mod08_ex01: Configuring Cloudera Manager for LDAP

The purpose of this exercise is to configure Cloudera Manager to use Plugable Authentication Modules (PAM) to connect to LDAP, to assign Cloudera Manager roles to LDAP users and groups, and to use Cloudera Manager's supergroup.

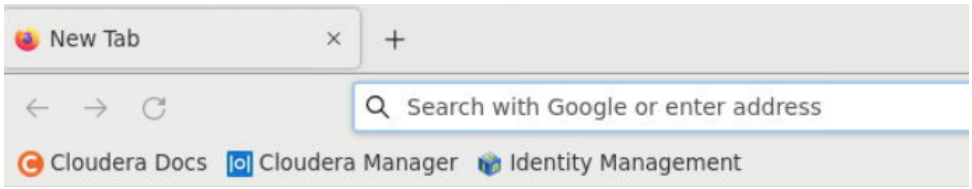
The LDAP database is a component of IPA. Cloudera Manager can use PAM to connect to LDAP for authentication. In this environment the PAM modules are configured when an IPA client is installed on to the host. You will configure Cloudera Manager to use PAM. After a restart of Cloudera Manager, you will be able to log in as the LDAP user allan_admin.

You will use Cloudera Manager roles to assign the user allan_admin full administrator privileges. From this point forward you will use allan_admin as the CDP administrator. One of the first tasks of the CDP administrator is to assign LDAP groups to various Cloudera Manager roles. When this task is done all of the users in LDAP will be able to log into Cloudera Manager, though each will have different privileges.

Cloudera Manager has a default group supergroup. Members of the group supergroup have superuser status for HDFS and YARN. During the build the group supergroup was added to LDAP. The administrative user, allan_admin, is assigned as a member of supergroup. The administrative user, allan_admin, is able to issue hdfs and yarn shell commands with superuser privileges. By creating the LDAP group supergroup you avoid configuring supergroup on each local host.

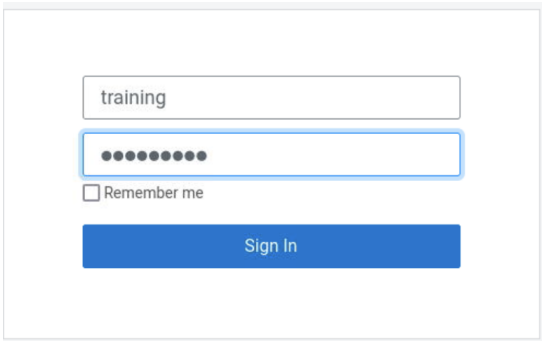
1. Login to Cloudera Manager as the local administrative user, training.

1.1 On the Firefox browser on the bookmark toolbar select Cloudera Manager.




```
http://cmhost.example.com:7180
```

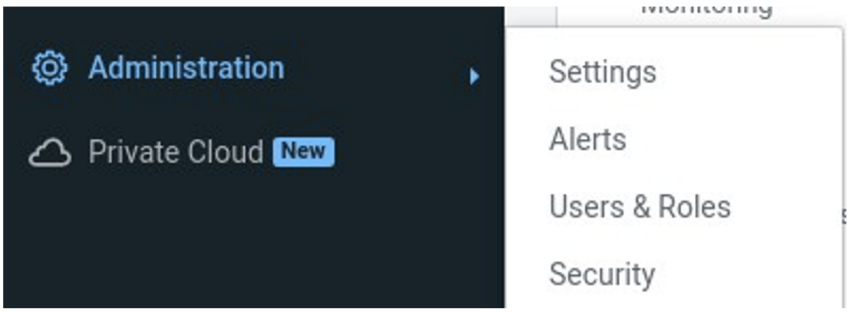
1.2 Log in to Cloudera Manager as the local administrative user, training, with password <password>.



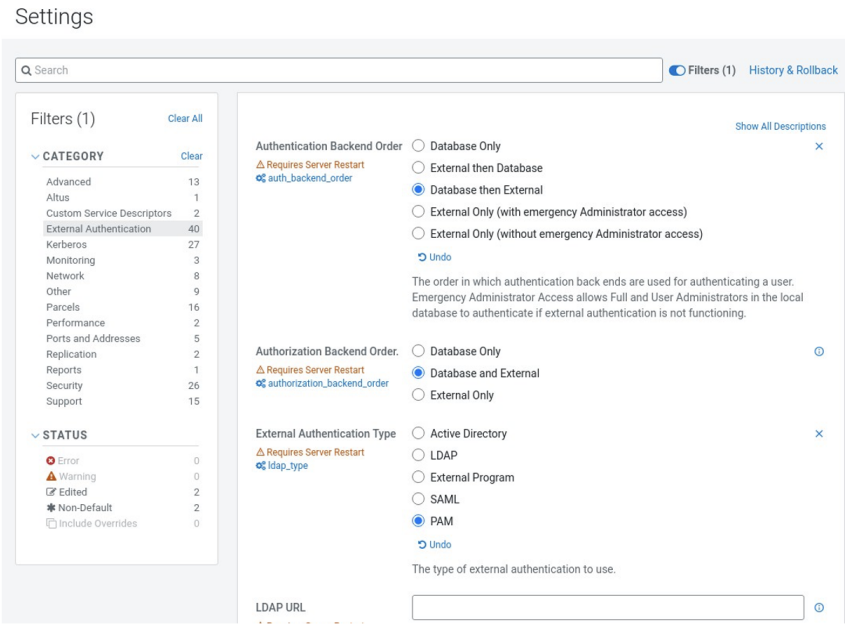
2. Configure Cloudera Manager to use LDAP.

