

mod08_ex01: Configuring Cloudera Manager for LDAP

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

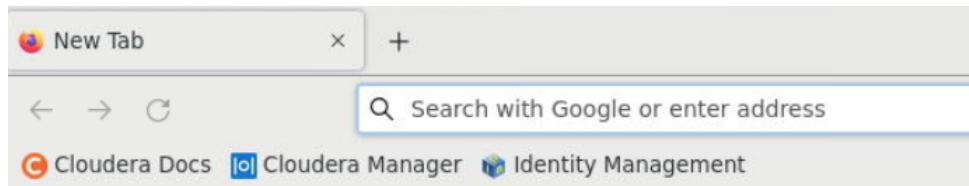
The LDAP database is a component of IPA. Cloudera Manager can use PAM to connect to LDAP for authentication. In this environment the PAM modules are configured when an IPA client is installed on to the host. You will configure Cloudera Manager to use PAM. After a restart of Cloudera Manager, you will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

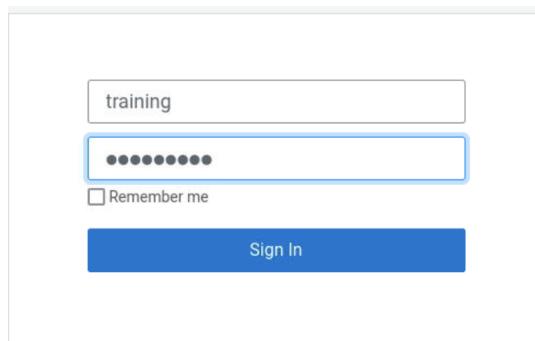
1. Login to Cloudera Manager as the local administrative user, training.

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



<http://cmhost.example.com:7180>

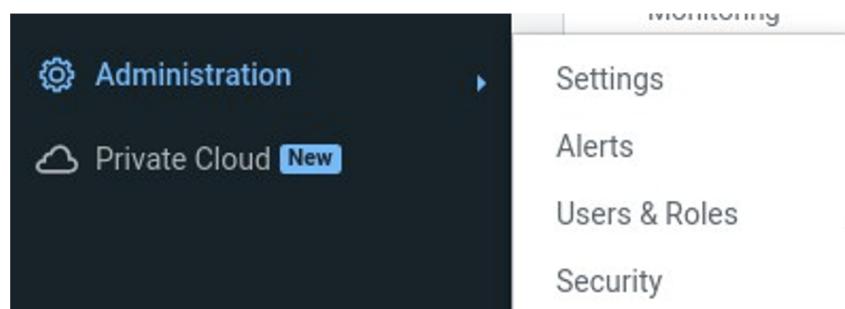
1.2 Log in to Cloudera Manager as the local administrative user, training, with password <password>.



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.

Settings

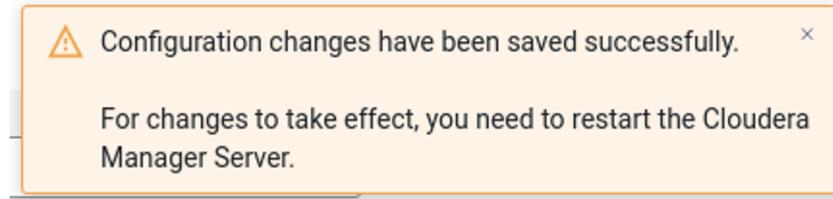
The screenshot shows the 'Settings' page with the following configuration:

- Authentication Backend Order:** Set to "Database then External". A note below states: "The order in which authentication back ends are used for authenticating a user. Emergency Administrator Access allows Full and User Administrators in the local database to authenticate if external authentication is not functioning."
- Authorization Backend Order:** Set to "Database and External".
- External Authentication Type:** Set to "PAM". A note below states: "The type of external authentication to use."
- LDAP URL:** An empty input field.

