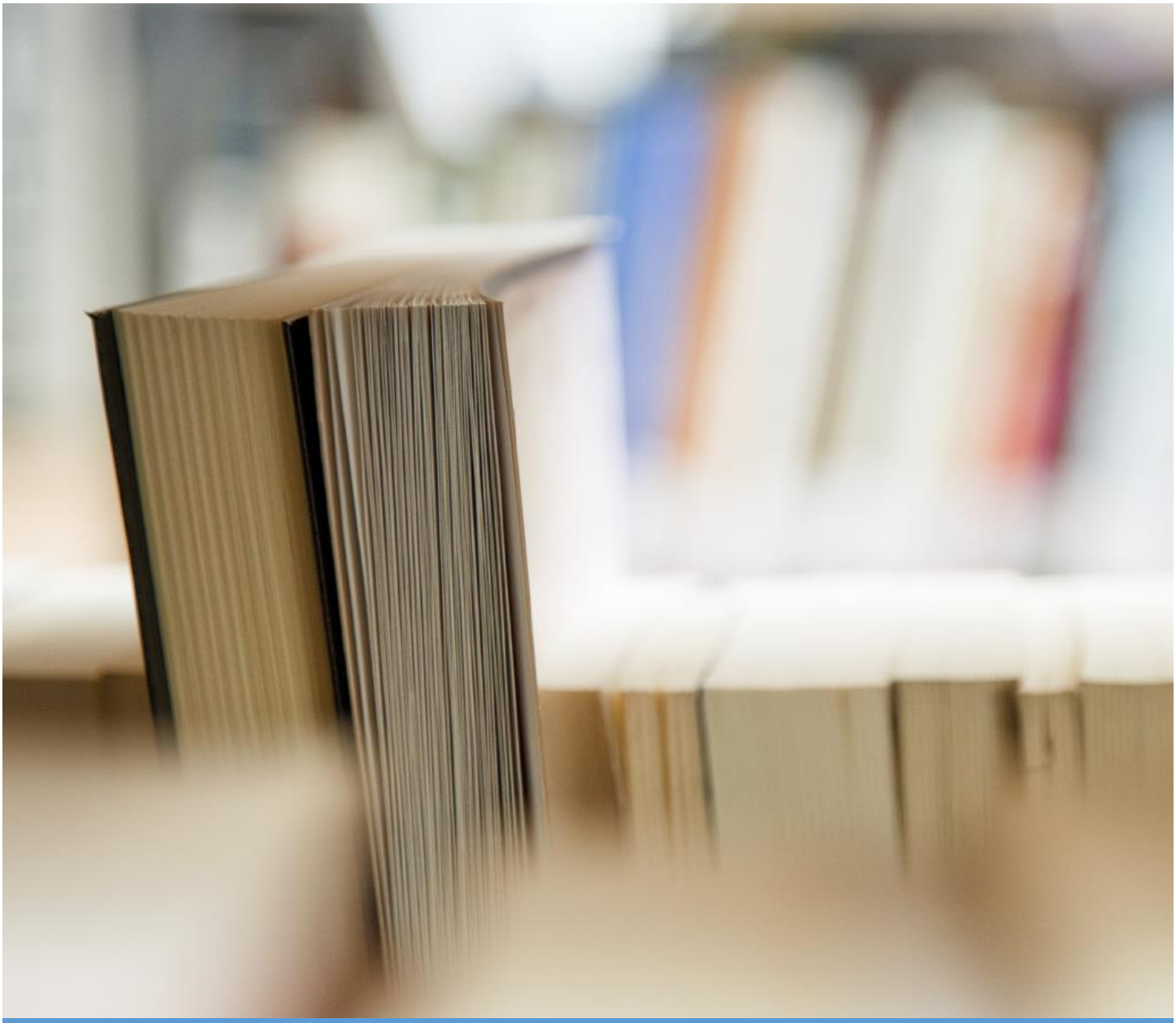

LDAP Server Setup

CIS 5690

lal pasha shaik

7/1/16

Advanced Systems Project

Table of Contents

Purpose of this document

- This document helps Linux administrators to setup openLDAP server. It provides guidance and required setting to setup LDAP master server.

Introduction

- As part of the CIS5690 - Data Center Build Automation , the following script configures the LDAP client.

  ASP-OEL-LDP.sh

- Which will setup the client with LDAP master with the following information

```
URI ldap://${pkgserver/
BASE dc=ucmo,dc=edu
```

- Where $pkgserver is the ldap master server hostname/ipaddress.

- For this project we are using 10.1.1.2 as the LDAP master server as well as the build/backup server.

