



## **HCL MT CH-MSP Product Documentation**

### **Multi-Tenant Dependencies**

## Multi-Tenant Dependencies

Topics include:

- Setting up OpenLDAP for Multi-Tenant
- Understanding the Keycloak dependency

## Setting up OpenLDAP for Multi-Tenant

Setup OpenLDAP for MT > [https://apps.na.collabserv.com/wikis/home?lang=en-us#!/wiki/W0d07dd0b225e\\_410e\\_a5c4\\_1b9cfc43101d/page/Setup%20OpenLDAP%20for%20MT](https://apps.na.collabserv.com/wikis/home?lang=en-us#!/wiki/W0d07dd0b225e_410e_a5c4_1b9cfc43101d/page/Setup%20OpenLDAP%20for%20MT)

The following updates were made to the way OpenLDAP is defined - the mtl dif.zip file attached contains the updates for the sample tree. You can populate these changes into your LDAP server.

1. redefining the DN to be uid=<subscriber Id> instead of cn=<users name>
2. uid attribute has the value of subscriberId instead of the name
3. the ibm-entryUuid attribute is available in the

schema however it is not populated now (not needed to be populated) These steps were performed on CentOS 7. In theory, similar commands should work on any other Linux-based platforms. [mtldif.zip](#)

### 1. Install OpenLDAP: - OS: Centos 7

1. Install OpenLDAP using yum:

```
$sudo yum install -y openldap openldap-clients openldap-servers
```

OpenLDAP would be installed in **/etc/openldap** directory. Please verify such directory was created after the install.

In the rest of the instruction, this directory would be used/assumed. If OpenLDAP was not installed at this location, please update the paths accordingly.

2. Set up admin account and base:

```
$ cd /etc/openldap/slapd.d/cn=config
```

- a). Edit **olcDatabase={2}hdb.ldif** with the following suffix:

```
olcSuffix: dc=hcl,dc=com  
olcRootDN: cn=<ENTER YOUR
```

LOGIN here - e.g.

```
mikib>,dc=hcl,dc=com Save file.
```

- b). Create your ldap admin password:

At command prompt, issue the following commands to create and retrieve admin credential:

```
$ slappasswd  
New password: <ENTER YOUR PASSWORD HERE>  
Re-enter password: <REENTER PASSWORD>
```

<OUTPUT is a

hash key> -

COPY IT c). Add

the root credential

to config file:

Edit **olcDatabase={2}hdb.ldif** :

At the end of the file, add the following line

olcRootPW: <the HASH KEY YOU COPIED FROM ABOVE>

Save file.

c). Verify configuration file by running

\$ slaptest -u  
(ignore

the CRC

error) d).

Start ldap

\$ service

slapd

start e).

Verify

ldap

query

\$ ldapsearch -x -b "dc=hcl,dc=com"

You should see the results with the base "dc=hcl,dc=com"

## II. **IMPORT BASE LDAP SCHEMA:**

i. Add BASE schema:

Locate the file base.ldif (from the mtlldif.zip package you unzipped), and run:

```
$ ldapadd -x -W -D "cn=<user
```

```
login you used>,dc=hcl,dc=com" -
```

f base.ldif b). Verify the structure

we imported above:

```
$ ldapsearch -x -W -D "cn=<user login you used>,dc=hcl,dc=com" -b "dc=hcl,dc=com" "(objectclass=*)"
```

2. Import MT schema:

In the mtl dif.zip package locate the file mt\_custom.schema, e.g. **/home/centos/mtldif/ldap**

```
$ cp mt_custom.schema /etc/openldap/schema/.
```

```
$ mkdir -p /tmp/ldap_config
```

```
$ cd /tmp/ldap_config
```

```
$ slaptest -f /home/centos/mtldif/ldap/mt.conf -F /tmp/ldap_config
```

Running the above command will create a bunch of files in **/tmp/ldap\_config/cn\=config**

Copy the ldif files to the OpenLDAP config directory and change the ownership if needed:

```
$ cp /tmp/ldap_config/cn\=config/cn\=schema/cn*.ldif /etc/openldap/slapd.d/cn\=config/cn\=schema/
```

```
$ chown ldap:ldap
```

```
/etc/openldap/slapd.d/cn\=confi
```

```
g/cn\=schema/*.ldif RESTART
```

ldap:

## Setting up OpenLDAP for Multi-Tenant

```
$ service slapd stop  
$ service slapd start
```

### iii. **IMPORT MT LDIF files: base, orgs, and USERS:**

cd to the directory you unzipped mtl dif.zip, and run the following commands in the exact order:

```
$ ldapadd -x -W -D "cn=<user login you used>,dc=hcl,dc=com" -f mt_base.ldif  
$ ldapadd -x -W -D "cn=<user login you used>,dc=hcl,dc=com" -f mt_orgs.ldif  
$ ldapadd -x -W -D "cn=<user login you used>,dc=hcl,dc=com" -f mt_users.ldif  
$ ldapadd -x -W -D "cn=<user login you used>,dc=hcl,dc=com" -f mt_users-generic.ldif
```

Verify the users were imported:

BROWSE the directory - either using query or apache directory studio or whatever you normally use and make sure the users and organization descriptions are present Note: ALL users in the mt\_users.ldif have their passwords set as: password

## Understanding the Keycloak dependency

Keycloak documentation is currently maintained in the MSP community.

See [https://apps.na.collabserv.com/wikis/home?lang=en-us#!/wiki/W0d07dd0b225e\\_410e\\_a5c4\\_1b9cfc43101d/page/Keycloak%20Authentication%20and%20SSO](https://apps.na.collabserv.com/wikis/home?lang=en-us#!/wiki/W0d07dd0b225e_410e_a5c4_1b9cfc43101d/page/Keycloak%20Authentication%20and%20SSO)

Note: The dotted line from connections to ldap is not required for authentication. It may be used for group support from application level. Although it should really be done using keycloak APIs, the existing code may be doing a direct ldap call.

