif`

```
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

dn: cn=admin,dc=nasa,dc=csie,dc=ntu
cn: admin
objectClass: organizationalRole
description: admin account

dn: ou=people,dc=nasa,dc=csie,dc=ntu
ou: people
objectClass: organizationalUnit

dn: ou=group,dc=nasa,dc=csie,dc=ntu
ou: group
objectClass: organizationalUnit
```

Steps

(1) Install the packages.

```
$ apt install -y slapd ldap-utils
```

(2) Modify the LDAP records.

```
$ ldapmodify -Y EXTERNAL -H ldapi:/// -f suffix.ldif
$ ldapmodify -Y EXTERNAL -H ldapi:/// -f root.ldif
$ ldapadd -D cn=admin,dc=nasa,dc=csie,dc=ntu -w admin \
    -H ldapi:/// -f records.ldif
```

Result

```
$ ldapsearch -x -b dc=nasa,dc=csie,dc=ntu
```

```
root@ldap:~/ldap# ldapsearch -x -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# nasa.csie.ntu
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

# admin, nasa.csie.ntu
dn: cn=admin,dc=nasa,dc=csie,dc=ntu
cn: admin
objectClass: organizationalRole
description: admin account

# group, nasa.csie.ntu
dn: ou=group,dc=nasa,dc=csie,dc=ntu
ou: group
objectClass: organizationalUnit

# people, nasa.csie.ntu
dn: ou=people,dc=nasa,dc=csie,dc=ntu
ou: people
objectClass: organizationalUnit

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

References

- LDAP Lab - HackMD
- OpenLDAP Software 2.6 Administrator's Guide: Configuring slapd

(b) **LDIF Files**

`tls_certificates.ldif`

```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/servercrt.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/serverkey.pem
```

Steps

(1) Download script for generating certificates.

```
$ wget https://github.com/xbmc/openssl/raw/master/apps/CA.sh
$ chmod +x CA.sh
```

(2) Generate CA certificate.

```
$ ./CA.sh -newca
CA certificate filename (or enter to create)

Making CA certificate ...

...

Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            2a:49:2b:c0:1a:64:ca:46:81:3b:8d:cf:13:fb:ca:e8:30:bf:ae:e1
        Validity
            Not Before: Apr 27 18:40:57 2024 GMT
            Not After : Apr 27 18:40:57 2027 GMT
        Subject:
            countryName               = TW
            stateOrProvinceName       = Taiwan
            organizationName          = NTU CSIE
            commonName                = ca.nasa.csie.ntu
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                54:37:93:4B:4E:C0:AA:16:F5:43:12:74:5E:23:AE:CD:30:AC:51:C8
            X509v3 Authority Key Identifier:
                54:37:93:4B:4E:C0:AA:16:F5:43:12:74:5E:23:AE:CD:30:AC:51:C8
            X509v3 Basic Constraints: critical
                CA:TRUE
Certificate is to be certified until Apr 27 18:40:57 2027 GMT (1095 days)

Write out database with 1 new entries
Database updated
```

(3) Generate a certificate request.

```
$ ./CA.sh -newreq-nodes

...

Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NTU CSIE
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:ldap
Email Address []:

...

Request (and private key) is in newreq.pem
```

(4) Sign the certificate.

```
$ ./CA.sh -sign

...

Certificate Details:
        Serial Number:
            2a:49:2b:c0:1a:64:ca:46:81:3b:8d:cf:13:fb:ca:e8:30:bf:ae:e3
        Validity
            Not Before: Apr 27 19:43:08 2024 GMT
            Not After : Apr 27 19:43:08 2025 GMT
        Subject:
            countryName               = TW
            stateOrProvinceName       = Taiwan
            organizationName          = NTU CSIE
            commonName                = ldap
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                56:48:59:6D:F1:53:E1:3D:19:40:5F:9B:52:BF:BA:CC:E6:E6:D3:D3
            X509v3 Authority Key Identifier:
                54:37:93:4B:4E:C0:AA:16:F5:43:12:74:5E:23:AE:CD:30:AC:51:C8
Certificate is to be certified until Apr 27 19:43:08 2025 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

...

