

## 1.1 Active Directory Integration

For the filtering, the following groups are being used (substitute <AD\_GROUP\_NAME> where required in the configuration below:

```
CN=DL-EMEA-GROUP,OU=zGroups,DC=emea,DC=paris,DC=corp
```

```
CN= DL-EMEA-GROUP,OU=zGroups,DC=emea,DC=paris,DC=corp
```

### 1.1.1 Ambari

#### 1.1.1.1 *Configure LDAP for Ambari*

Run `ambari-server setup-ldap` as root and insert the configuration parameters as below:

```
$ sudo ambari-server setup-ldap
Using python /usr/bin/python2.6
Setting up LDAP properties...
Primary URL* {host:port} : <domain controller>:389
Secondary URL {host:port} : <domain controller>:389
Use SSL* [true/false] (false):
User object class* (posixAccount): organizationalPerson
User name attribute* (uid): sAMAccountName
Group object class* (posixGroup): group
Group name attribute* (cn):
Group member attribute* (memberUid): member
Distinguished name attribute* (dn): distinguishedName
Base DN* : DC=emea,DC=paris,DC=corp
Referral method [follow/ignore] : ignore
Bind anonymously* [true/false] (false):
Manager DN* : CN=xxxxxxx,OU=xxxxx,OU=xxxxx,DC=xxxx,DC=xxxx,DC=xxxx
Enter Manager Password* : <input hidden>
Re-enter password: <input hidden>
=====
Review Settings
=====
authentication.ldap.managerDn: CN=xxxxx,OU=xxxxx,OU=xxxx,DC=xxxx,DC=xxxx,DC=xxx
authentication.ldap.managerPassword: *****
Save settings [y/n] (y)? y
Saving...done
Ambari Server 'setup-ldap' completed successfully.
```

#### 1.1.1.2 *Restart Ambari*

```
$ sudo ambari-server restart
Using python /usr/bin/python2.6
Restarting ambari-server
Using python /usr/bin/python2.6
Stopping ambari-server
Ambari Server stopped
Using python /usr/bin/python2.6
Starting ambari-server
Ambari Server running with administrator privileges.
Organizing resource files at /var/lib/ambari-server/resources...
Server PID at: /var/run/ambari-server/ambari-server.pid
Server out at: /var/log/ambari-server/ambari-server.out
Server log at: /var/log/ambari-server/ambari-server.log
Waiting for server start.....
```

Ambari Server 'start' completed successfully.

### 1.1.1.3 Sync the required users from AD

Create a file with the user names to be imported, separated by comma.

Import the users by running the below command as root:

```
$ sudo ambari-server sync-ldap --users <USERLIST>
Using python /usr/bin/python2.6
Syncing with LDAP...
Enter Ambari Admin login: admin
Enter Ambari Admin password:
Syncing specified users and groups..
```

Completed LDAP Sync.

```
Summary:
memberships:
removed = 0
created = 0
users:
updated = 0
removed = 0
created = 3
groups:
updated = 0
removed = 0
created = 0
```

Ambari Server 'sync-ldap' completed successfully.

The users will be now available in Ambari as regular users; they may log in using their AD password.

## 1.1.2 Ranger

### 1.1.2.1 Configure Ranger User Sync in Ambari

Expand the **Advanced usersync-properties** and set the properties as below:

```
MIN_UNIX_USER_ID_TO_SYNC = 0
SYNC_INTERVAL = 120
SYNC_SOURCE = ldap
SYNC_LDAP_BIND_DN =
CN=yyyyyyy,OU=yyyyyy,OU=yyyyyyy,DC=yyyy,DC=yyyy,DC=yyyy
SYNC_LDAP_BIND_PASSWORD = yyyyyyyyy
SYNC_LDAP_GROUPNAME_CASE_CONVERSION = lower
SYNC_LDAP_URL = ldap://<domain controller>:389
SYNC_LDAP_USERNAME_CASE_CONVERSION = lower
SYNC_LDAP_USER_GROUP_NAME_ATTRIBUTE = memberOf
SYNC_LDAP_USER_NAME_ATTRIBUTE = sAMAccountName
SYNC_LDAP_USER_OBJECT_CLASS = organizationalPerson
SYNC_LDAP_USER_SEARCH_BASE = DC=emea,DC=paris,DC=corp
SYNC_LDAP_USER_SEARCH_FILTER =
(|(memberOf=<AD_GROUP_NAME>,OU=zGroups,DC=emea,DC=paris,DC=corp)(memberOf
=CN=<AD_GROUP_NAME>,OU=zGroups,DC=emea,DC=paris,DC=corp))
SYNC_LDAP_USER_SEARCH_SCOPE = sub
SYNC_SOURCE = ldap
```

### 1.1.2.2 Promote users to Admin

Before switching to AD Authentication, some AD users should be granted Admin permissions.

