Systems - AD: Groups synchronization

---

https://wiki.czechidm.com/

2020/02/20 12:19

Table of Contents

Systems - AD: Groups synchronization

This tutorial is intended as a guide for administrators that want to load AD groups into CzechIdM (either one time or as a scheduled job).

You will learn

- how to connect an AD system for groups synchronization
- how to use a groups sync workflow
- how to prepare users to be able to assign them IdM roles by their AD groups

Before you start

First of all, you need to download the connector from Connid (e.g. Connid AD bundle 1.3.4 jar file). Then add the jar file into the CzechIdM folder inside the application server. In case you installed CzechIdM into tomcat by standard installation, the path would be `/opt/tomcat/current/webapps/idm/WEB-INF/lib/`.

To preserve the connector during future upgrades of CzechIdM core, put the connector in e.g. /opt/czechidm/lib/ and create symbolic link in the CzechIdM webapp folder:

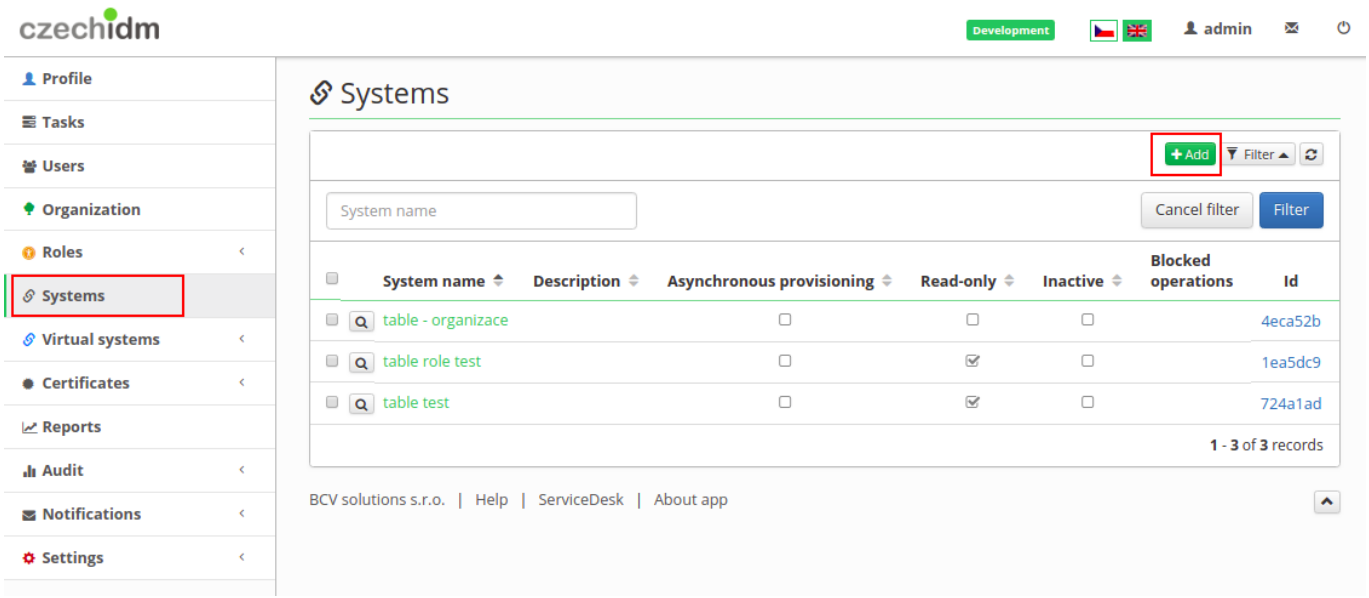
```
ln -s /opt/czechidm/lib/net.tirasa.connid.bundles.ad-1.3.4.jar
/opt/tomcat/current/webapps/idm/WEB-
INF/lib/net.tirasa.connid.bundles.ad-1.3.4.jar
```

Then restart the application server. If you had CzechIdM already running in the web browser, refresh also the web browser window (e.g. Ctrl+F5).