Signed certificate is in newcert.pem
```

(5) Copy the certificates to SLAPD's configuration folder, and set the file ownership and permission for `serverkey.pem`.

```
$ cp demoCA/cacert.pem /etc/ldap/cacert.pem
$ mv newcert.pem /etc/ldap/servercrt.pem
$ mv newreq.pem /etc/ldap/serverkey.pem
$ chown openldap /etc/ldap/serverkey.pem
$ chgrp openldap /etc/ldap/serverkey.pem
$ chmod 600 /etc/ldap/serverkey.pem
```

(6) Add the TLS certificate options to SLPD.

```
$ ldapmodify -Y EXTERNAL -H ldapi:/// -f tls_certificates.ldif
```

(7) Change `SLAPD_SERVICES` in `/etc/default/slap`.

```
# /etc/default/slapd
SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"
```

(8) Restart the SLAPD service.

```
$ systemctl restart slapd.service
```

(9) Set the CA certificate in the client configuration file `/etc/ldap/ldap.conf`.

```
# /etc/ldap/ldap.conf
TLS_CACERT /etc/ldap/cacert.pem
```

Result

```
$ ldapsearch -x -ZZ -b dc=nasa,dc=csie,dc=ntu
```

```
root@ldap:/etc/ldap# ldapsearch -x -ZZ -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# nasa.csie.ntu
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

# admin, nasa.csie.ntu
dn: cn=admin,dc=nasa,dc=csie,dc=ntu
cn: admin
objectClass: organizationalRole
description: admin account

# group, nasa.csie.ntu
dn: ou=group,dc=nasa,dc=csie,dc=ntu
ou: group
objectClass: organizationalUnit

# people, nasa.csie.ntu
dn: ou=people,dc=nasa,dc=csie,dc=ntu
ou: people
objectClass: organizationalUnit

# search result
search: 3
result: 0 Success

# numResponses: 5
# numEntries: 4
```

```
$ ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu
```

```
root@ldap:/etc/ldap# ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# nasa.csie.ntu
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

# admin, nasa.csie.ntu
dn: cn=admin,dc=nasa,dc=csie,dc=ntu
cn: admin
objectClass: organizationalRole
description: admin account

# group, nasa.csie.ntu
dn: ou=group,dc=nasa,dc=csie,dc=ntu
ou: group
objectClass: organizationalUnit

# people, nasa.csie.ntu
dn: ou=people,dc=nasa,dc=csie,dc=ntu
ou: people
objectClass: organizationalUnit

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

References

- OpenLDAP Software 2.6 Administrator's Guide: Using TLS
- OpenLDAP Faq-O-Matic: How do I use TLS/SSL?
- openssl/apps/CA.sh at master ·xbmc/openssl ·GitHub
- /docs/man3.3/man1/openssl-ca.html
- /docs/man3.3/man1/openssl-req.html
- Certificate signing request - Wikipedia
- OpenLDAP Software 2.6 Administrator's Guide: The slapd Configuration File
- ssl - How to enable TLS on OpenLDAP - Server Fault
- ldap - ldap_modify: Other (e.g., implementation specific) error (80) - Stack Overflow
- [SOLVED] Issues with OpenLDAP and SSL / TLS
- ldap_start_tls: Connect error (-11)
- `man slapd`, `man slapd.conf`, and `man slapd-config`

2 Client setup

(a) **Steps**

Install the `openldap` package.

```
$ pacman -S openldap
```

Result

```
$ ldapsearch -x -H ldap://192.168.8.0 -b dc=nasa,dc=csie,dc=ntu
```

```
[root@arch openldap]# ldapsearch -x -H ldap://192.168.8.0 -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# nasa.csie.ntu
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

# admin, nasa.csie.ntu
dn: cn=admin,dc=nasa,dc=csie,dc=ntu
cn: admin
objectClass: organizationalRole
description: admin account

# group, nasa.csie.ntu
dn: ou=group,dc=nasa,dc=csie,dc=ntu
ou: group
objectClass: organizationalUnit

# people, nasa.csie.ntu
dn: ou=people,dc=nasa,dc=csie,dc=ntu
ou: people
objectClass: organizationalUnit

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
[root@arch openldap]#
```