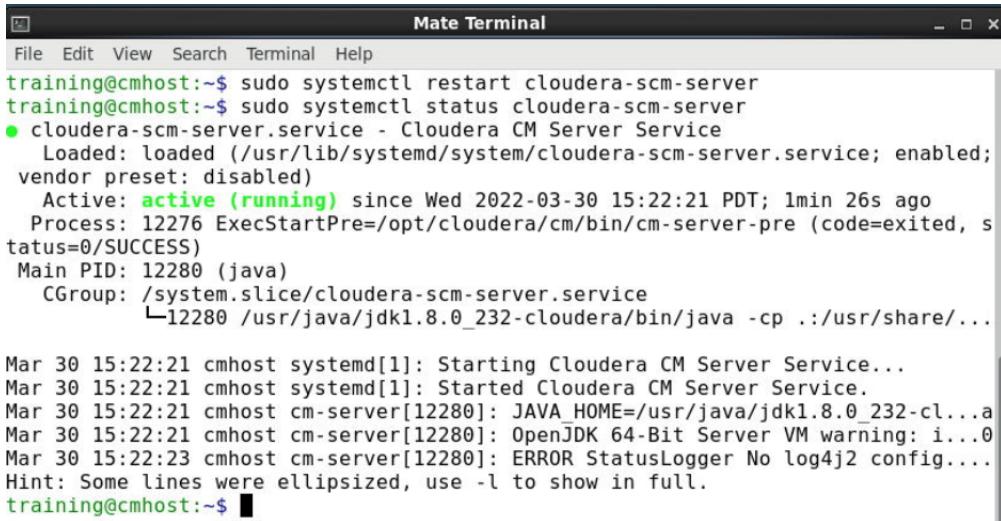
On the left, there is a sidebar with filters and status information:

- CATEGORY:**
 - Advanced: 13
 - Altus: 1
 - Custom Service Descriptors: 2
 - External Authentication: 40
 - Kerberos: 27
 - Monitoring: 3
 - Network: 8
 - Other: 9
 - Parcels: 16
 - Performance: 2
 - Ports and Addresses: 5
 - Replication: 2
 - Reports: 1
 - Security: 26
 - Support: 15
- STATUS:**
 - Error: 0
 - Warning: 0
 - Edited: 2
 - * Non-Default: 2
 - Include Overrides: 0

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.



```
Mate Terminal
File Edit View Search Terminal Help
training@cmhost:~$ sudo systemctl restart cloudera-scm-server
training@cmhost:~$ sudo systemctl status cloudera-scm-server
● cloudera-scm-server.service - Cloudera CM Server Service
  Loaded: loaded (/usr/lib/systemd/system/cloudera-scm-server.service; enabled;
  vendor preset: disabled)
  Active: active (running) since Wed 2022-03-30 15:22:21 PDT; 1min 26s ago
    Process: 12276 ExecStartPre=/opt/cloudera/cm/bin/cm-server-pre (code=exited, s
  status=0/SUCCESS)
   Main PID: 12280 (java)
      CGroup: /system.slice/cloudera-scm-server.service
              └─12280 /usr/java/jdk1.8.0_232-cloudera/bin/java -cp ./usr/share/...
Mar 30 15:22:21 cmhost systemd[1]: Starting Cloudera CM Server Service...
Mar 30 15:22:21 cmhost systemd[1]: Started Cloudera CM Server Service.
Mar 30 15:22:21 cmhost cm-server[12280]: JAVA_HOME=/usr/java/jdk1.8.0_232-cl...a
Mar 30 15:22:21 cmhost cm-server[12280]: OpenJDK 64-Bit Server VM warning: i...0
Mar 30 15:22:23 cmhost cm-server[12280]: ERROR StatusLogger No log4j2 config....
Hint: Some lines were ellipsized, use -l to show in full.
training@cmhost:~$
```