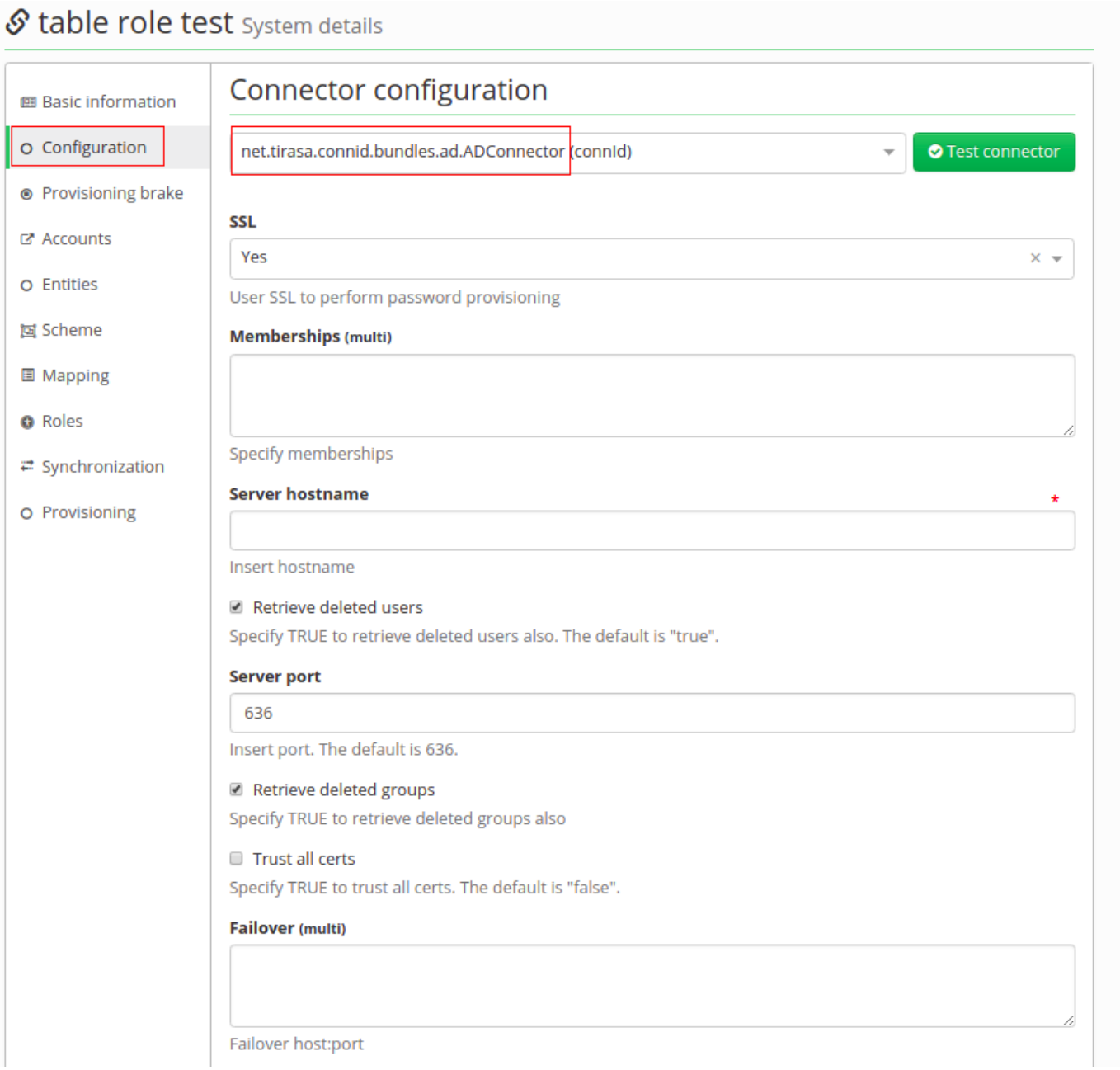
Then with tutorial Extended attributes - managing EAVs and forms, you should create EAVs for IdmTreeNode, IdmIdentity and IdmIdentityContract, so this EAVs can be used to create automatic roles. IdmTreeNode for an automatic role by organization and the others for an automatic role by attributes.

Create system

- Go to **Systems** in the left menu and then click on **Add**.