References

- OpenLDAP - ArchWiki
- Arch Linux - openldap 2.6.7-2 (x86_64)

(b) **LDIF files**

`security.ldif`

```
dn: cn=config
changetype: modify
add: olcSecurity
olcSecurity: tls=1
```

Steps

(1) On the server configuration, set the `olcSecurity` option to `tls=1`.

```
$ ldapmodify -Y EXTERNAL -H ldapi:/// -f security.ldif
```

(2) Set `TLS_REQCERT allow` in the client's `/etc/opneldap/ldap.conf`. This allows bad certificates (our certificate is self-signed) to be ignored, and the session proceeds normally.

```
# /etc/openldap/ldap.conf
TLS_REQCERT allow
```

Result

```
$ ldapsearch -x -H ldap://192.168.8.0 -b dc=nasa,dc=csie,dc=ntu
```

```
[root@arch openldap]# ldapsearch -x -H ldap://192.168.8.0 -b dc=nasa,dc=csie,dc=ntu
ldap_bind: Confidentiality required (13)
        additional info: TLS confidentiality required
[root@arch openldap]#
```

```
$ ldapsearch -ZZ -x -b dc=nasa,dc=csie,dc=ntu
$ ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu
```

```
root@ldap:/etc/ldap# ldapsearch -x -ZZ -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# nasa.csie.ntu
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

# admin, nasa.csie.ntu
dn: cn=admin,dc=nasa,dc=csie,dc=ntu
cn: admin
objectClass: organizationalRole
description: admin account

# group, nasa.csie.ntu
dn: ou=group,dc=nasa,dc=csie,dc=ntu
ou: group
objectClass: organizationalUnit

# people, nasa.csie.ntu
dn: ou=people,dc=nasa,dc=csie,dc=ntu
ou: people
objectClass: organizationalUnit

# search result
search: 3
result: 0 Success

# numResponses: 5
# numEntries: 4
```

```
root@ldap:/etc/ldap# ldapsearch -x -H ldaps:/// -b dc=nasa,dc=csie,dc=ntu
# extended LDIF
#
# LDAPv3
# base <dc=nasa,dc=csie,dc=ntu> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# nasa.csie.ntu
dn: dc=nasa,dc=csie,dc=ntu
dc: nasa
objectClass: top
objectClass: domain

# admin, nasa.csie.ntu
dn: cn=admin,dc=nasa,dc=csie,dc=ntu
cn: admin
objectClass: organizationalRole
description: admin account

# group, nasa.csie.ntu
dn: ou=group,dc=nasa,dc=csie,dc=ntu
ou: group
objectClass: organizationalUnit

# people, nasa.csie.ntu
dn: ou=people,dc=nasa,dc=csie,dc=ntu
ou: people
objectClass: organizationalUnit

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

References

- OpenLDAP - ArchWiki (2.5.3 Start slapd with SSL)
- ldap - Configure OpenLDAP with TLS=required - Server Fault
- `man ladp.conf` and `man slapd-config`

(c) **Steps**

(1) Install the `sssd` and `sudo` packages.

```
$ pacman -S sssd sudo
```

(2) Edit `/etc/sssd/sssd.conf` to the following configuration.

```
#/etc/sssd/sssd.conf
[sssd]
config_file_version = 2
services = nss, pam, sudo
domains = LDAP

[domain/LDAP]
cache_credentials = true
enumerate = true
id_provider = ldap
auth_provider = ldap
ldap_uri = ldap://192.168.8.0
ldap_search_base = dc=nasa,dc=csie,dc=ntu
ldap_id_use_start_tls = true
ldap_tls_reqcert = allow
chpass_provider = ldap
ldap_chpass_uri = ldap://192.168.8.0
```

(3) Change permission of `/etc/sssd/sssd.conf` to 600.

