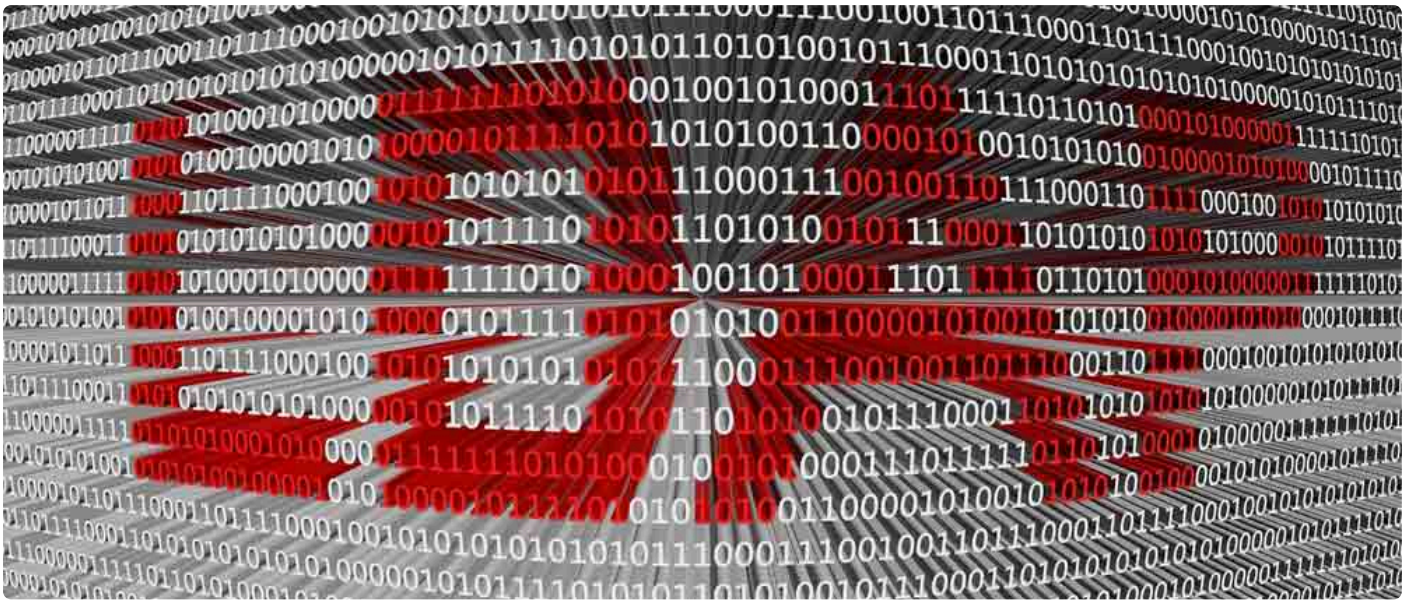
LDAP authentication and authorisation, part 1: OpenLDAP setup

Cliff Stayley · 2019-01-28



It is a common practice to use LDAP / Active Directory within organisations to authenticate and authorise employees. This is probably the reason why it is the most commonly used Search Guard feature. In this post we provide an overview of LDAP with a live demo. This will help you to understand how LDAP works and test the integration of LDAP with Search Guard powered Elasticsearch cluster.

LDAP Overview

Active Directory is a directory service developed by Microsoft while LDAP (The Lightweight Directory Access Protocol) is an open industry standard directory service.

Directory services allow to store objects in a directory tree. Each object is identified by its distinguished name (DN) and contains attributes. A distinguished name is a chosen subset of object attributes. LDAP comes with predefined object classes that may be helpful for managing organisation's assets.

It is a common practice to store users and their passwords within LDAP. In that case the password is an attribute of a user entry. Together with the ability to manage a users' groups, this allows to use LDAP for authentication and authorisation. Both of them are supported with Search Guard.

OpenLDAP demo setup

We will run OpenLDAP within a Docker container. There are many ready-made Docker images containing OpenLDAP out there with you can use as quickstart.