This step is required, as after switching to AD Authentication, the internal admin user will not be able to access anymore.

Log in to the Ranger UI as an Admin user and find a user who is supposed to have Admin privileges between the AD users which have just been synced:

y1009838		User	External	<a href="#">cegsec_deny_sa_ts_logon</a> <a href="#">cegorg_external_users_ez</a> <a href="#">eudl_life_uk_consumption_prod</a>
w998712		User	External	<a href="#">cegsec_isp_zurich_eu_palantir_dsb</a> <a href="#">cegsec_isp_gc_europe_datalake_infa_sit_admin</a> <a href="#">cegorg_external_users_ez</a> <a href="#">cegsec_isp_csc_europe_palantir_hadoop_admin</a> <a href="#">+ More..</a>
w1001816		User	External	<a href="#">cegsec_isp_zurich_eu_palantir_dsb</a> <a href="#">cegorg_external_users_ez</a> <a href="#">cegsec_isp_csc_europe_palantir_hadoop_admin</a> <a href="#">cegsec_isp_gc_europe_datalake_sit_admin</a> <a href="#">+ More..</a>
w1008774		User	External	<a href="#">eudl_gi_gc_pal_dev_developers</a> <a href="#">cegorg_external_users_ez</a> <a href="#">cegsec_isp_gc_europe_datalake_sit_admin</a> <a href="#">cegsec_isp_zurich_eu_gc_lake_dev_admin</a> <a href="#">+ More..</a>
w1009962		User	External	<a href="#">cegorg_external_users_ez</a> <a href="#">cegsec_isp_gc_europe_datalake_sit_admin</a> <a href="#">cegsec_isp_zurich_eu_gc_lake_dev_admin</a> <a href="#">eudl_prod_hadoop_admins</a>
w1002988		User	External	<a href="#">cegsec_prod_usersslvpn</a> <a href="#">eudl_life_uk_sfdc_prod_app_support</a> <a href="#">cegorg_external_users_ez</a> <a href="#">cegsec_isp_zurich_eu_ukl_lake_dev_admin</a> <a href="#">+ More..</a>
w1003000		User	External	<a href="#">eudl_life_uk_sfdc_prod_app_support</a> <a href="#">cegorg_external_users_ez</a> <a href="#">cegsec_isp_zurich_eu_ukl_lake_dev_admin</a> <a href="#">cegsec_isp_csc_europe_palantir_hadoop_admin</a> <a href="#">+ More..</a>

Promote the user to Admin by using the “Select Role” dropdown box, then click “save”:

Users/Groups > User Edit

### User Detail

User Name \*

First Name

Last Name

Email Address

Select Role \*

Group

Verify that at least one admin user from AD is able to log in before proceeding to the Authentication method switch.

### 1.1.2.3 Add a service user for Ambari to log in to Ranger

In Ranger, create an “ambari” user with a secure password and Admin status.

In Ambari, open the Ranger configuration properties and specify the details for the newly created user:

Advanced ranger-env

Ranger User	<input type="text" value="ranger"/>	🔒	↻
Ranger Group	<input type="text" value="ranger"/>	🔒	↻
admin_username	<input type="text" value="ambari"/>	🔒	➕ 🔁 ↻
admin_password	<input type="password" value="....."/> <input type="password" value="....."/>	🔒	🔁
xml_configurations_supported	<input type="text" value="false"/>	🔒	➕ ↻
ranger_usersync_log_dir	<input type="text" value="/var/log/hadooplogs/ranger/usersync"/>	🔒	➕ ↻
ranger_pid_dir	<input type="text" value="/var/run/ranger"/>	🔒	➕ ↻
ranger_admin_username	<input type="text" value="amb_ranger_admin"/>	🔒	➕ ↻
ranger_admin_log_dir	<input type="text" value="/var/log/hadooplogs/ranger/admin"/>	🔒	➕ ↻
oracle_home	<input type="text" value="-"/>	🔒	➕ ↻

#### 1.1.2.4 Switch to AD Authentication for the Ranger UI

In Ambari, open the Ranger configuration page, and change the settings as below:

Ranger Settings

Authentication method

- LDAP
- ACTIVE\_DIRECTORY
- UNIX
- NONE

External URL

HTTP enabled  ↻

---

AD Settings

xa\_ldap\_ad\_domain  ↻

xa\_ldap\_ad\_url  ↻

Restart Ranger.