- Fill in name of a system. And click on **Save and continue**.
- In tab **Configuration** choose AD connector (net.tirasa.connid.bundles.ad.ADConnector)



Connector configuration

On this page fill in these important values:

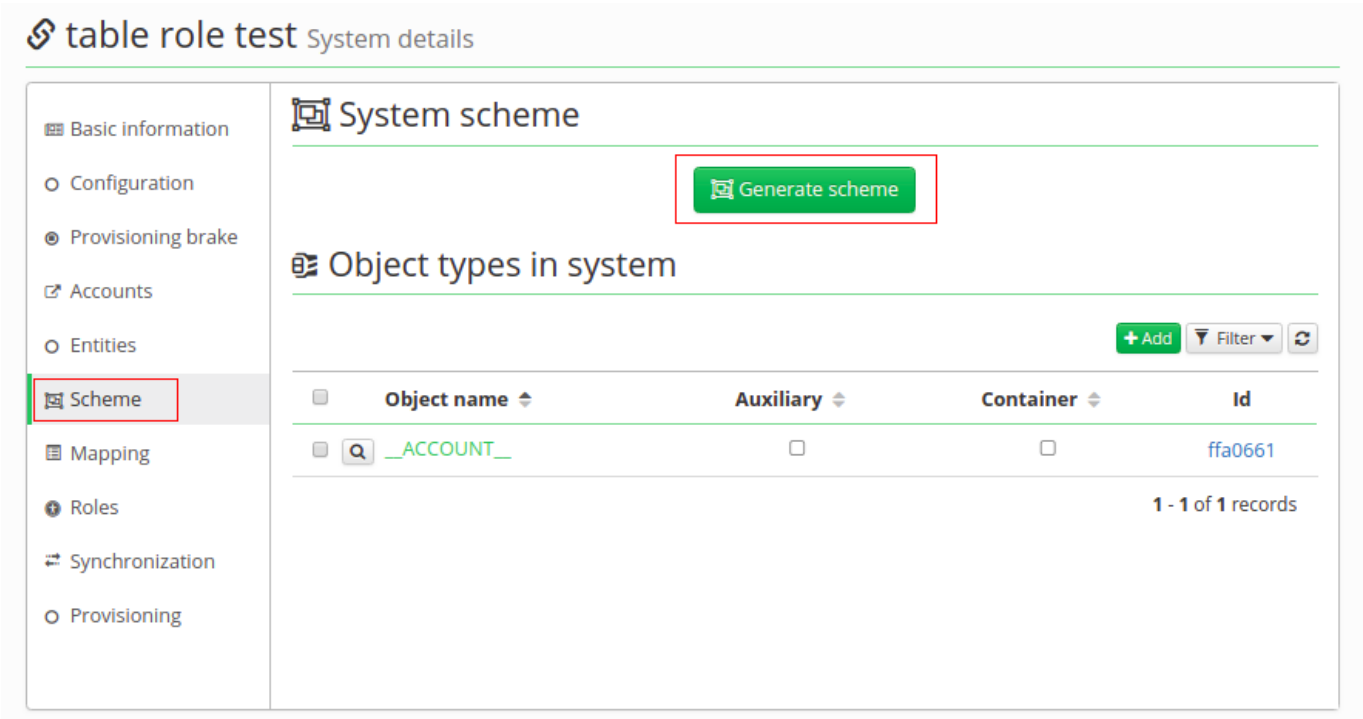
- **Server hostname** - IP address of ad server or hostname
- **Server port** - on this port will server listen
- **Principal** - with this username connector will connect to the AD system, this user has to have enough rights to reads groups
- **Principal password** - password of the "principal" account
- **Root suffixes** - there should be DNs of **Base contexts**, groups outside of these "paths" will be ignored. Content of **Root suffixes** could be same as **Base contexts** or just put in domain.
- **Entry object classes** - List of all objectClasses groups have in AD. It is necessary to find just groups. With wrong settings, it could find even users.
- **Group search scope** - Choose object, onlevel or subtree. It means where it will search for groups. As a **subtree**, a search will start on paths in **Base context** and it will search in every **Organization Unit** in this path. **onlevel** will search just one **OU**, where distinguished names of

Base context points to and the last **object** means, in **Base context** there are DNs of groups we want to synchronize.
- **Custom group search filter** - this enables additional filter for groups, which will be searched for. You can use it e.g. to filter out roles with some specific substrings in their CN by using LDAP filter `(&(!(cn=*Administrator*))(!(cn=*Auditor*)))`
- **Base contexts for group entry searches** - list of distinguished names (paths), where it will search for groups.
- **Group members reference attribute** - a name of the attribute, which indicates membership. It contains whole DNs of users.
- **useVlvControls** - have to be enabled - this is only supported option
- **pageSize** - number, it should be lower than maximum page size limit in AD, which is by default 1000. Recommended: 100.
- **vlvSortAttribute** - this should be identifier with sorting properties. Recommended for groups is cn.
- **Uid Attribute for groups** - unique identifier, recommended is objectGUID.
- **Object classes to synchronize** - Based on this filled object classes, groups to synchronized will be found. Content is usually same as **Entry object classes**.