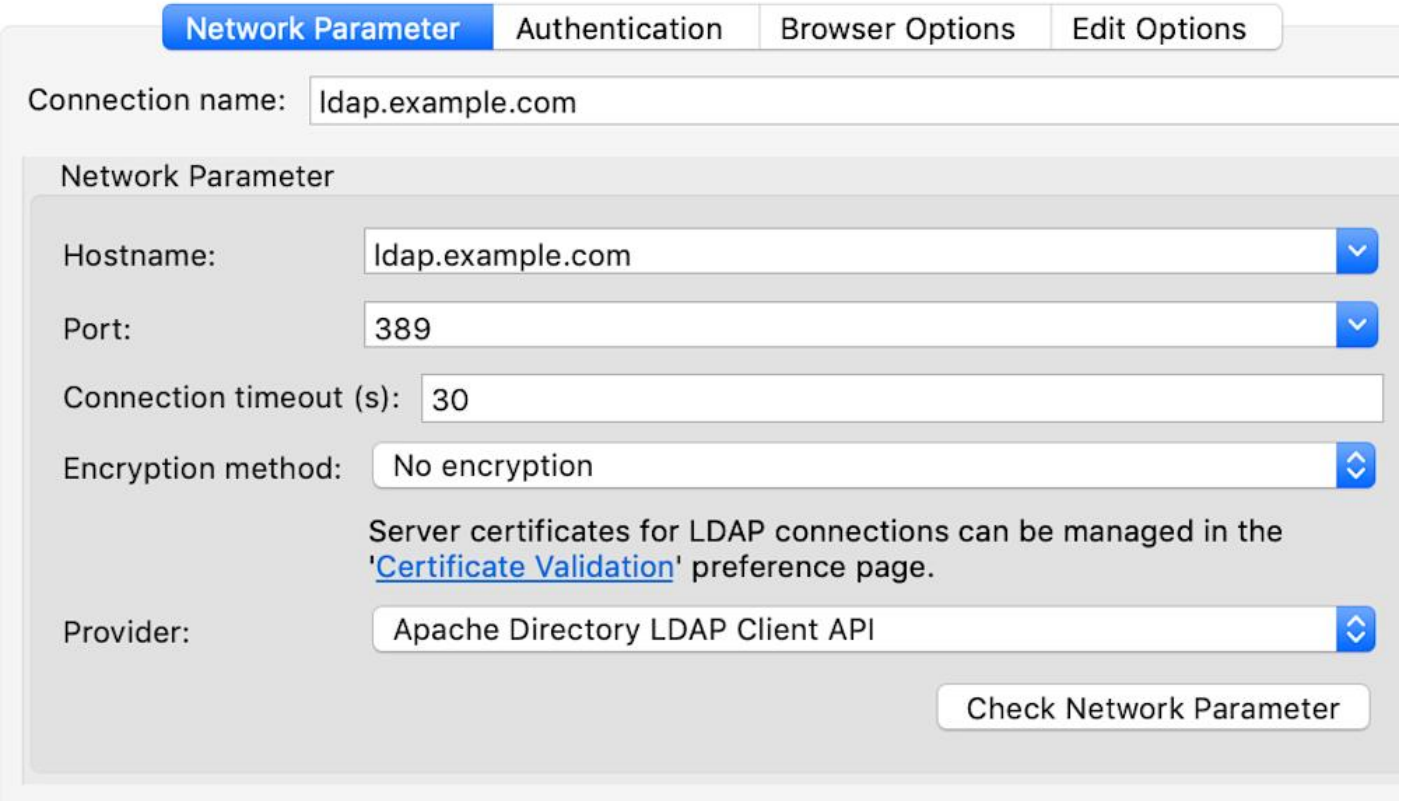
The LDAP server will be accessed via ldap.example.com in the remainder of this article, so we add an entry to local */etc/hosts*:

