

# Configure LDAP Cache Service

This Step by Step guide is intended to demonstrate a basic configuration using Aspire, the LDAP Cache Service, and an LDAP server using a simple authentication method.

## Step-by-step guide

Follow these steps

1. Start Aspire version 4.0 using either the Elasticsearch or MongoDB as NoSQL providers.
2. Verify connection with the LDAP server either using JXplorer or Softerra LDAP Browser applications.

10.89.26.99:1389 Properties

Displayed Attributes | Paging Policy | Group Membership

Profile | Credentials | LDAP Settings | Entry

10.89.26.99:1389

Host: 10.89.26.99 : 1389

Lookup Servers...

Base DN: dc=example,dc=com ...

Fetch Base DNs

Type: OpenDJ Community Edition 2.6.4

URL: ldap://10.89.26.99:1389/dc=example,dc=com


☐ Use secure connection (SSL)

OK Cancel Apply Help




10.89.26.99:1389 Properties ? X


Displayed Attributes    Paging Policy    Group Membership

Profile    Credentials    **LDAP Settings**    Entry

 Bind using one of the following authentication options.

☐ Anonymous user  
☐ Currently logged on user (Active Directory only)  
☐ External (SSL Certificate)  
☒ Other credentials

Mechanism: Simple   
 Principal: cn=Directory Manager   
 Password:   
☒ Save password 

 [Select Credentials](#)

☒ Try matching the credentials required for referral rebind.

OK Cancel Apply Help

3. Add the Group Expansion Manager Service on Aspire (Service Manager page)

**ASPIRE** **Service Configuration**

Service Manager

Done Save

General Workflow

Service

General

Service name: groupExpansion

Expansion Timeout: 30

Additional groups

☒ Add PUBLICALL group

☐ Select Group

Domain handling

Request domain: Leave alone

Response domain: Leave alone

LDAP Proxy

Configure LDAP Proxy

Advanced Service Properties

Advanced Configuration

4. Save default configurations for the GEM.
5. Once verified, add the LDAP Cache service on Aspire (Service Manager page)

**ASPIRE** Service Configuration

LDAP Groups

Group Expansion Manager: None

Run scripts: [icon]

Server

Server url: ldap://10.89.12.104:389

Authentication: Simple

Connection timeout: 30s

Read timeout: 30s

Use Single Search Base: [checked]

Search base: dc=example,dc=com

Scope: Subtree

User query: (&(|objectClass=ldapCategoryPerson))

Group query: (&(|ldapCategoryGroup))

Cache user attributes: [checked]

Cache group attributes: [checked]

Group membership attributes

User key: dn

User name: uidAccountName

Group key: dn

Group name: uidAccountName

Group mapping: memberOf

☐ Groups hold members

6. Configure the service using at least the following fields.
  - a. Group Expansion Manager (previously configured)
  - b. Server URL. Example: ldap://<IP\_ADDRESS>:<PORT>
  - c. Authentication: Simple
  - d. LDAP Server username. Example: cn=Directory Manager
  - e. LDAP Server password
  - f. Check the Use Single Search Base field.
  - g. Specify the node in the directory to begin the searches. Example: dc=example,dc=com
  - h. Additional fields: User Query and Group Query. These fields required to be set up according to LDAP's configurations. Use the JXplorer or Softerra LDAP Browser to navigate through User and Groups attributes.
7. The Group Membership Attributes section might be configured as well depending on LDAP's group attributes. Use the JXplorer or Softerra LDAP Browser to navigate through User and Groups attributes. Check the following User and Groups from the LDAP server being used as an example:

**ou=People**

- uid=abarnes
- uid=abergin**
- uid=achassin
- uid=ahall
- uid=ahel
- uid=ahunter
- uid=ajensen
- uid=aknutson
- uid=alangdon
- uid=alutz
- uid=ashelton
- uid=awalker
- uid=awhite
- uid=aworrell
- uid=bfrancis
- uid=bfree
- uid=bhal2
- uid=bhall
- uid=bjablons
- uid=bjense2
- uid=bjensen
- uid=bmaddock

Name	Value
objectClass	top
objectClass	inetOrgPerson
objectClass	posixAccount
objectClass	organizationalPerson
objectClass	person
mail	abergin@example.com
roomNumber	3472
ou	Product Testing
ou	People
givenName	Andy
telephoneNumber	+1 408 555 8585
sn	Bergin
cn	Andy Bergin
homeDirectory	/home/abergin
facsimileTelephoneNumber	+1 408 555 7472
gidNumber	1000
userPassword	{SSHA}mC8Ldoek9KpNYKdaenV1VCFz03eToNH5GrWAfg==
uidNumber	1005
uid	abergin
l	Cupertino