Currently a LDAP user cannot log into Cloudera Manager. Configure Cloudera Manager to use PAM as the external source. PAM will allow authentication from the LDAP database. After restarting Cloudera Manager users from the LDAP database will be able to log in.

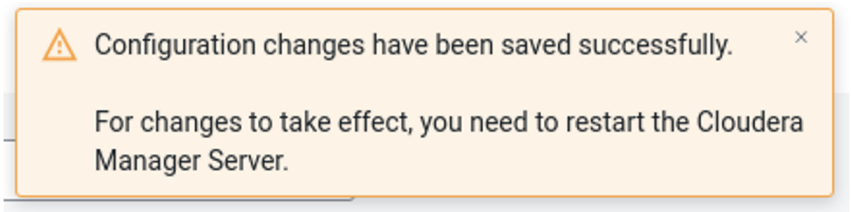
2.1 On Cloudera Manager Home select Administration > Settings.



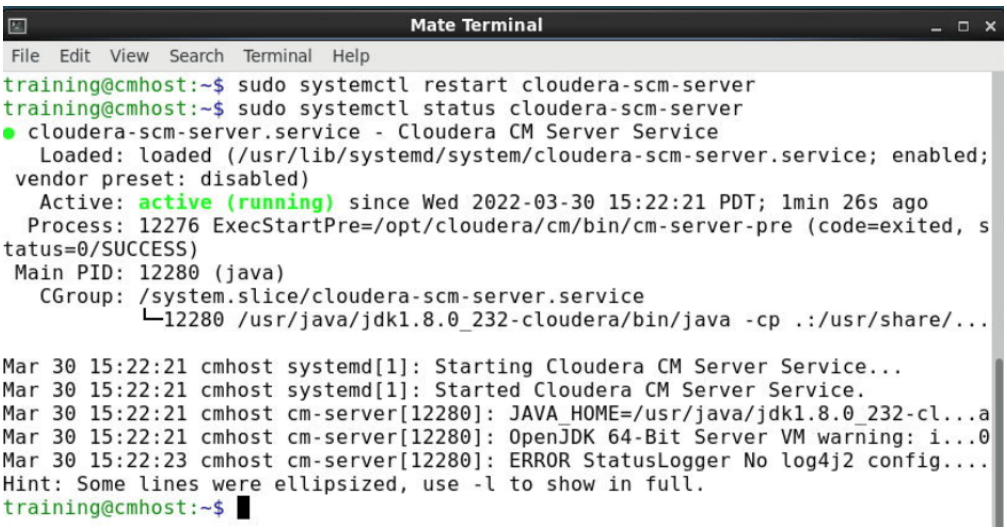
2.2 Search for External. For Authentication Backend Order select Database then External. This will first look for users in the Cloudera Manager database and then search for LDAP users. For External Authentication Type select PAM. This will use the Pluggable Authentication Modules. Click Save Changes.



2.3 An alert opens. You will need to restart the Cloudera Manager server. Click x Close.



2.4 Open a Mate terminal. Run the command to restart Cloudera Manager Server.




```
$ sudo systemctl restart cloudera-scm-server
$ sudo systemctl status cloudera-scm-server
```

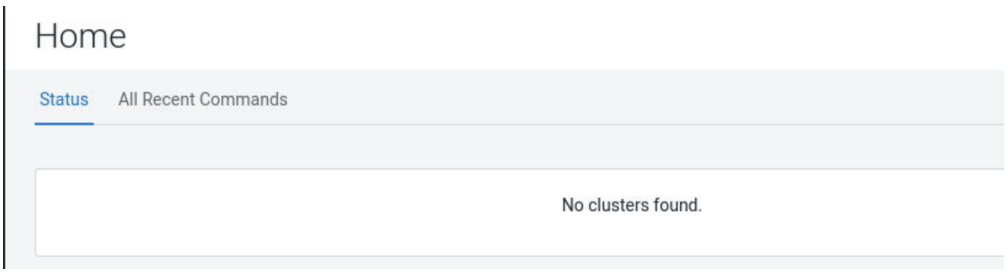
2.5 The restart cloudera-scm-server runs for up to 2 minutes. You can tail the Cloudera Manager log file. Watch for a message saying the WebServer has started.

```
$ sudo tail -f /var/log/cloudera-scm-server/cloudera-scm-server.log
```

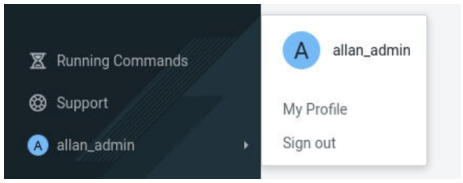
```
$ sudo tail -f /var/log/cloudera-scm-server/cloudera-scm-server.log
```

3. Assign a Cloudera Manager role to a single user.

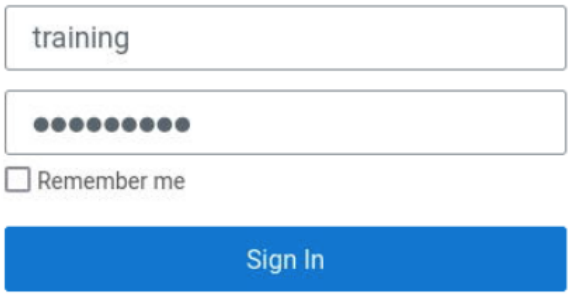
3.1 After the restart the Cloudera Manager log in screen will open. Log in as the administrative user, allan_admin, with password <password>. You will see a message “No clusters found”. This is because no roles for the administrative user, allan_admin, are assigned.