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

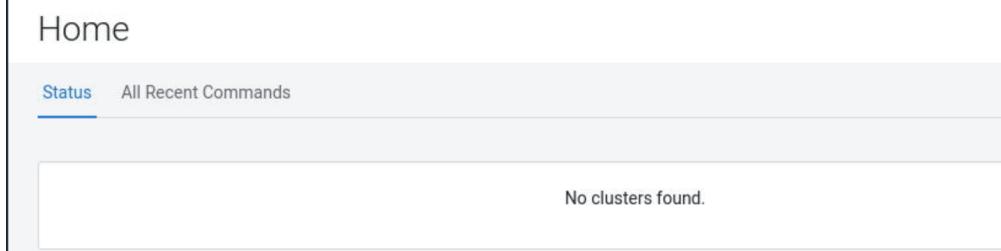
2.5 The restart cloudera-scm-server runs for up to 2 minutes. You can tail the Cloudera Manager log file. Watch for a message saying the WebServer has started.

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

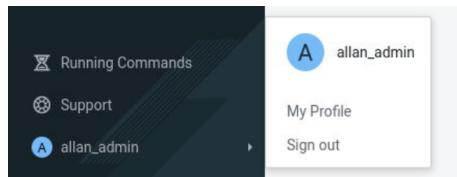
```
$ sudo tail -f /var/log/cloudera-scm-server/cloudera-scm-server.log
```

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>.

A screenshot of the Cloudera Manager login interface. It features a top search bar with the word 'training'. Below it is a password input field containing several black dots. Underneath the password field is a 'Remember me' checkbox followed by a 'Sign In' button.

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

A screenshot of the Cloudera Manager home screen. On the left is a dark sidebar with various icons and links: Hosts, Diagnostics, Audits, Charts, Replication, Administration (which is currently selected and has a dropdown arrow), Experiences (New), Parcels, Running Commands, and Support. To the right of the sidebar is a light-colored panel titled 'Cluster1' which shows cluster status: Cloudera Runtime 7.1.7 (Parcels) with 7 hosts, hbase, and hdfs services. A vertical dropdown menu is open under the 'Administration' link, listing: Settings, Alerts, Users & Roles (which is highlighted in blue), Security, License, Language, and External Accounts.

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

The screenshot shows the 'Users & Roles' page with the 'Users' tab selected. A search bar and 'Remove' button are at the top. Below is a table with columns: Username, Roles, Type, and Actions. Three users are listed: 'admin' (Local, Full Administrator), 'allan_admin' (External, checked, Full Administrator), and 'training' (Local, Full Administrator). An 'Assign Roles' button is highlighted in blue at the top right of the table area.

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.

The screenshot shows the 'Assign Roles' modal dialog. On the left, a 'Roles' dropdown menu is open, showing a list of roles: Auditor, Cluster Administrator, Cluster Creator, Configurator, Dashboard User, Key Administrator, Limited Cluster Administrator, Limited Operator, Navigator Administrator, Operator, Read-Only, Replication Administrator, and User Administrator. The 'Full Admin' role is selected. On the right, there are 'Cancel' and 'Save' buttons.

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

The screenshot shows the 'Users & Roles' page with the 'Users' tab selected. A search bar and 'Remove' button are at the top. Below is a table with columns: Username, Roles, Type, and Actions. Three users are listed: 'admin' (Local, Full Administrator), 'allan_admin' (External, checked, Full Administrator), and 'training' (Local, Full Administrator). An 'Assign Roles' button is highlighted in blue at the top right of the table area.

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 judicious 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.

The screenshot shows the search results for 'superuser group'. A single result is found: 'dfs.permissions.superusergroup' with the value 'supergroup'. The 'dfs' entry is highlighted in blue.

Property	Value
dfs.permissions.superusergroup	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>.