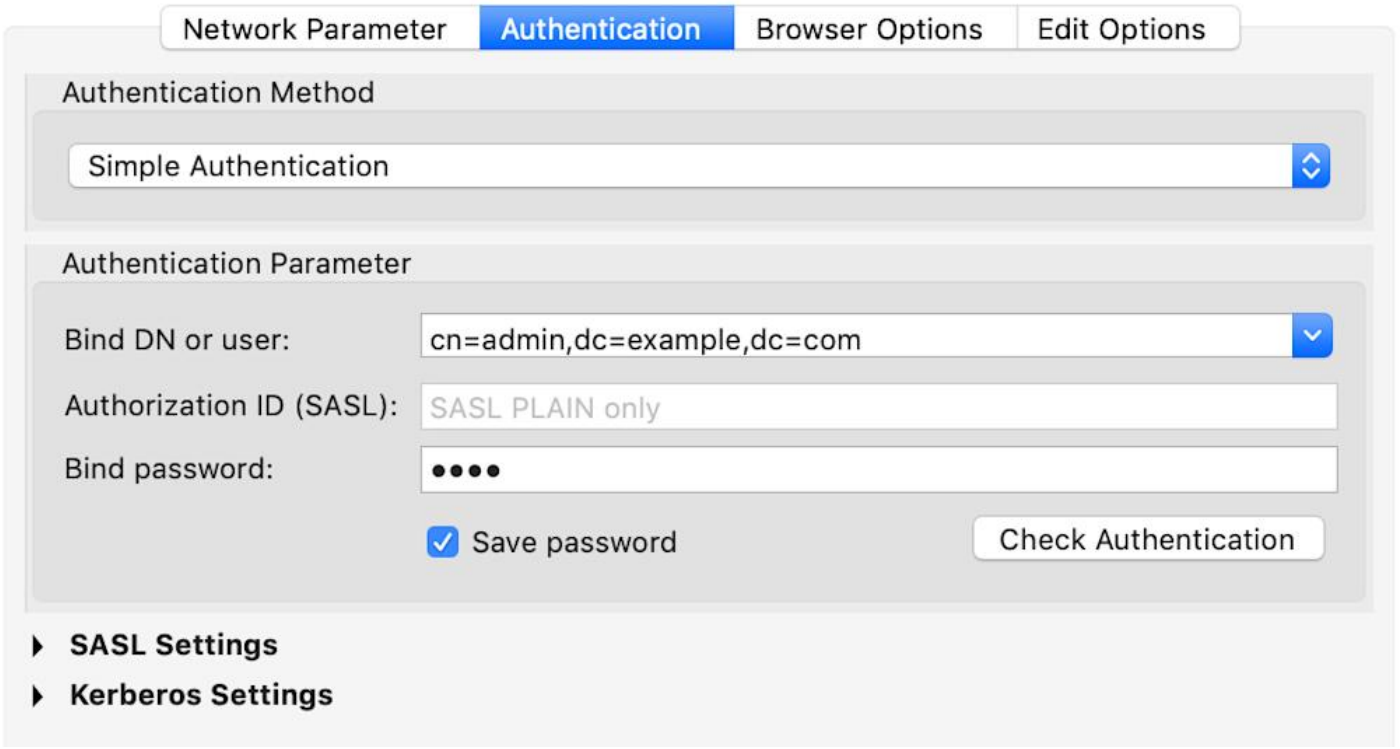
```
127.0.0.1 ldap.example.com
```

We can then run the LDAP server based on the docker image available on Github with:

```
docker run -p 389:389 \
  --env LDAP_ORGANISATION="My Company"
  --env LDAP_DOMAIN="example.com" \
  --env LDAP_ADMIN_PASSWORD="pass" \
  --detach osixia/openldap:1.2.2
```

We also install ApacheDirectoryStudio on our local machine to manage LDAP users. The LDAP connection can be configured with the following network and authentication parameters:

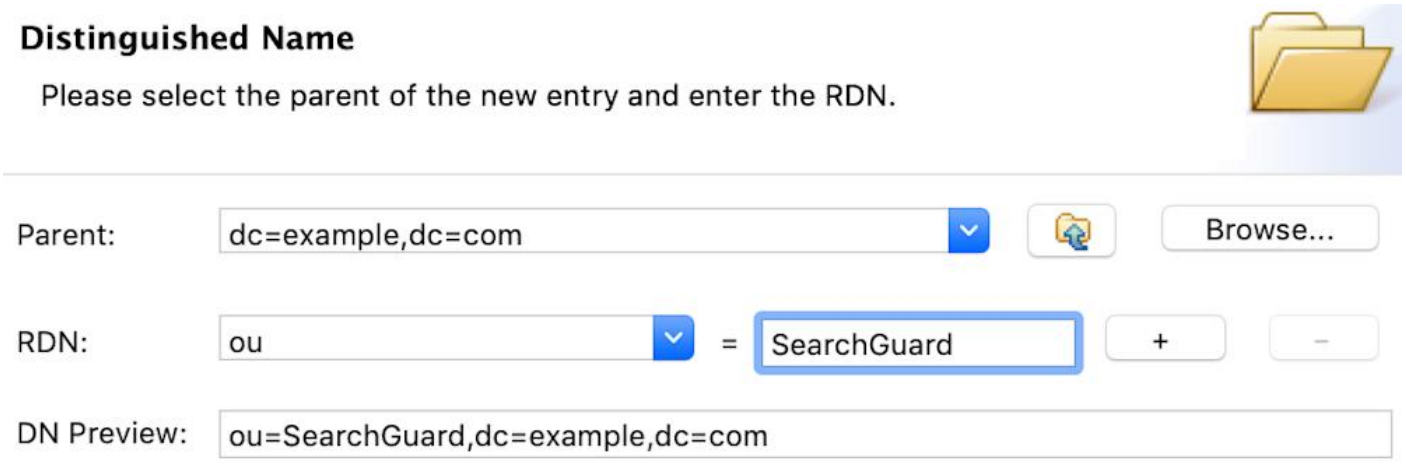




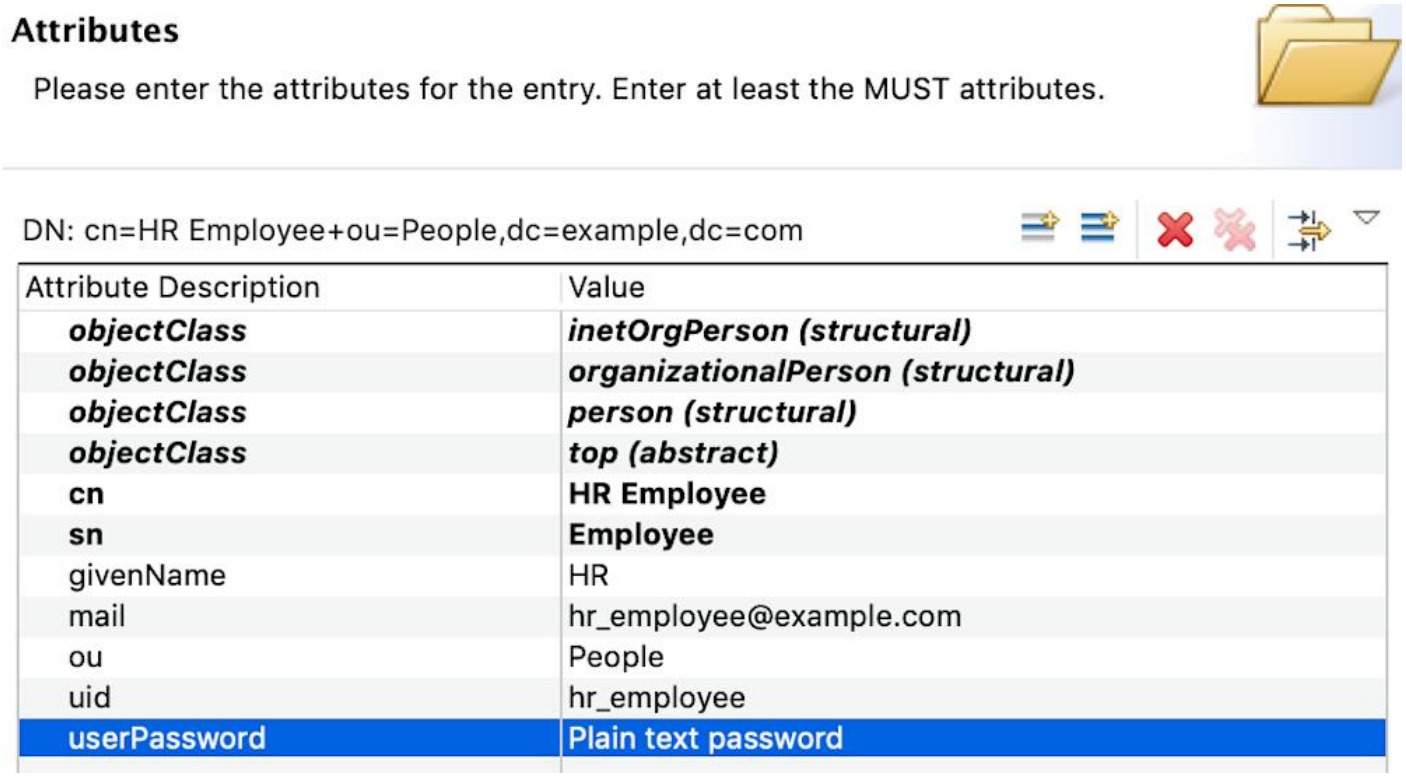
Creating sample users

Next we create a sample user *hr*employee_ in ApacheDirectoryStudio:

- We create entry based on inetOrgPerson class.
- We define the following DN attributes:



- and other attributes including user's password:



Now we can use *ldapsearch*, from a command line on a docker's host, to check if the user was created correctly:

```
ldapsearch -h ldap.example.com \
  -p 389 \
  -D "cn=admin,dc=example,dc=com" \
  -W \
  -b "dc=example,dc=com" \
  "uid=hr_employee"
```

The command parameters are applied to:

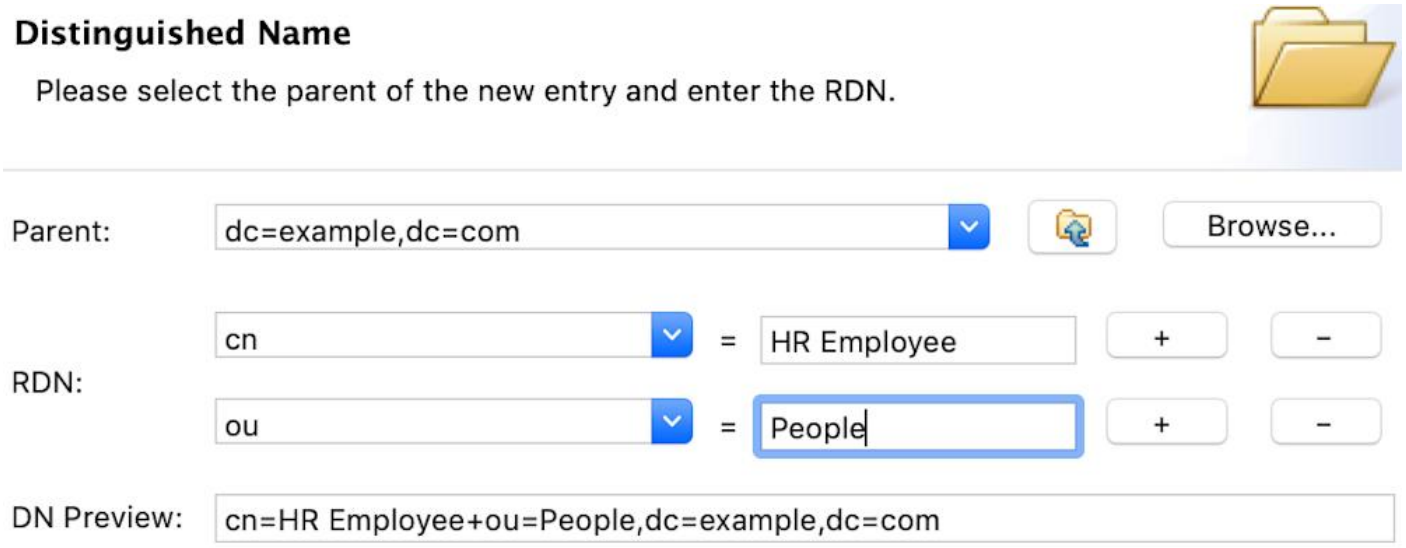
- -h and -p specify LDAP host and port,
- -D specifies distinguished name to bind within LDAP directory,
- -W prompt for simple authentication,
- -b the starting point for search.
- "uid=hr*employee" stands for searching all the entries with an attribute uid equal to hr*employee

This should output hr_employee user's attributes:

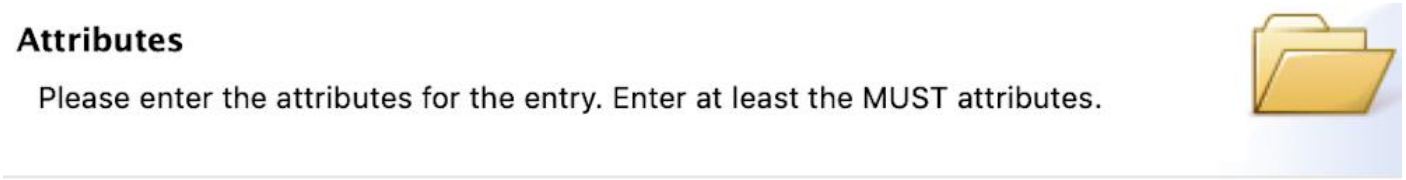
```
# HR Employee + People, example.com
dn: cn=HR Employee+ou=People,dc=example,dc=com
uid: hr_employee
mail: hr_employee@example.com
givenName: HR
ou: People
sn: Employee
cn: HR Employee
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
userPassword:: cGFzcw==
```

Creating a sample group

Let us now create a sample group SearchGuard and add a hr*employee to it. We create LDAP entry of a class* groupOfNames_:



and add the member attribute *uid=hr_employee*:



DN: cn=SearchGuard,dc=example,dc=com

Attribute Description	Value
objectClass	***groupOfNames (structural)***
objectClass	***top (abstract)***
cn	**SearchGuard**
member	**uid=hr_employee**

Note that a group can have multiple member attributes for other members.

This ends our demo. We can now use the created setup for a demo Search Guard & LDAP integration that we show in the next article.

Where to go next

- Read the next article in this series about how to configure LDAP for Search Guard (upcoming)
- Read the LDAP authentication configuration guidelines in our docs
- Read the LDAP authorisation guidelines in our docs
- Download the Search Guard Active Directory / LDAP presentation

Image: shutterstock / Profit_Image

This article was published on the Search Guard blog: https://search-guard.com/blog/elasticsearch-ldap-openldap/
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · Start a free trial