```
$ chmod 600 /etc/sssd/sssd.conf
```

(4) Edit the following options in `/etc/nsswitch.conf`.

```
#/etc/nsswitch.conf
passwd: files systemd sss
group: files [SUCCESS=merge] systemd sss
shadow: files systemd sss
gshadow: files systemd sss
sudoers: files sss

...
```

(5) Add the following lines to `/etc/pam.d/system-auth`.

```
#/etc/pam.d/system-auth
auth sufficient pam_sss.so forward_pass
auth required pam_faillock.so preauth

...

account [default=bad success=ok user_unknown=ignore authinfo_unavail=ignore]
↪  pam_sss.so
-account [success=1 default=ignore] pam_systemd_home.so

...

password sufficient pam_sss.so

...

session required pam_mkhomedir.so skel=/etc/skel/ umask=0077
-session optional pam_systemd_home.so
session required pam_limits.so
session required pam_unix.so
session optional pam_sss.so
```

(6) `/etc/pam.d/sudo` includes `system-auth` by default, so we don't need to make manual changes.

(7) Restart services.

```
$ systemctl sssd.service sshd.service
```

References

- System Security Services Daemon - Wikipedia
- LDAP authentication - ArchWiki (2.2 Online and offline authentication with SSSD)
- sssd.conf(5) —Arch manual pages
- sssd-ldap(5) —Arch manual pages
- nsswitch.conf(5) - Linux man page
- pam.d(5) - Linux man page

(d) **LDIF files**

groups.ldif

```
dn: cn=ta,ou=group,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: posixGroup
cn: ta
gidNumber: 100

dn: cn=student,ou=group,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: posixGroup
cn: student
gidNumber: 101
```

users.ldif

```
dn: uid=ta1,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: ta1
uid: ta1
uidNumber: 1111
gidNumber: 100
homeDirectory: /home/ta1
loginShell: /bin/bash
# password: ta1
userPassword: {SSHA}VJK0YEvGVD9EXyFRgUzZLCqPh+51AJe6

dn: uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: b12902110
uid: b12902110
uidNumber: 2222
gidNumber: 101
homeDirectory: /home/b12902110
loginShell: /bin/bash
# password: b12902110
userPassword: {SSHA}UUp1zw0J+1LAoopRqTz0flwBzjbIMmWr
```

sudoers.ldif

```
dn: ou=SUDOers,dc=nasa,dc=csie,dc=ntu
objectClass: organizationalUnit
ou: SUDOers

dn: cn=%ta,ou=SUDOers,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: sudoRole
cn: %ta
sudoUser: %ta
sudoHost: ALL
sudoCommand: ALL
```

Steps

(1) Temporarily disable `olcSecurity`, then add the sudo schema.

```
$ wget https://github.com/sudo-project/sudo/raw/main/docs/schema.olcSudo
$ ldapadd -Y EXTERNAL -H ldapi:/// -f schema.olcSudo
```

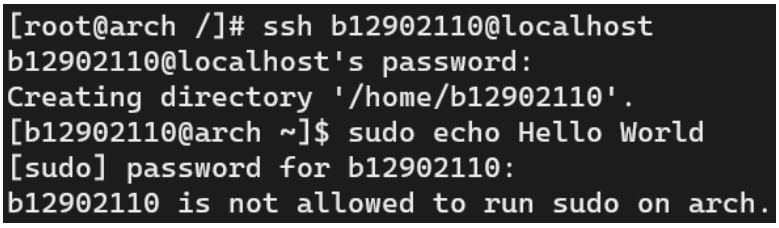
(2) Add the groups, users, and sudoers records.

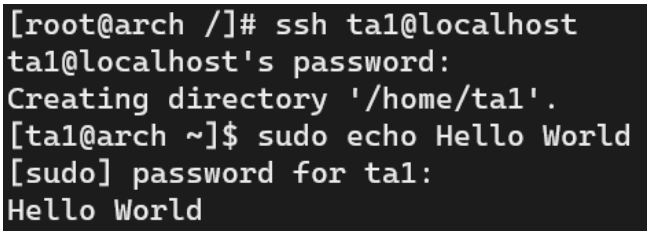
```
$ ldapadd -Z -D cn=admin,dc=nasa,dc=csie,dc=ntu -w admin -H ldapi:/// \
    -f groups.ldif
$ ldapadd -Z -D cn=admin,dc=nasa,dc=csie,dc=ntu -w admin -H ldapi:/// \
    -f users.ldif
$ ldapadd -Z -D cn=admin,dc=nasa,dc=csie,dc=ntu -w admin -H ldapi:/// \
    -f sudoers.ldif
```

Result