**Softerra LDAP Browser**

- Internet Public Servers
- 10.89.12.104
- 10.89.26.99:1389
- ou=Company Servers
- ou=Groups**
  - cn=Accounting Managers
  - cn=Directory Administrators
  - cn=HR Managers
  - cn=PD Managers
  - cn=QA Managers**

Name	Value
objectClass	top
objectClass	groupOfUniqueNames
uniqueMember	uid=jwalker, ou=People, dc=example, dc=com
uniqueMember	uid=fsalazar, ou=People, dc=example, dc=com
uniqueMember	uid=abergin, ou=People, dc=example, dc=com
cn	QA Managers
description	People who can manage QA entries
ou	groups

## 8. Save service configuration. Check the image below with an example of the service configured.

### LDAP Groups

Group Expansion Manager:

Run script: ☐

Server

Server url:

Authentication:

LDAP Server username:

LDAP Server password:

Connection timeout:

Read timeout:

Use Single Search Base: ☒

Search base:

Scope:

User query:

Group query:

Group membership attributes

User key:

User name:

Group key:

Group name:

Group mapping:

☒ Groups hold members

The steps above will let you have the service up and running. If the configurations were provided correctly, Aspire had cached the information about users and groups in the NoSQL provider configured for it.

```
2020-09-23T20:30:48Z INFO [/Ldap_Cache/Main/LdapCache]: Beginning LDAP download: Ldap_Cache
2020-09-23T20:30:48Z INFO [/Ldap_Cache/Main]: Installed component: /Ldap_Cache/Main/LdapCache
2020-09-23T20:30:48Z INFO [/Ldap_Cache]: Installed component: /Ldap_Cache/Main
2020-09-23T20:30:48Z INFO [/Ldap_Cache]: Starting component: CacheLoadScheduler (aspire-scheduler)
2020-09-23T20:30:48Z INFO [aspire]: Registering component: /Ldap_Cache/CacheLoadScheduler
2020-09-23T20:30:48Z INFO [/Ldap_Cache/CacheLoadScheduler]: Starting scheduler (enabled)
2020-09-23T20:30:48Z INFO [/Ldap_Cache]: Installed component: /Ldap_Cache/CacheLoadScheduler
2020-09-23T20:30:48Z INFO [aspire]: Successfully started appBundle: /Ldap_Cache (location: com.accenture.aspire:app-ldap-group-cache [11])
2020-09-23T20:30:48Z INFO [aspire]: Fetching: com.accenture.aspire:app-ldap-group-cache:4.0
2020-09-23T20:31:05Z INFO [/Ldap_Cache/Main/LdapCache]: Finished LDAP download: Ldap_Cache
2020-09-23T20:31:05Z INFO [/Ldap_Cache/Main/LdapCache]: Lock released
```

Let's take a look at the "usersAndGroups" MongoDB collection or corresponding on the Elasticsearch engine for the Group Expansion Manager database.

db.getCollection('usersAndGroups').find({})

Key	Value
(1) 1600882414564_Andy_Ldap_Cache	{ 7 fields }
_id	1600882414564_Andy_Ldap_Cache
@isGroup	false
@name	Andy
groups	Andy
src	Ldap_Cache
ts	1600882414564
key	andy
(2) 1600882414564_John_Ldap_Cache	{ 7 fields }
_id	1600882414564_John_Ldap_Cache
@isGroup	false
@name	John
groups	John
src	Ldap_Cache
ts	1600882414564
key	john

Aspire provides other resources through the Aspire Debug Console, that will let you run the service and cache users and groups.

- Open the Aspire Debug Console.
- Click on the LDAP Cache Service name listed on the Top-Level Applications Installed section.
- Click on CacheLoadScheduler sub-component.

- Click on the Start button on the loadScheduler row. This should cache the users/groups from the LDAP. Some lines must appear in the Aspire Console referring to the start and end of the LDAP information download.
- Click the Back button on your IE.
- Click on the Main sub-component.
- Click on the LdapCache sub-component.
- Click on the List button to dump the users/groups cached.



## Related articles

- [Configure LDAP Cache Service](#)
- [Security Access Control Configuration](#)