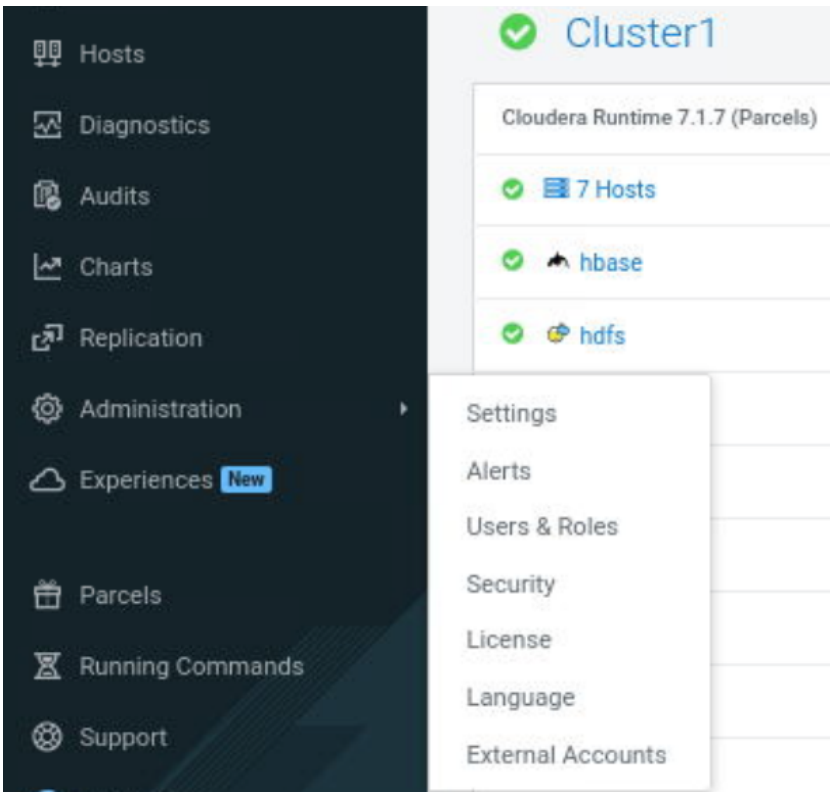
3.2 In the lower left corner sign select user allan_admin. Select Sign Out.



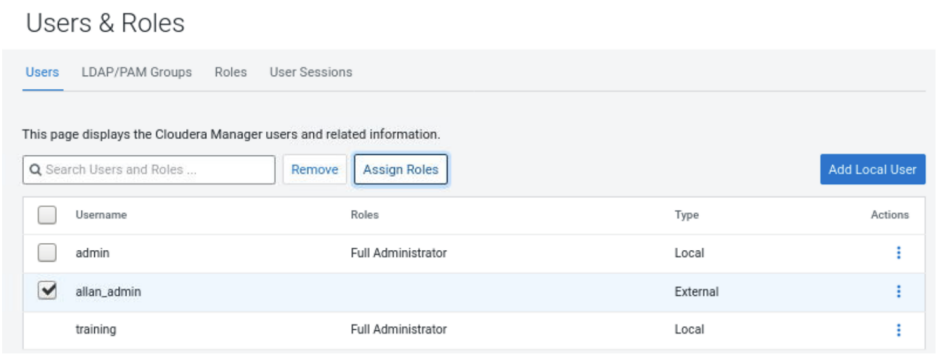
3.3 Log in to Cloudera Manager as the local administrative user, training, with password <password>.



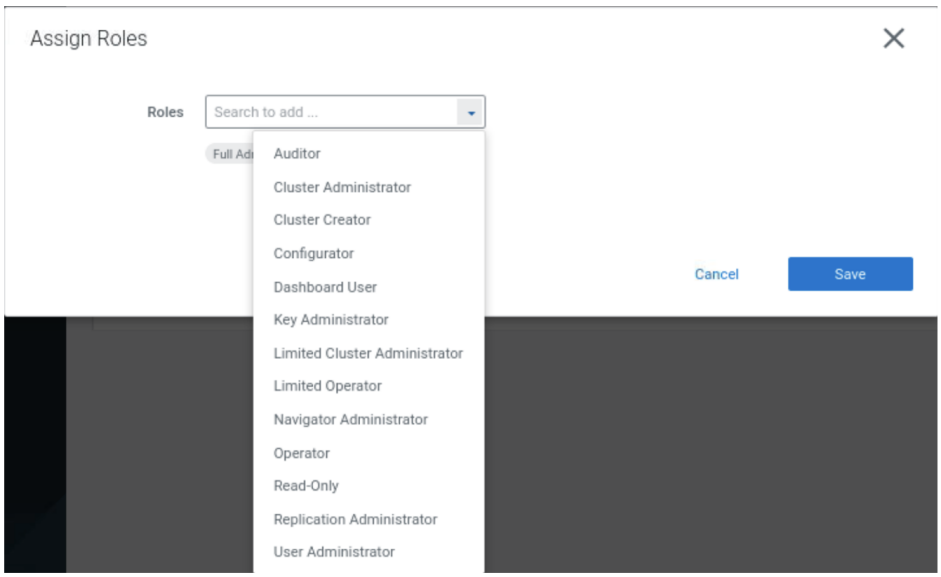
3.4 On Cloudera Manager Home select Administration -> Users & Roles.



