# LDAP User and Group sync in Openshift

whitelist.txt

oauth.yaml

ldap-groupsync.yaml

blacklist.txt

Openshift users and group sync from LDAP

## Docker pull

```
sudo docker pull fabric8/389ds:latest
```

## Docker Run

```
sudo docker run -d --name my-389ds -e "DIRSRV_ADMIN_USERNAME=admin,DIRSRV_ADMIN_PASSWORD=12345,
DIRSRV_MANAGER_PASSWORD=12345,DIRSRV_SUFFIX=dc=example,dc=com" -p 0.0.0.0:389:389 fabric8/389ds:latest
```

## git clone this repo files and copy the .ldif files into my-389ds docker container

```
docker cp dsuser.ldif containerid:/tmp/
```

## Create user password

```
slappasswd -h {SSHA} -s user@123 {SSHA}GGcZ8O1vCFWnRE3QsyquKVcll+JKbVqi
```

Add user password into user schema

```
userPassword: {SSHA}GGcZ8O1vCFWnRE3QsyquKVcll+JKbVqi
```

## Ldapadd the schema into docker image.

```
ldapadd -f /tmp/schema.ldif -D "cn=directory manager" -w admin@123 ldapadd -f schema.ldif -D "cn=directory manager" -w admin@123
 ldapadd -f /tmp/dsusers.ldif -D "cn=directory manager" -w admin@123 ldapadd -f schema.ldif -D "cn=directory manager" -w admin@123
```

Now the custom users and groups added into the LDAP DB.

## Verify the newly added users into LDAP DB

```
ldapsearch -b "dc=example,dc=com" -D "cn=directory manager" -w admin@123
```

## Create openshift Oauth configuration..

To use the identity provider, you must define an OpenShift Container Platform Secret that contains the bindPassword.

Define an OpenShift Container Platform Secret that contains the bindPassword.

```
$ oc create secret generic ldap-bind-password-bbgr4
 --from-literal=bindPassword=admin@123 -n openshift-config
```

## Edit openshift oauth

Oc edit oauth cluster and add identity providers as ldap

Ref file oauth.yaml

## Create the ldap-groupsync kind for group sync.

Ref file : ldap-groupsync.yaml

## Create whitelist groups file:

Whitelist file is used to import specific groups users only

Ref file : whitelist.txt

```
% cat whitelist.txt
CN=CO_epgs,ou=CO,ou=epgs_application,dc=example,dc=com
```

## Create a blacklist groups file.

It is used to block the specific groups to import into openshift.

Ref file : blacklist.txt

```
% cat blacklist.txt
cn=Accounting Managers,ou=Groups,dc=example,dc=com
cn=HR Managers,ou=Groups,dc=example,dc=com
cn=QA Managers,ou=Groups,dc=example,dc=com
cn=PD Managers,ou=Groups,dc=example,dc=com
```

## Sync the LDAP groups

```
oc adm groups sync --blacklist=blacklist.txt --whitelist=whitelist.txt --sync-config=ldap-groupsync.yaml --confirm

group/CO_epgs
```

### Verify the imported groups

```
% oc get groups

NAME      USERS

CO_epgs   user2, user3, user4, user5, user6, user7, user8, user9, user10, user11, user12, user13, user14, user15, user16
```

### Verify the openshift users

```
% oc get users

NAME          UID                                   FULL NAME   IDENTITIES

admin         e48e8921-3b86-414c-8874-4634068a24e2              htpasswd:admin

opentlc-mgr   70d7b518-0d59-4e6d-a1de-088eb741c5b3              htpasswd_provider:opentlc-mgr

user10        c251d050-bfda-4560-84af-a2535f9cf9dd   user10      ldap:
dWlkPXVzZXIxMCxvdT16b25lMSxvdT1QZW9wbGUsZGM9ZXhhbXBsZSxkYz1jb20
```