```
[root@arch /]# ssh b12902110@localhost
b12902110@localhost's password:
Creating directory '/home/b12902110'.
[b12902110@arch ~]$ sudo echo Hello World
[sudo] password for b12902110:
b12902110 is not allowed to run sudo on arch.

[root@arch /]# ssh ta1@localhost
ta1@localhost's password:
Creating directory '/home/ta1'.
[ta1@arch ~]$ sudo echo Hello World
[sudo] password for ta1:
Hello World
```





References

- `ws5:~$ ldapsearch -x cn=student`
- Sudoers LDAP Manual | Sudo
- README.LDAP | Sudo
- sudo/docs/schema.olcSudo at main ·sudo-project/sudo ·GitHub

3 Access Control Lists

LDIF files

`acl.ldif`

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to attrs=userPassword
  by self write
  by anonymous auth
  by * none
olcAccess: {1}to attrs=uid,uidNumber,gidNumber,homeDirectory
  by * read
olcAccess: {2}to *
  by self write
  by * read
```

Steps

Temporarily disable `olcSecurity`, then commit `ACL.ldif`.

```
$ ldapmodify -Y EXTERNAL -H ldapi:/// -f acl.ldif
```

Result

(a) Users can only change its own information, and cannot change other users' information.

```
root@ldap:~# ldapmodify -Z -D uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu -w b12902110
dn: uid=ta1,ou=people,dc=nasa,dc=csie,dc=ntu
changetype: modify
replace: cn
cn: ta1

modifying entry "uid=ta1,ou=people,dc=nasa,dc=csie,dc=ntu"
ldap_modify: Insufficient access (50)

root@ldap:~# ldapmodify -Z -D uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu -w b12902110
dn: uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu
changetype: modify
replace: cn
cn: b12902110

modifying entry "uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu"

^C
```

(b) Users cannot change UID, GID and home directory.

```
root@ldap:~# ldapmodify -Z -D uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu -w b12902110
dn: uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu
changetype: modify
replace: homeDirectory
homeDirectory: /home/b12902110_changed

modifying entry "uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu"
ldap_modify: Insufficient access (50)

root@ldap:~# ldapmodify -Z -D uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu -w b12902110
dn: uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu
changetype: modify
replace: uidNumber
uidNumber: 1001

modifying entry "uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu"
ldap_modify: Insufficient access (50)
```

(c) Anonymous can read information except password.

```
root@ldap:~# # (c) Anonymous can read information except password.
ldapsearch -LLL -Z -x -b dc=nasa,dc=csie,dc=ntu "(objectClass=posixAccount)"
dn: uid=ta1,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: ta1
uid: ta1
uidNumber: 1111
gidNumber: 100
homeDirectory: /home/ta1
loginShell: /bin/bash

dn: uid=b12902110,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
uid: b12902110
uidNumber: 2222
gidNumber: 101
homeDirectory: /home/b12902110
loginShell: /bin/bash
cn: b12902110
```

References

- OpenLDAP Software 2.6 Administrator's Guide: Access Control
- debian - How to correctly ldapmodify replace olcAccess lines? - Server Fault

4 Scripts

The scripts should be run at the server since we're using `-H ldapi:///`.