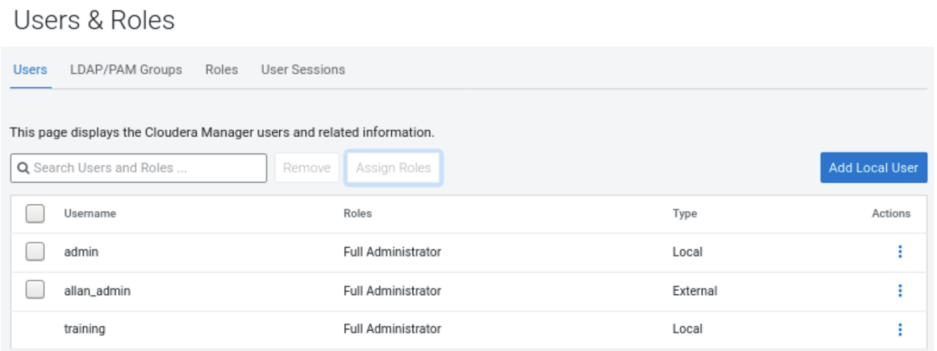
3.5 You can assign roles to individual users. Select allan_admin. Select Assign Roles.



3.6 Select the Roles pull down menu. There is a list of a number of different roles. Select Full Administrator. This will grant full administration privileges to the administrative user, allan_admin. Click Save.



3.7 Verify the administrative user, allan_admin, is an external user and is assigned full administrator privileges.



CDP Administrator recommend practice is to remove the user admin or at a minimum is to change the password. For educational purposes do not make changes to the user admin at this time.

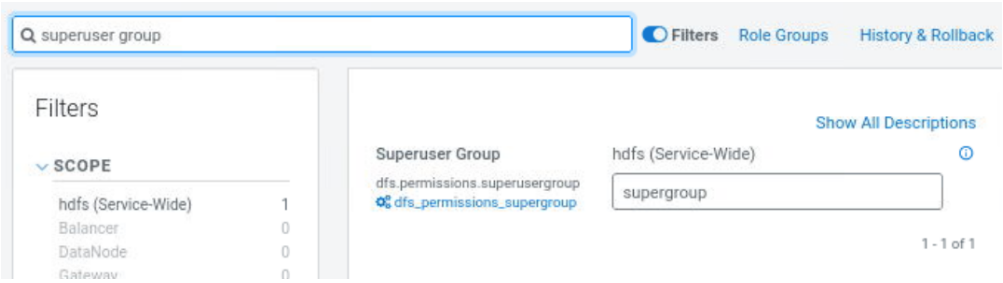
4. Assign administrative users to LDAP supergroup.

A common practice is to create the group supergroup in LDAP. The group supergroup grants superuser privileges to HDFS and to YARN. This practice avoids manually creating a local configuration /etc/group on every host. Be judicial in assigning only administrative users to supergroup.This exercise build has created the LDAP group supergroup.

Later you will assign administrative roles in Ranger and create policies to override supergroup.

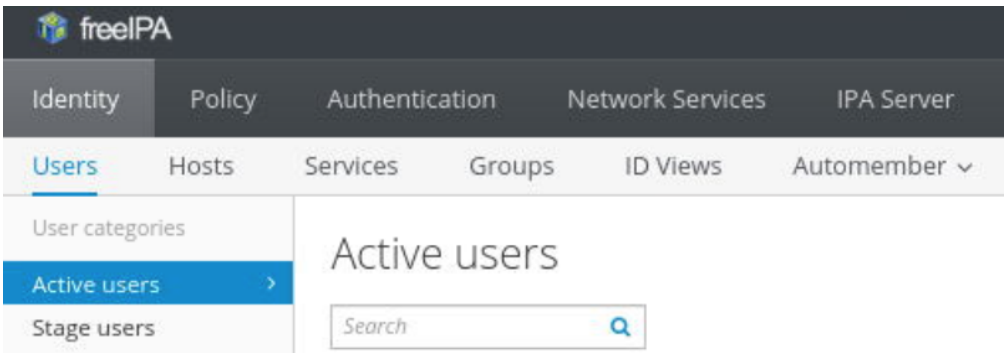
4.1 From Cloudera Manager Home select hdfs. Select Configuration.