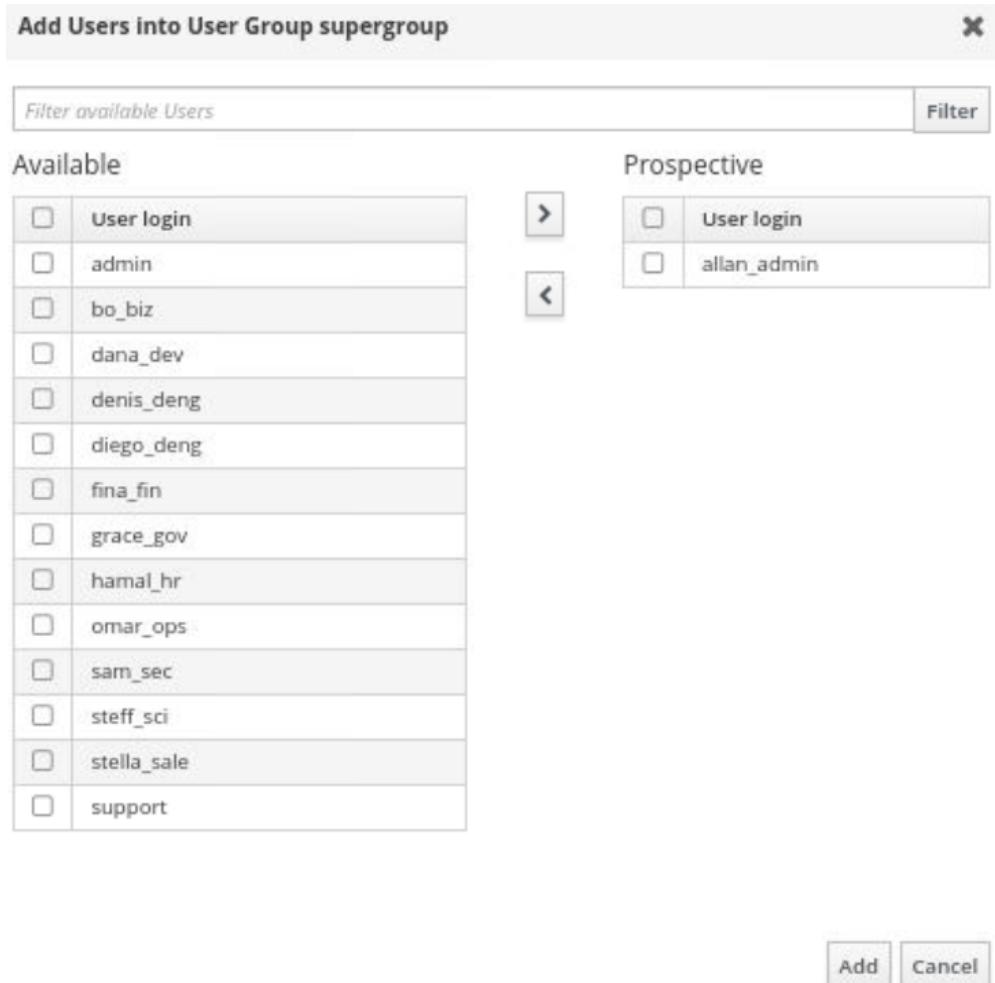
The screenshot shows the freeIPA interface under the 'Identity' tab. The 'Users' sub-tab is selected. On the left, 'User categories' are shown with 'Active users' and 'Stage users' options. The main area displays the 'Active users' list, which is currently empty. A search bar is at the bottom.

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

The screenshot shows the freeIPA web interface. The top navigation bar has tabs for Identity, Policy, Authentication, and Network Services. Below that is a secondary navigation bar with tabs for Users, Hosts, Services, Groups (which is underlined in blue), and ID Views. On the left, there's a sidebar titled "Group categories" with options for User Groups (selected and highlighted in blue), Host Groups, and Netgroups. The main content area is titled "User Groups" and contains a search bar with a magnifying glass icon. A table lists various groups, each with a checkbox next to it. The groups listed are: admins, biz, deng, dev, editors, fin, gov, hr, ipausers, keyadmins, ops (which is highlighted with a blue background), sale, sci, sec, supergroup, and trust admins.

