Tutorial 2

From ACE Lab

Team Name: _____

LDAP

LDAP allows you to centralise authentication on your cluster. This allows users to have a single account which is shared across all the cluster's services.

Part 1 – Server Setup

1. Install dependencies

```
yum install openldap-servers openldap-clients
```

2. Setup LDAP server

```
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown ldap. /var/lib/ldap/DB_CONFIG
systemctl start slapd
```

3. Set the slapd service to run at startup.

4. Generate a password hash

```
slappasswd
```

You should see:

```
{SSHA}xxxxxxxxxxxxxxxxxxxxxxxx
```

QUESTION 1:
What is a hash?

_____

_____

_____

import your hash:

```
vim chrootpw.ldif
```

```
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx
```

import configuration into LDAP:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.ldif
```

5. Import basic Schemas:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

6. Populate LDAP database

generate directory manager's password:

```
slappasswd
```

You should see:

```
{SSHA}xxxxxxxxxxxxxxxxxxxxxxx
```

create database configuration file chdomain.ldif :

```
dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
  read by dn.base="cn=Manager,dc=<localdomain>,dc=<com>" read by * none

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=<localdomain>,dc=<com>

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=<localdomain>,dc=<com>

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}xxxxxxxxxxxxxxxxxxxxxxxx

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange by
  dn="cn=Manager,dc=<localdomain>,dc=<com>" write by anonymous auth by self write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=Manager,dc=<localdomain>,dc=<com>" write by * read
```

NOTE: Be sure to replace "cn=Manager,dc=localdomain,dc=com" with the domain name you set for your cluster.

import configuration into LDAP:

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

QUESTION 2:
What is a domain?

_____
_____
_____

7. Restart the LDAP Server

8. Generate an SSL certificate

```
openssl req -new -x509 -nodes -out  /etc/pki/tls/certs/slapdcert.pem -keyout  /etc/pki/tls/certs/slapdkey.pem -days 365
```

QUESTION 3:
What is the purpose of an SSL certificate?

_____
_____
_____

9. Copy and change ownership of the certificates you generated

```
cp /etc/pki/tls/certs/slapdkey.pem /etc/pki/tls/certs/slapdcert.pem /etc/pki/tls/certs/ca-bundle.crt /etc/openldap/certs/
chown ldap. /etc/openldap/certs/slapdkey.pem /etc/openldap/certs/slapdcert.pem /etc/openldap/certs/ca-bundle.crt
```

10. Create certificate insertion script:

```
vim mod_ssl.ldif
```

```
# create new
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/openldap/certs/ca-bundle.crt
-
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/openldap/certs/slapdcert.pem
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/openldap/certs/slapdkey.pem
```

link certificates

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

edit /etc/sysconfig/slapd

```
# line 9: add
SLAPD_URLS="ldapi:/// ldap:/// ldaps:///"
```

11. Restart slapd

Part 2 – LAM

1. Install LAM web frontend

```
yum install php php-ldap
```

2. Download LAM

```
https://www.ldap-account-manager.org/lamcms/releases
```

and install it:

```
rpm -i ldap-account-manager
```

3. restart httpd

4. Tunnel into the cluster. Call a tutor for assistance

5. With your web-browser visit http://headnode/lam

```
http://headnode/lam
```

6. Follow "LAM Configuration" link

7. Follow "Edit general settings" link, login with password "lam" and set master password

8. Follow "Edit server profiles" link, login with password "lam"

9. Set all the domains and the password on "General settings" and Account types" tabs

10. Login with LDAP root password

11. Click create to create base LDAP Configuration

12. Click "groups", "new group"

13. Create group "users"

14. Create group "admins"

15. Create a user account for yourself, add your username to the users group.

LDAP Client Setup

These steps need to executed on the head node and the compute nodes.

1. Install nss-pam-ldapd

2. Enable TLS support for the client

```
echo "TLS_REQCERT allow" >> /etc/openldap/ldap.conf
echo "tls_reqcert allow" >> /etc/nslcd.conf
```

3. Run through the LDAT client setup wizard

```
authconfig-tui
```

```
[*] Use LDAP
[*] Use Shadow Passwords
[*] Use LDAP Authetication
[*] Local authorization is sufficient
```

```
[*] Use TLS
Server: ldap://headnode.cluster.scc
Base DN: dc=cluster,dc=scc
```

4. By default user home directories are not created automatically, enable it

```
authconfig --enablemkhomedir --update
```

5. Test the LDAP Server

```
slaptest -u
ldapsearch -x -b "dc=<localdomain>,dc=<com>"
```

it should return “search: 2”

6. Test with TLS encryption:

```
ldapsearch -x -b "dc=<localdomain>,dc=<com>" -ZZ
```

it should return “search: 3”

7. The easiest way to propagate sudo access is you create an LDAP group for sudo users and add that group to the sudoers file. Edit sudoers file, add:

```
%<admin_group>    ALL=(ALL)       ALL
```