4.2 Search for 'Superuser Group'. Validate the property value of dfs.permissions.superusergroup is supergroup.

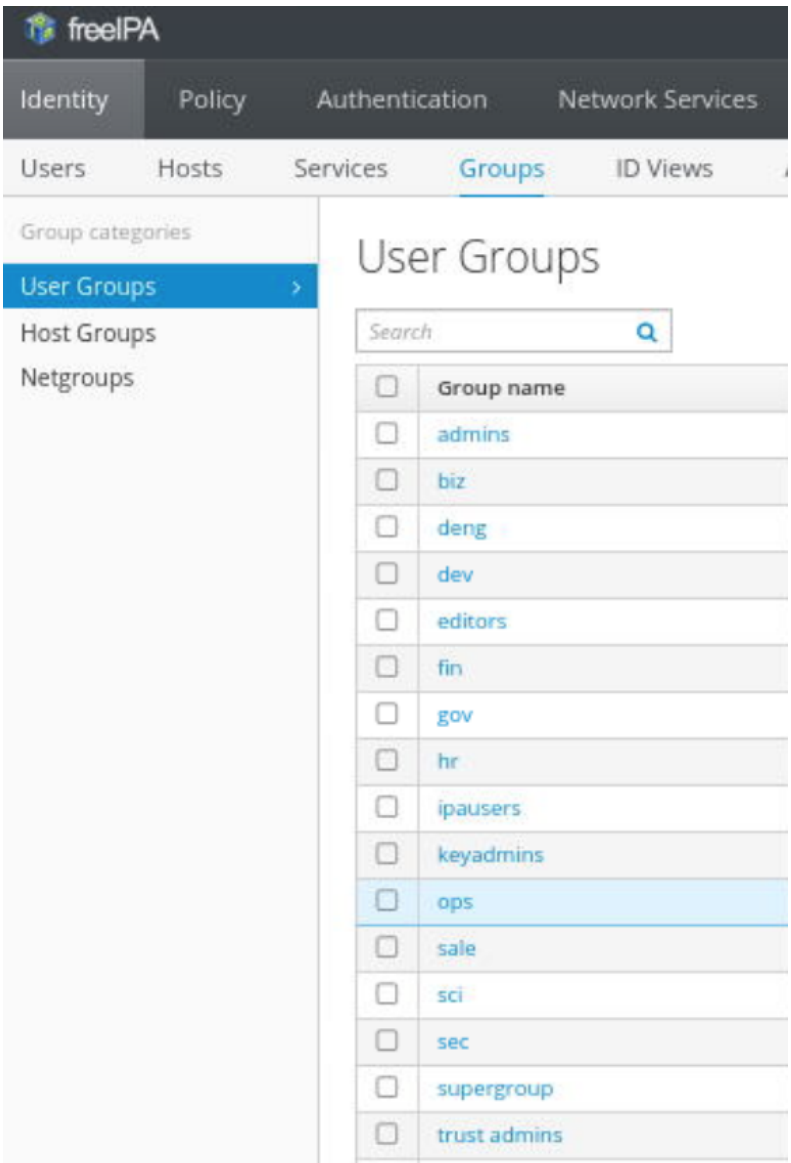


Common practice is to leave the group name as supergroup; however, the group name may be changed.

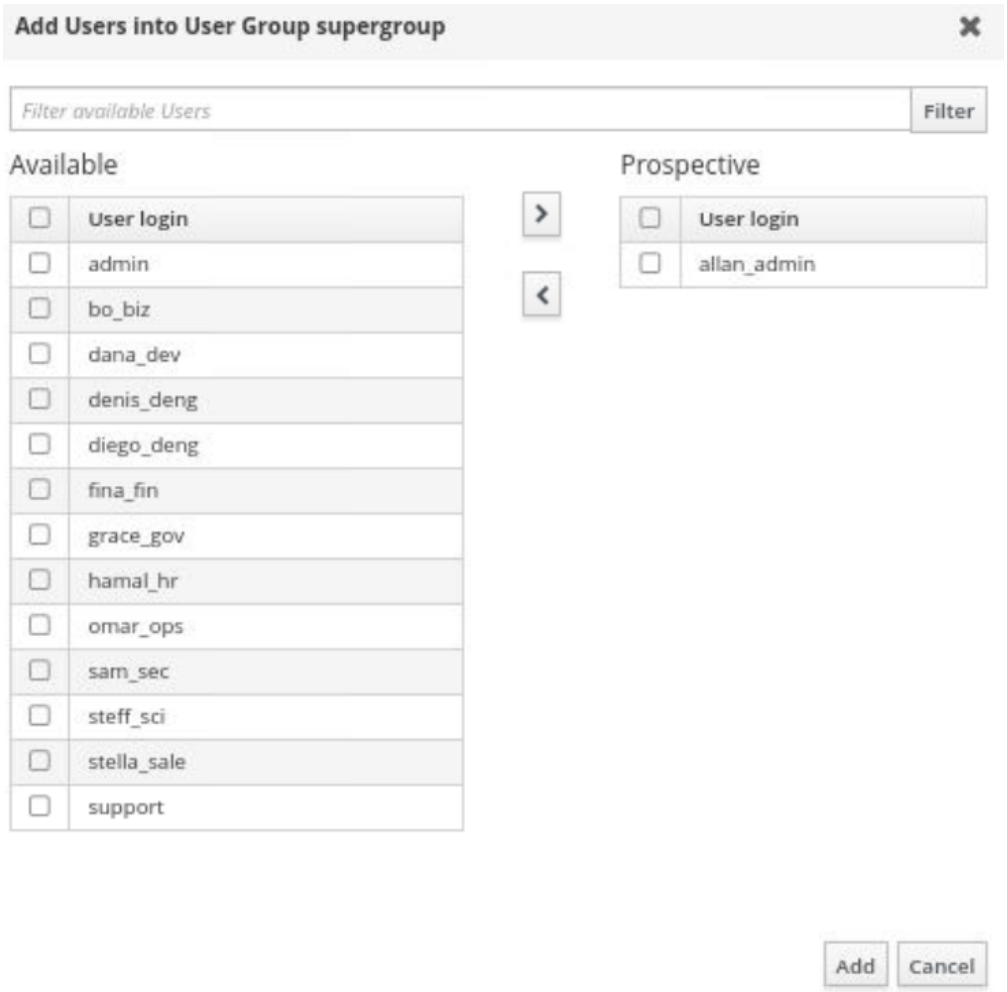
4.3 Return to IPA. If you need to login again use the security administrator, sam_sec, with password <password>.