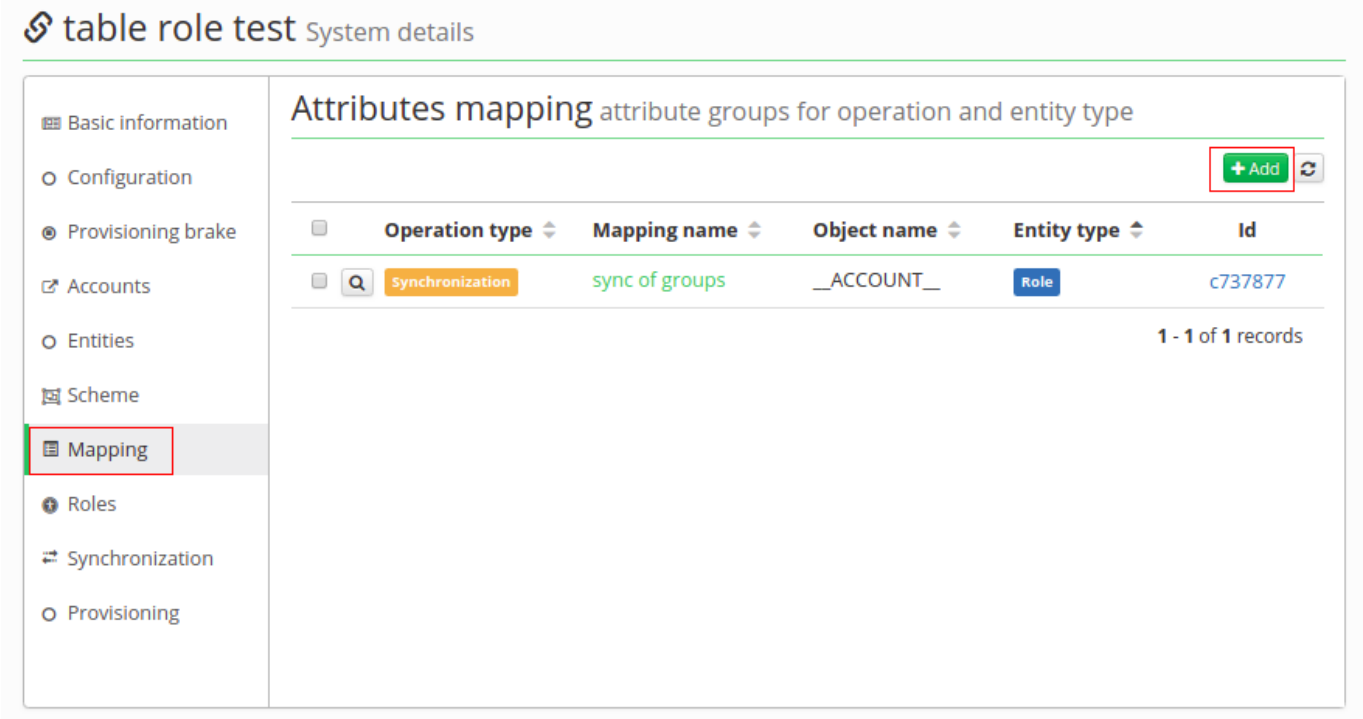
When you configure the system for the first time, root suffix should lead to the top container (e.g. DC=domain,DC=local), so the system schema can be correctly generated

Connector's mapping

- Firstly in **Scheme** tab generate a schema with a green button. If there is some exception, you have probably mistake in the configuration of the connector.