SCOPE

- This procedure is tested in the Oracle enterprise Linux 7.2 version.
- It should also work on CentOS7/RHEL7 versions.
- Options may be different in the previous version such as RHEL5/RHEL6

Install OpenLDAP server

- Install the appropriate LDAP packages "openldap" and "migrationtools" using yum
- Yum should be configured as part of the ASP-OEL-RPO.sh script.
- Run the following command to install openldap servers packages

```
# yum -y install *openldap* migrationtools
```

Create a LDAP root password

- Create the ldap administrative password using the command : “slappasswd”.

```
# slappasswd
New password:
Re-enter new password:
{SSHA}LnQRK8/1YnCvYe1AxGErNm8GrqLivvvB
```

- Enter the password and copy the encrypted string

Edit the OpenLDAP Server Configuration

- OpenLDAP server Configuration files are located in /etc/openldap/slapd.d/.
- Go to cn=config directory under /etc/openldap/slapd.d/ and edit the "olcDatabase={2}hdb.ldif" for changing the configuration.

```
# cd /etc/openldap/slapd.d/cn=config
# vi olcDatabase={2}hdb.ldif
```

- Change the variables of "olcSuffix" and "olcRootDN" according to our domain as below.

```
olcSuffix: dc=ucmo,dc=edu
olcRootDN: cn=Manager,dc=ucmo,dc=edu
```

- add ldap password entry to the file : olcDatabase={2}hdb.ldif

```
olcRootPW: {SSHA}dizb1yD3YD3P+vkn9tyzaZKgwVFh3XE2
```

Verify the configuration

- Run slaptest –u to verify the configuration

```
# slaptest -u
57773d8c ldif_read_file: checksum error on
"/etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif"
57773d8c ldif_read_file: checksum error on
"/etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldif"
config file testing succeeded
```

- ignore checksum errors

Enable and Start the SLAPD service

- Use systemctl to start and enable the slapd server

```
systemctl start slapd
systemctl enable slapd
```

- Run netstat command and verify if the ldap port is opened

```
# netstat -lt4
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:nfs             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ldap            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:57959           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:56426           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:http            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:mountd          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
```

Configure the LDAP Database

- Copy the Sample Database Configuration file, change the file permissions as below.

```
cp /usr/share/openldap-servers/DB_CONFIG.example  \
/var/lib/ldap/DB_CONFIG

chown -R ldap:ldap /var/lib/ldap/
```

Add the following LDAP Schemas

- Run the following commands to add 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
```

Create base objects in OpenLDAP

- To create base objects in OpenLDAP, we need migration tools to be installed.
- Change below predefined values in the file "migrate_common.ph" according to our domain name.

```
cd /usr/share/migrationtools/
vi migrate_common.ph
```

- Go to Line Number 71 and change your domain name

```
$DEFAULT_MAIL_DOMAIN = "ucmo.edu"
```

- Go to line number 74 and change your base name

```
$DEFAULT_BASE = "dc=ucmo,dc=edu";
```

- Go to line number 90 and change your EXTENDED_SCHEMA from "0" to "1"

```
$EXTENDED_SCHEMA = 1
```

Generate a base.ldif file for the Domain

- Copy the below lines and paste inside the file /root/base.ldif.

```
dn: dc=ucmo,dc=edu
objectClass: top
objectClass: dcObject
objectclass: organization
o: ucmo edu
dc: ucmo

dn: cn=Manager,dc=ucmo,dc=edu
objectClass: organizationalRole
cn: Manager
description: Directory Manager

dn: ou=People,dc=ucmo,dc=edu
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=ucmo,dc=edu
objectClass: organizationalUnit
ou: Group
```

Create Users and migrate to LDAP

- Create users and set password to : cis5690

```
useradd ucm1
useradd ucm2
echo "cis5690" | passwd --stdin ucm1
echo "cis5690" | passwd --stdin cum2
```

- Filter out these user from /etc/passwd to another file:

```
grep ucm /etc/passwd > /root/passwd
```

- Filter out user group from /etc/group to another file:

```
grep ucm /etc/group > /root/group
```

- Now Convert the Individual Users file to LDAP Data Interchange Format (LDIF)
  Generate a ldif file for users

```
./migrate_passwd.pl /root/passwd /root/users.ldif
```

- Generate a ldif file for groups

```
./migrate_group.pl /root/group /root/groups.ldif
```

Import Users in to the LDAP Database.

- User ldapadd command to import these ldif file

```
ldapadd -x -W -D "cn=Manager,dc=ucmo,dc=edu" -f /root/base.ldif
ldapadd -x -W -D "cn=Manager,dc=ucmo,dc=edu" -f /root/users.ldif
ldapadd -x -W -D "cn=Manager,dc=ucmo,dc=edu" -f /root/groups.ldif
```

Test the configuration.

- Use ldapsearch to verify the configuration

```
# ldapsearch -x cn=ucm1 -b dc=ucmo,dc=edu
```

- Sample output

```
# ucm1, people, ucmo.edu
dn: uid=ucm1,ou=people,dc=ucmo,dc=edu
uid: ucm1
cn: ucm1
sn: ucm1
mail: ucm1@ucmo.edu
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword::
e2NyeXB0fSQ2JDc5N3h0YVRQJFI4cFVoclBiMnlkc2MwbWIyM2M1aXZkbG0ybGV

MUUovUVNIeGdCVHJjc3Q5MTF4QzV3WlU3UFJLTURUeU5wc09VbzhmMFhXdXl1eFhhN1phSGVHeEYw
shadowLastChange: 16983
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1002
gidNumber: 1002
```

Ldap Client Configuration to use LDAP Server

```
yum install -y openldap-clients nss-pam-ldapd
```

- authconfig-tui can be used to configure ldap client.

```
URI ldap://10.1.1.2/
BASE dc=ucmo,dc=edu
```

Test the Client Configuration.

From the client use getent to query the password.

```
# getent passwd ucm1
ucm1:x:1002:1002::/home/ucm1:/bin/bash
```

DOCUMENT SIGNOFF

Nature of Signoff	Person	Signature	Date
Author	Lal Pasha Shaik		
Reviewer	Dr. Kesh		