4.4 Select Groups. From the list of groups select supergroup.



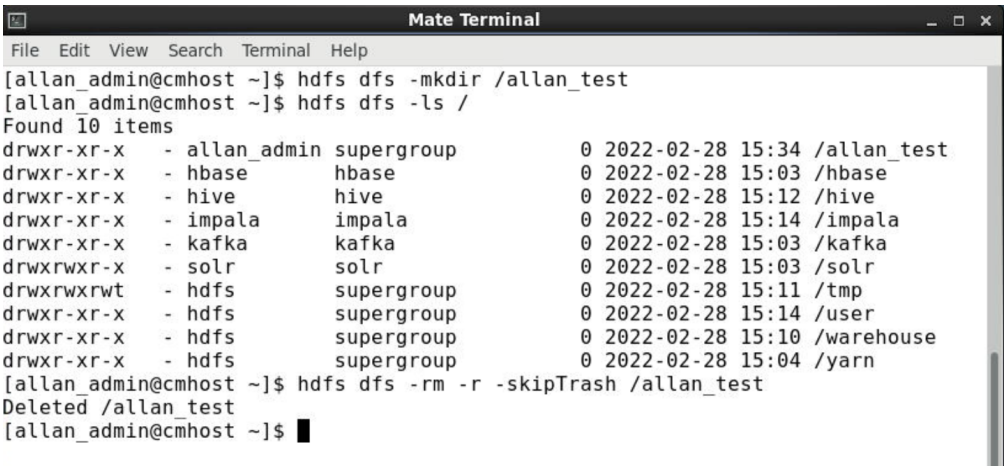
4.5 Select + Add. Select allan_admin. Select >. Click Add.



4.6 Open a Mate Terminal. Switch user to allan_admin with password <password>.

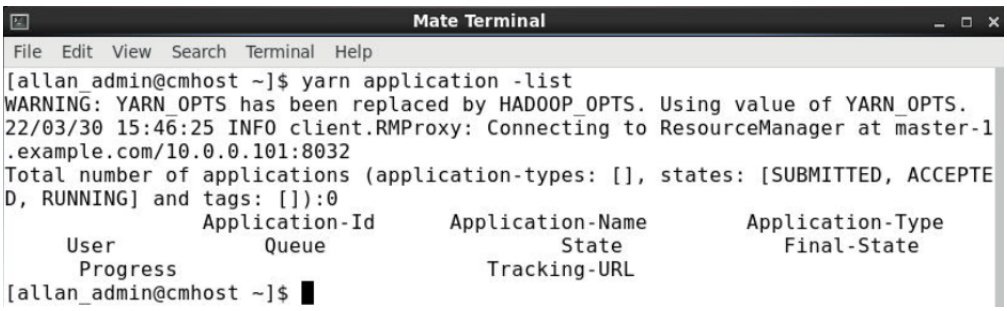

```
% su -l allan_admin
```

4.7 Run the hdfs dfs command to create a test directory at root /. Use the hdfs dfs command with the -skipTrash option to remove the test directory.




```
$ hdfs dfs –mkdir /allan_test
            $ hdfs dfs –ls /
            $ hdfs dfs –rm –r –skipTrash /allan_test
```

4.8 Members of the group admins will also have superuser privileges for YARN. Members will be able to delete any job in any YARN queue.