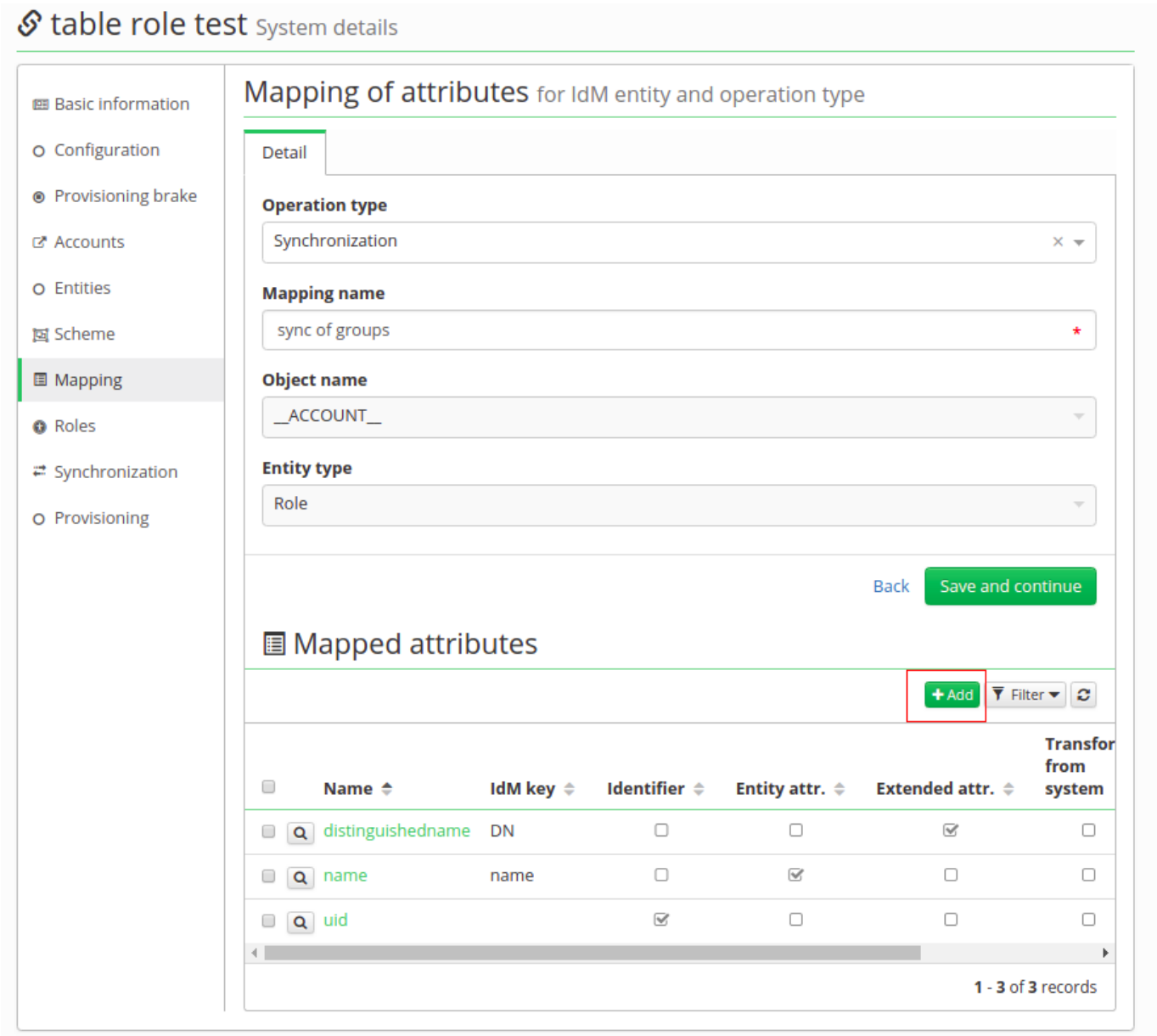


- Then in **Mapping** tab create new mapping - synchronization (__GROUP__ (Object name), Role (Entity type)).

