https://app.titra.io/try

LDAP interface working example

The first official titra extension is LDAP authentication support. It should support most LDAP configurations out-of-the-box and is available in the titra Extension Store.

To prevent exposure of sensitive credentials, the configuration of the interface is only available through environment variables passed to the titra service.

A minimal working example for an LDAP interface without authentication could look like this:

```
LDAP_HOST=ldap.kromit LDAP_PORT=389 LDAP_BASEDN="ou=People,dc=kromit,dc=com"
```

And a more complex working example if the uid in your LDAP is not the e-mail address which is the main identifier for titra before using LDAP and anonymous binds are not available:

```
LDAP_HOST=ldap.kromit LDAP_PORT=389 LDAP_BASEDN="dc=kromit,dc=at"
LDAP_AUTHENTICATION_USERDN="cn=admin,dc=kromit,dc=at" LDAP_AUTHENTICATION_PASSWORD="supersecret"
LDAP_USER_SEARCH_FIELD="mail" LDAP_USER_AUTHENTICATION=none LDAP_EMAIL_MATCH_ENABLE=true
LDAP_MERGE_EXISTING_USERS=true
```

Due to the fact that environment variables are used for configuring the LDAP interface, the titra service has to be restarted to use it.

The following variables are available:

- LDAP_HOST: The hostname of the LDAP server (mandatory)
- LDAP_PORT: The port of the LDAP server (mandatory)
- LDAP_BASEDN: The base dn for the LDAP search (mandatory)
- LDAP_RECONNECT: Reconnect to the server if the connection is lost?
- LDAP_TIMEOUT: The timeout of the LDAP connection (defaults to 10000ms)
- LDAP_CONNECT_TIMEOUT: The timeout of the LDAP connection attempt (defaults to 10000ms)

- LDAP_IDLE_TIMEOUT: The idle timeout of the LDAP connection
- LDAP_ENCRYPTION: If using LDAPS, set it to 'ssl', else it will use 'ldap://'
- LDAP_CA_CERT: The certificate for the LDAPS server
- LDAP_REJECT_UNAUTHORIZED: Reject Unauthorized Certificates? (defaults to true)
- LDAP_AUTHENTICATION_USERDN: The search user dn (defaults to the LDAP_BASEDN parameter if not provided)
- LDAP_AUTHENTICATION_PASSWORD: The search user password (optional)
- LDAP_LOGIN_FALLBACK: If the user is not found in the LDAP, try to login with the username and password? (defaults to false)
- LDAP_USER_AUTHENTICATION: The user authentication (defaults to LDAP_USERNAME_FIELD or 'uid' if neither is provided) - set to "none" to prevent user binds all-together (see complex example for a use case above)
- LDAP_USER_AUTHENTICATION_FIELD: The field used for authenticating users (defaults to 'uid')
- LDAP_USER_ATTRIBUTES: The attributes to retrieve from the LDAP
- LDAP_USER_SEARCH_FILTER: The search filter for the LDAP user search
- LDAP_USER_SEARCH_SCOPE: The scope of the LDAP user search filter
- LDAP_USER_SEARCH_FIELD: The field containing the user field for the LDAP search filter (defaults to LDAP_USERNAME_FIELD or 'uid' if neither is provided)
- LDAP_SEARCH_PAGE_SIZE: The number of results per page for the LDAP user search
- LDAP_SEARCH_SIZE_LIMIT: The maximum number of results for the LDAP user search
- LDAP_GROUP_FILTER_ENABLE: Enable LDAP group filter? (defaults to false)
- LDAP_GROUP_FILTER_OBJECTCLASS: The objectclass for the LDAP group filter
- LDAP_GROUP_FILTER_GROUP_ID_ATTRIBUTE: The attribute containing the group id for the LDAP group filter
- LDAP_GROUP_FILTER_GROUP_MEMBER_ATTRIBUTE: The attribute containing the group members for the LDAP group filter
- LDAP_GROUP_FILTER_GROUP_MEMBER_FORMAT: The format for the LDAP group filter
- LDAP_GROUP_FILTER_GROUP_NAME: The name of the group for the LDAP group filter
- LDAP_USERNAME_FIELD: The field containing the username field (defaults to 'uid')
- LDAP_LOG_ENABLED: Specifies wether logs are printed to STDOUT or not (defaults to false)
- LDAP_EMAIL_MATCH_ENABLE: Try to find the titra user based on the e-mail address (defaults to false)

- LDAP_MERGE_EXISTING_USERS: Try to merge existing users when they try to login through LDAP for the first time (defaults to false)

Revision #4

Created 30 July 2021 09:07:12 by Thomas Leb

Updated 16 February 2022 16:48:12 by Fabian Kromer