<input type="checkbox"/>	Group name
<input type="checkbox"/>	admins
<input type="checkbox"/>	biz
<input type="checkbox"/>	deng
<input type="checkbox"/>	dev
<input type="checkbox"/>	editors
<input type="checkbox"/>	fin
<input type="checkbox"/>	gov
<input type="checkbox"/>	hr
<input type="checkbox"/>	ipausers
<input type="checkbox"/>	keyadmins
<input type="checkbox"/>	ops
<input type="checkbox"/>	sale
<input type="checkbox"/>	sci
<input type="checkbox"/>	sec
<input type="checkbox"/>	supergroup
<input type="checkbox"/>	trust admins

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

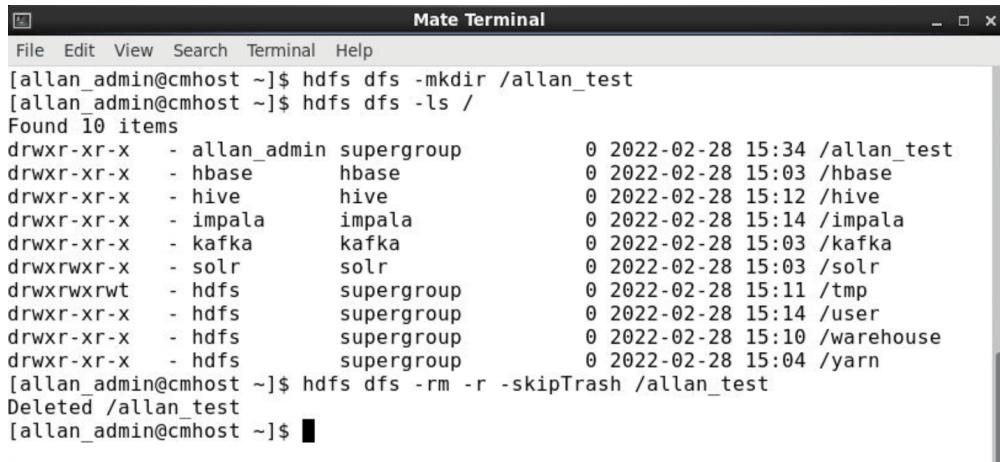


4.6 Open a Mate Terminal. Switch user to allan_admin with password <password>.

```
File Edit View Search Terminal Help
training@cmhost:~$ su -l allan_admin
Password:
Creating home directory for allan_admin.
[allan_admin@cmhost ~]$
```

```
% su -l allan_admin
```

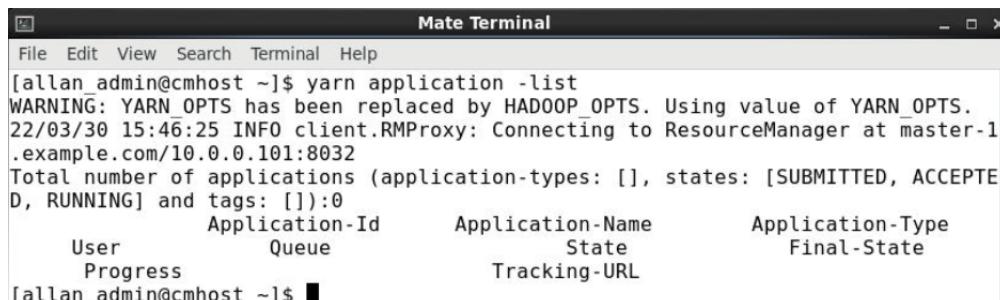
4.7 Run the hdfs dfs command to create a test directory at root /. Use the hdfs dfs command with the -skipTrash option to remove the test directory.



```
[allan_admin@cmhost ~]$ hdfs dfs -mkdir /allan_test
[allan_admin@cmhost ~]$ hdfs dfs -ls /
Found 10 items
drwxr-xr-x  - allan_admin supergroup      0 2022-02-28 15:34 /allan_test
drwxr-xr-x  - hbase      hbase            0 2022-02-28 15:03 /hbase
drwxr-xr-x  - hive       hive             0 2022-02-28 15:12 /hive
drwxr-xr-x  - impala     impala           0 2022-02-28 15:14 /impala
drwxr-xr-x  - kafka      kafka            0 2022-02-28 15:03 /kafka
drwxrwxr-x  - solr       solr             0 2022-02-28 15:03 /solr
drwxrwxrwt - hdfs      supergroup        0 2022-02-28 15:11 /tmp
drwxr-xr-x  - hdfs      supergroup        0 2022-02-28 15:14 /user
drwxr-xr-x  - hdfs      supergroup        0 2022-02-28 15:10 /warehouse
drwxr-xr-x  - hdfs      supergroup        0 2022-02-28 15:04 /yarn
[allan_admin@cmhost ~]$ hdfs dfs -rm -r -skipTrash /allan_test
Deleted /allan_test
[allan_admin@cmhost ~]$
```

```
$ 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.



