Systems - LDAP: Manage users

Introduction

This tutorial will show you how to connect LDAP as target system for users from CzechIdM. We will use default LDAP connector from ConnId.

Basic configuration

Go to **Systems** from main menu, then above list of current systems use Add button. On first page just fill system name. On the same page you may need to set new password policy in case that your default policy does not meet your all requirements of your LDAP configuration.

Connector configuration

In next step switch to menu **Configuration** of your new system. At first you need to choose connector, which in this case is **LDAP connector**. It will open specific configuration for that choice.

Thereafter fill important fields.

Example configuration for our local LDAP: TODO

Switch on **Use VLV Controls** and set **VLV Sort Attribute** to the same value as **Uid Attribute**. Otherwise, searching of accounts doesn't work well in the current version of LDAP connector (first result is skipped due to a bug).

Base Contexts

The property **Base Contexts** contains one or more starting points in the LDAP tree that will be used when searching the tree.

When you run synchronization in the reconciliation mode, the connector starts the search for every value in the Base Context separately. The search uses paging, which means that the entries are processed in blocks consisting of (by default) 100 records according to the configured (VLV) sort. Be careful, when you have multiple values in the Base Contexts and you **modify distinguished name** of the entries **during the reconciliation**. If entries are moved to a different base, then other entries may omitted due to the paging and they fall to the **Missing account** state.

Scheme

For next step, go to menu **Scheme** on your system.

You can let CzechIdM generate scheme for you by click on **Generate scheme** button. But if you want to set everything by yourself:

- Use button **Add** for create new scheme. For users you need to name it "__**ACCOUNT**__", because it is ConnId constant
- Add all file columns which you want to work with. Instead of name of your identifier column use ConnId constant "__**NAME**__"
- Set all attributes as **Able to read**

Example scheme: TODO

The attribute **uid** must be set with the following checkboxes: Able to read, Able to create, Returned by default. The checkbox "able to create" is important especially if you manage posixGroups. The LDAP connector requires the attribute "uid" during create, if "posixGroups" is also set. Otherwise it throws an error "Cannot add entry "uid=john.doe,ou=people,o=domain,c=tld" to POSIX groups because it does not have a "uid" attribute".

On the other hand, the checkbox **Able to edit** mustn't be set, if uid is the part of distinguishedName. Otherwise changing of uid throws an error "javax.naming.directory.SchemaViolationException: [LDAP: error code 67 - Not Allowed On RDN];"

Mapping

Now go to menu **Mapping**. There you must set how data from LDAP will be promoted to CzechIdM.

At first set:

- **Operation type:** Provisioning
- **Object name:** __ACCOUNT__
- **Entity type:** Identity
- As **Mapping name** set whatever you want to, for example Provisioning of users.

Then map all columns as entity attributes as you can see it on picture below. Just **__NAME__** set as identifier.

Example attribute mapping:

The distinguished name should be mapped in the attribute **__NAME__**. If the DN contains CN (common name - that is a typical setting), then don't map the attribute **cn** again. The CN is already filled by the DN and if you map it again, then a change of CN

can be refused by LDAP with the message "LDAP: error code 67 - Not Allowed On RDN".

Provisioning

Finally go to menu **Provisioning** and add new one set its **Name** and these fields:

- **Allowed:** true
- **Set of mapped attributes:** Select mapping from previous step.
- **Correlation attribute:** __NAME__

You can leave the rest of configuration at the default values.

Example provisioning results: TODO

Create LDAP role in IdM

To provision an account to LDAP, one must create a role for the system with LDAP provisioning mapping.

- Create a role e.g. "LDAP - user" and save it
- Go to System tab on role detail and add a system LDAP created in this tutorial and save.

To provision a user to LDAP, assign them a role "LDAP - user". The provisioning will be provided as soon as the role is assigned to the user. The state of the provisioning you can check at the user profile detail at the tab "provisioning".