LDAP Identity Connector - Features

Introduction

The LDAP Identity connector will crawl data about groups, persons, and more. It accomplishes this goal by storing data in the LDAP directory and authenticating users to access the directory.

Environment and Access Requirements

Account Privileges

For the LDAP Identity connector to be able to crawl the data from the LDAP directory that corresponds to the domain specified in the connection, it needs that the specified credentials have enough permissions to read said identities from the directory.

Other Requirements

The Aspire worker nodes must be able to reach the LDAP directory specified in the connection.

Framework and Connector Features

Framework Features

Name	Supported
Content Crawling	No
Identity Crawling	Yes
Snapshot-based Incrementals	No
Non-snapshot-based Incrementals	Yes
Document Hierarchy	No

Connector Features

The LDAP Identity connector has the following features:

- Get attributes specific to a user or groups.
- Specify a unit key for users or groups.
- Specify a group mapping: The LDAP attribute that maps users to groups is an attribute from the set of group attributes.
- Specify a membership relationship (if groups have the members or members have the groups).

Content Crawled

The LDAP Identity connector can crawl the following objects:

Name	Type	Relevant Metadata	Content Fetch and Extraction	Description
User	document	User ID Common Name (cn) Surname ObjectClass Attributes	No	The users of the LDAP directory.
Group	document	Unique member Common Name (cn) Organizational unit (ou) ObjectClass Attributes	Yes	The groups of the LDAP directory.