```
[allan_admin@cmhost ~]$ yarn application -list
WARNING: YARN_OPTS has been replaced by HADOOP_OPTS. Using value of YARN_OPTS.
22/03/30 15:46:25 INFO client.RMProxy: Connecting to ResourceManager at master-1
.example.com/10.0.0.101:8032
Total number of applications (application-types: [], states: [SUBMITTED, ACCEPTED, RUNNING] and tags: []):0
          Application-Id      Application-Name      Application-Type
          User          Queue          State          Final-State
          Progress          Tracking-URL
[allan_admin@cmhost ~]$
```

```
$ 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.

Users & Roles

Users **LDAP/PAM Groups** Roles User Sessions

This page displays the external authorization mechanism that Cloudera Manager uses and related information.

Search LDAP/PAM Group Mappings ... **Add LDAP/PAM Group Mapping**

LDAP/PAM Group	Roles	Actions
No results found.		

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

Add LDAP/PAM Group Mapping X

LDAP and PAM share the same mapping rules. Groups can have multiple roles assigned to them.

LDAP/PAM Group	admins
Roles <small>(i)</small>	<input type="text"/> Search to add ...
<input type="text"/> Full Administrator X	

Cancel **Add**

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

Users **LDAP/PAM Groups** Roles User Sessions

This page displays the external authorization mechanism that Cloudera Manager uses and related information.

Search LDAP/PAM Group Mappings ... **Test LDAP Connectivity** **Add LDAP/PAM Group Mapping**

LDAP/PAM Group	Roles	Actions
admins	Full Administrator	⋮

1 - 1 of 1

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

Users **LDAP/PAM Groups** Roles User Sessions

This page displays the external authorization mechanism that Cloudera Manager uses and related information.

Search LDAP/PAM Group Mappings ... **Test LDAP Connectivity** **Add LDAP/PAM Group Mapping**

LDAP/PAM Group	Roles	Actions
admins	Full Administrator	⋮

1 - 1 of 1

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.

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

The screenshot shows a sign-in form with the following fields:
 - Username: allan_admin
 - Password: (redacted)
 - Remember me:
 - Sign In: A blue button at the bottom.

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

6.1 Return to Cloudera Manager Home.

The screenshot shows the Cloudera Manager Home page with the following elements:
 - Sidebar: Clusters, Hosts, Diagnostics, Audits.
 - Main Panel: Cluster1 (green checkmark), Cloudera Runtime 7.1.7 (Parcels), 8 Hosts (green checkmark), 4 alerts (orange exclamation marks).

6.2 Select Administration. Select Settings.

The screenshot shows the Administration menu with the following options:
 - Administration (selected)
 - Experiences (New)

A dropdown menu is open over 'Administration' showing:
 - Settings (selected)
 - Alerts
 - Users & Roles

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

The screenshot shows the search results for 'session_timeout' with the following details:
 - Search bar: session_timeout
 - Filters: CATEGORY (Advanced, 0), Session Timeout (session_timeout)
 - Value: 8 hour(s)

6.4 Click Save Changes.

The screenshot shows a save dialog with the following fields:
 - Reason for change: Modified Session Timeout
 - Save Changes(CTRL+S) button

7. Return to Cloudera Manager Home.