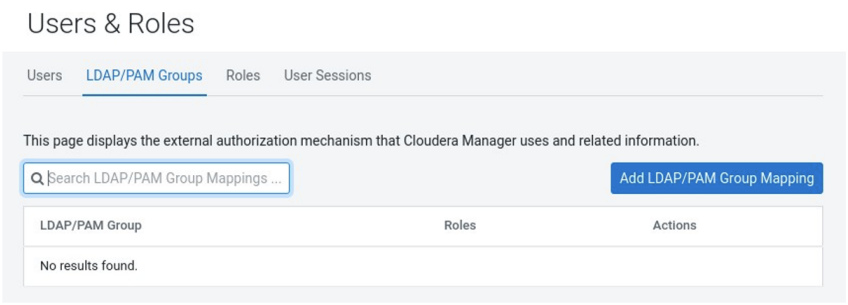



```
$ yarn application –list
```

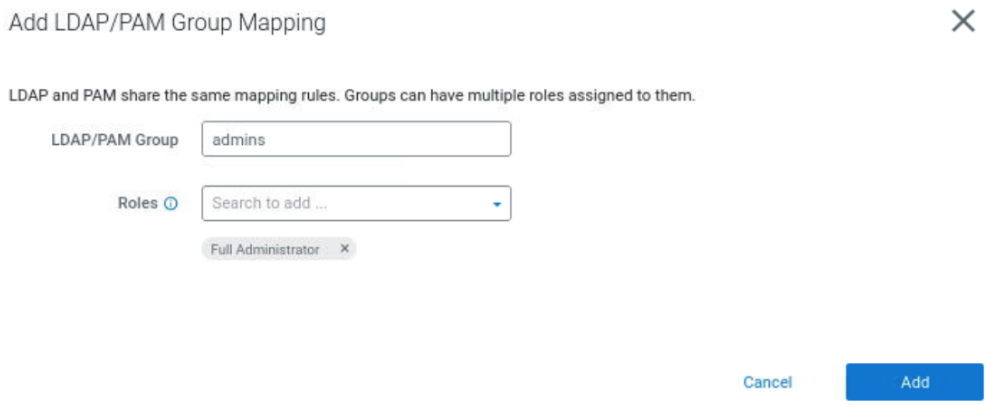
5. Assign Cloudera Manager roles using LDAP groups.

CDP Administrator recommended practice is to manage all users and groups from LDAP. Cloudera Manager includes a function to map LDAP groups to Cloudera Manager roles.
By mapping a LDAP group to a Cloudera Manager role you will grant the assigned privilege to every member of the group.

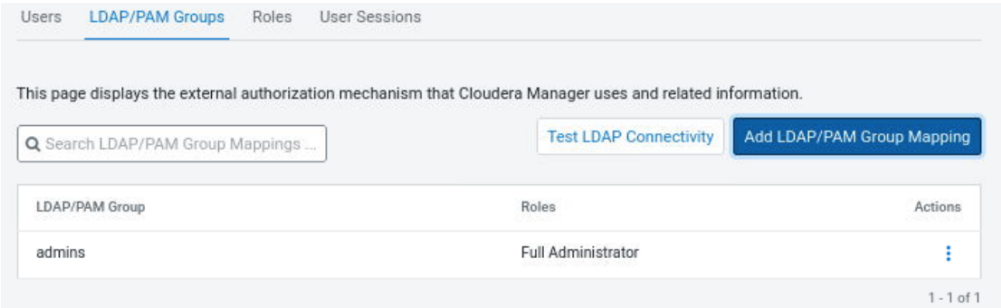
5.1 Select LDAP/PAM Groups. Select Add LDAP/PAM Group Mappings.



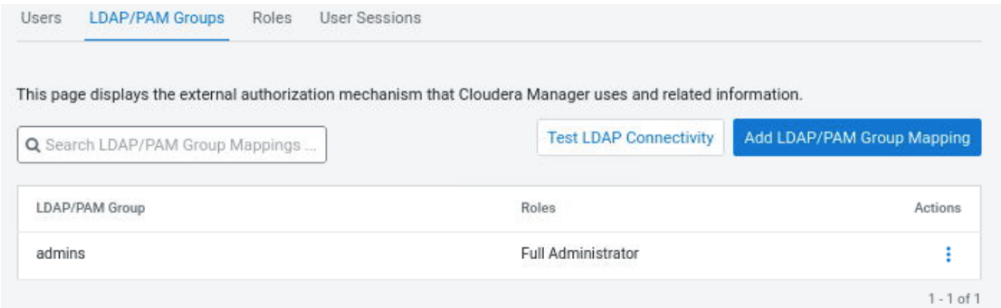
5.2 For LDAP/PAM Group enter admins. For Roles pull down and select Full Administrator. Click Add.



5.3 Verify the group admins is assigned the role Full Administrator.



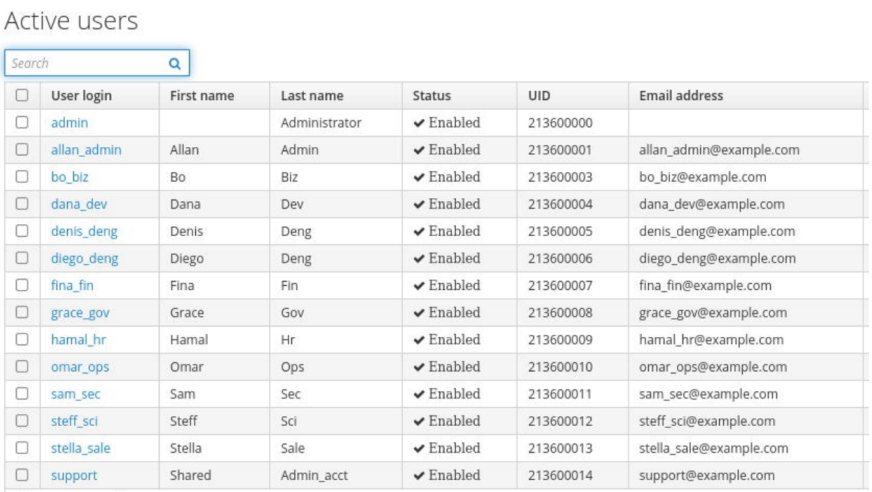
5.4 Select LDAP/PAM Group mappings to assign other LDAP groups to Cloudera Manager roles.