`add_user.sh`

```
#!/bin/bash

read -rs -p "Admin password (password for cn=admin,dc=nasa,dc=csie,dc=ntu): " \
  admin_password
echo
read -r -p "Username: " username
read -rs -p "Password: " password
echo
echo

hashed_password="$(slappasswd -s "${password}")"
max_uid="$(
  ldapsearch -LLL -Z -D cn=admin,dc=nasa,dc=csie,dc=ntu -w "${admin_password}" \
      -H ldapi:/// -b "ou=people,dc=nasa,dc=csie,dc=ntu" uidNumber |
    grep uidNumber: |
    sed 's/uidNumber: //g' |
    sort -n |
    tail -n 1
)"
next_uid="$(( "${max_uid}" + 1 ))"

echo "Adding user ${username}..."
echo "dn: uid=${username},ou=people,dc=nasa,dc=csie,dc=ntu"
echo "uidNumber: ${next_uid}"
echo "homeDirectory: /home/${username}"
echo

ldapadd -Z -D cn=admin,dc=nasa,dc=csie,dc=ntu -w "${admin_password}" \
  -H ldapi:///<<END
dn: uid=${username},ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: ${username}
uid: ${username}
uidNumber: ${next_uid}
gidNumber: 101
homeDirectory: /home/${username}
loginShell: /bin/bash
userPassword: ${hashed_password}
END
```

del_user.sh

```
#!/bin/bash

read -rs -p "Admin password (password for cn=admin,dc=nasa,dc=csie,dc=ntu): " \
  admin_password
echo
read -r -p "Username: " username
echo

echo "Deleting user ${username}..."
echo "dn: uid=${username},ou=people,dc=nasa,dc=csie,dc=ntu"
echo

ldapdelete -Z -D cn=admin,dc=nasa,dc=csie,dc=ntu -w "${admin_password}" \
  -H ldapi:/// "uid=${username},ou=people,dc=nasa,dc=csie,dc=ntu"
```

Result

```
$ ./add_user.sh
Admin password (password for cn=admin,dc=nasa,dc=csie,dc=ntu):
Username: user1
Password:

...

adding new entry "uid=user1,ou=people,dc=nasa,dc=csie,dc=ntu"

$ ldapsearch -LLL -x -b dc=nasa,dc=csie,dc=ntu uid=user1
dn: uid=user1,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: user1
uid: user1
uidNumber: 2223
gidNumber: 101
homeDirectory: /home/user1
loginShell: /bin/bash

$ ./del_user.sh
Admin password (password for cn=admin,dc=nasa,dc=csie,dc=ntu):
Username: user1

Deleting user user1...
dn: uid=user1,ou=people,dc=nasa,dc=csie,dc=ntu

$ ldapsearch -LLL -x -b dc=nasa,dc=csie,dc=ntu uid=user1
```

```
root@ldap:~/scripts# ./add_user.sh
Admin password (password for cn=admin,dc=nasa,dc=csie,dc=ntu):
Username: user1
Password:

Adding user user1...
dn: uid=user1,ou=people,dc=nasa,dc=csie,dc=ntu
uidNumber: 2223
homeDirectory: /home/user1

adding new entry "uid=user1,ou=people,dc=nasa,dc=csie,dc=ntu"

root@ldap:~/scripts# ldapsearch -LLL -x -b dc=nasa,dc=csie,dc=ntu uid=user1
dn: uid=user1,ou=people,dc=nasa,dc=csie,dc=ntu
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: user1
uid: user1
uidNumber: 2223
gidNumber: 101
homeDirectory: /home/user1
loginShell: /bin/bash

root@ldap:~/scripts# ./del_user.sh
Admin password (password for cn=admin,dc=nasa,dc=csie,dc=ntu):
Username: user1

Deleting user user1...
dn: uid=user1,ou=people,dc=nasa,dc=csie,dc=ntu

root@ldap:~/scripts# ldapsearch -LLL -x -b dc=nasa,dc=csie,dc=ntu uid=user1
root@ldap:~/scripts#
```

References

- Users, Groups, UIDs and GIDs on systemd Systems
- shell - How do I read user input into a variable in Bash? - Stack Overflow
- Bash Builtins (Bash Reference Manual) (read)
- Redirections (Bash Reference Manual) (3.6.6 Here Documents)
- slappasswd
- ldapdelete