5.5 Use this table to map LDAP/PAM Groups to Cloudera Manager Roles.

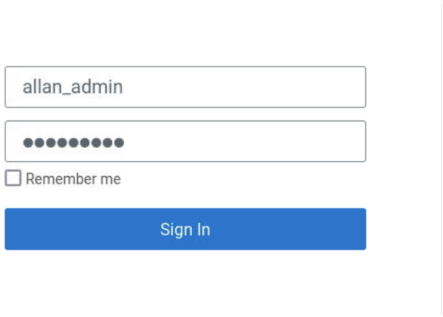
LDAP/PAM Group	Roles
admins	Full Administrator
biz	Dashboard User, Read-Only
deng	Limited Cluster Administrator
dev	Limited Operator
fin	Dashboard User, Read-Only
gov	Dashboard User, Auditor
hr	Dashboard User, Read-Only
ops	User Administrator, Operator, Replication Administrator
sale	Dashboard User, Read-Only
sci	Dashboard User, Read-Only
sec	Dashboard User, Read-Only

5.6 Sign out of Cloudera Manager. Review the list of users in IPA. Log in as various LDAP users. Compare the different levels of privileges.



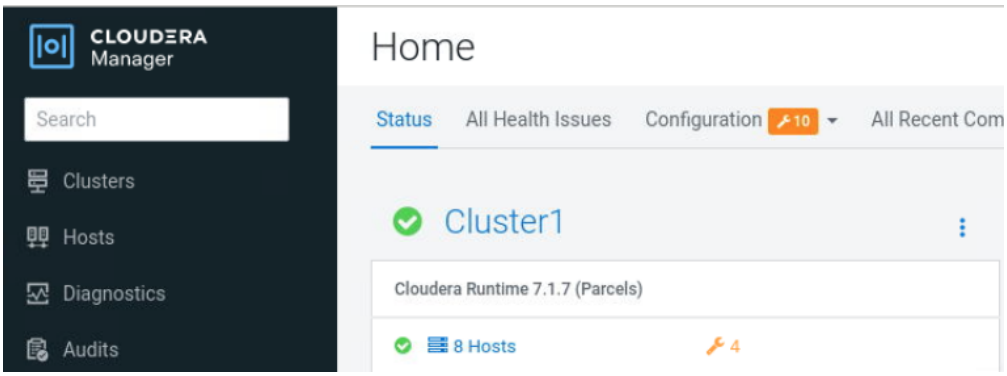
User login	First name	Last name	Status	UID	Email address
admin		Administrator	✔ Enabled	213600000	
allan_admin	Allan	Admin	✔ Enabled	213600001	allan_admin@example.com
bo_biz	Bo	Biz	✔ Enabled	213600003	bo_biz@example.com
dana_dev	Dana	Dev	✔ Enabled	213600004	dana_dev@example.com
denis_deng	Denis	Deng	✔ Enabled	213600005	denis_deng@example.com
diego_deng	Diego	Deng	✔ Enabled	213600006	diego_deng@example.com
fina_fin	Fina	Fin	✔ Enabled	213600007	fina_fin@example.com
grace_gov	Grace	Gov	✔ Enabled	213600008	grace_gov@example.com
hamal_hr	Hamal	Hr	✔ Enabled	213600009	hamal_hr@example.com
omar_ops	Omar	Ops	✔ Enabled	213600010	omar_ops@example.com
sam_sec	Sam	Sec	✔ Enabled	213600011	sam_sec@example.com
steff_sci	Steff	Sci	✔ Enabled	213600012	steff_sci@example.com
stella_sale	Stella	Sale	✔ Enabled	213600013	stella_sale@example.com
support	Shared	Admin_acct	✔ Enabled	213600014	support@example.com

5.7 Sign out of the previous user. Log in as the administrative user, allan_admin, with password <password>.

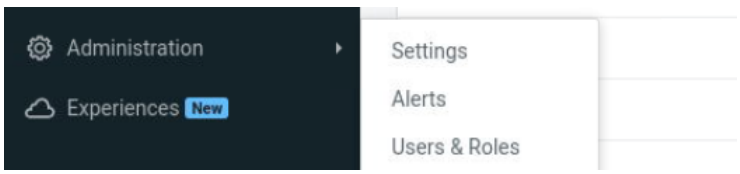


6. Extend session timeout. This for classroom purposes and is not a recommended practice.

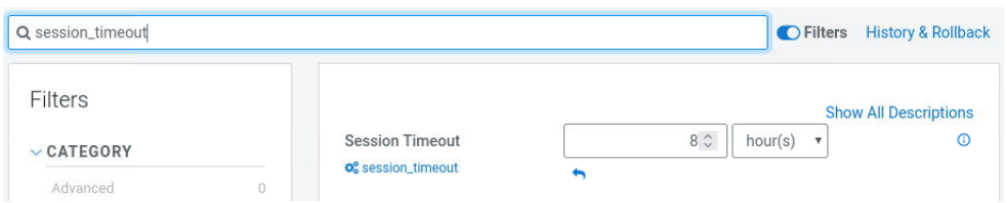
6.1 Return to Cloudera Manager Home.



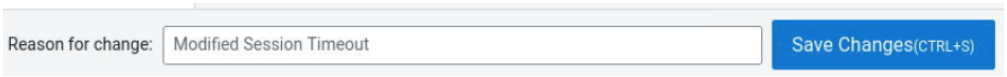
6.2 Select Administration. Select Settings.



6.3 Search for 'session_timeout'. Set it to 8 hours.



6.4 Click Save Changes.



7. Return to Cloudera Manager Home.