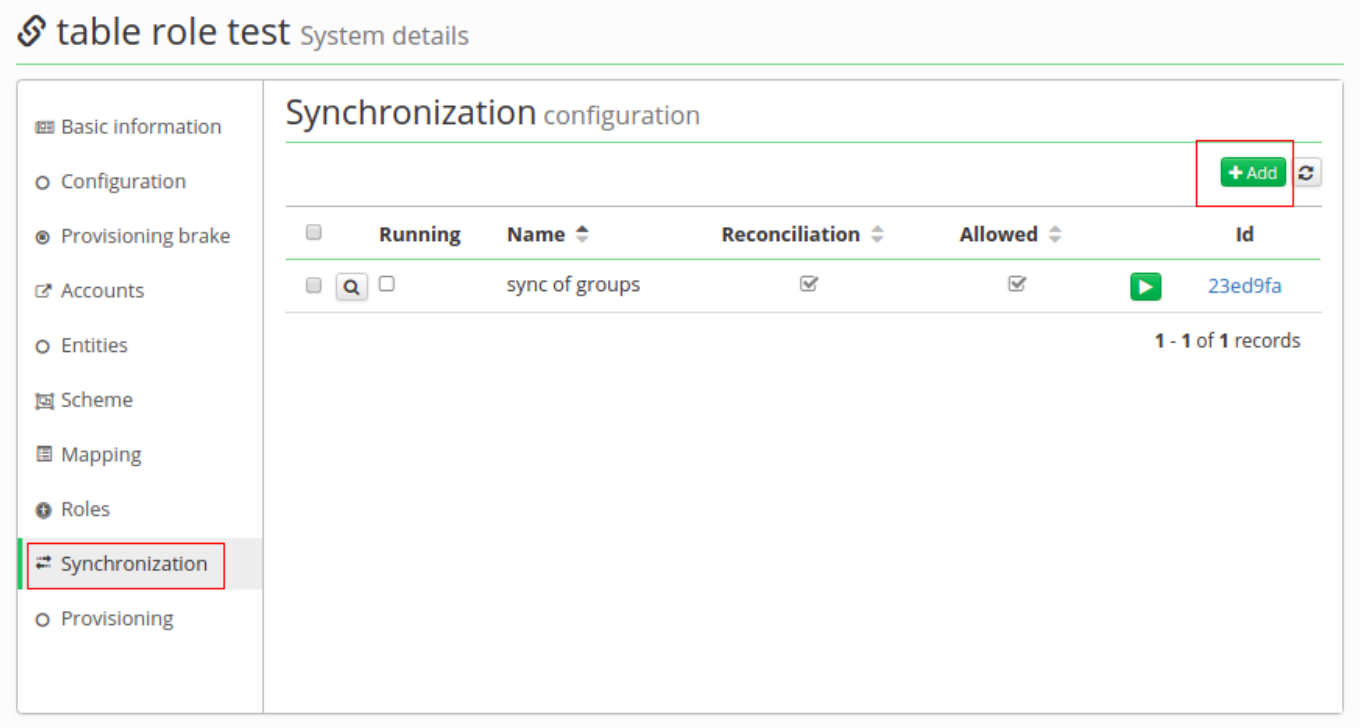


- Now we will map just 3 attributes. Click on green add button like on picture below and this fill in:

```
| Attribute in schema | Name                | Attribute          | IdM key
|
| __Name__ (__GROUP__)| Distinguished name | extended           |
distinguished_name |
| name (__GROUP__)    | name                | identifier, entity | name
|
| __UID__ (__GROUP__) | __UID__             |                    |
|
```



- In **Synchronization** tab create new synchronization.



- Enable **Allowed** and **Reconcillation**. Fill **Name, Set of mapped attributes** and then **Correlation attribute** as '__UID__'.
- Bellow there are 4 possibilities on state when synchronization starts (Linked, Not linked, Missing entity, Missing account).
  - **Linked** - it's like update, group is in the AD and also in IdM, but it is possible in the AD could be some change, so usually **Action** is "Update entity"
  - **Not Linked** - this means the group is in the AD and also in IdM, but in IdM was not created by synchronization, so it does not have an account on this system.
  - **Missing entity** - in other words - create action - group is in the AD, but in IdM it is not. It could be newly created in the AD, so it is not yet in IdM or it could be already erased in IdM. But this situation only supports "Ignore" and "Create entity" action.
  - **Missing account** - or "delete" - group is in IdM, but missing in AD. Groups are synchronized from the AD, and this situation usually means group was deleted in the AD, so in IdM we expect to be erased as well.
- In each of these possibilities there is a select box "Workflow". It is for selecting additional steps, which will be done. For example, when groups are synchronized, we want them to be in **Role catalog** or some of them as an **automatic role by organization**. And this is done in a workflow. You could write your own, but we have one, which covers basic actions with a just little bit of adjusting (Systems - Groups synchronization workflow).

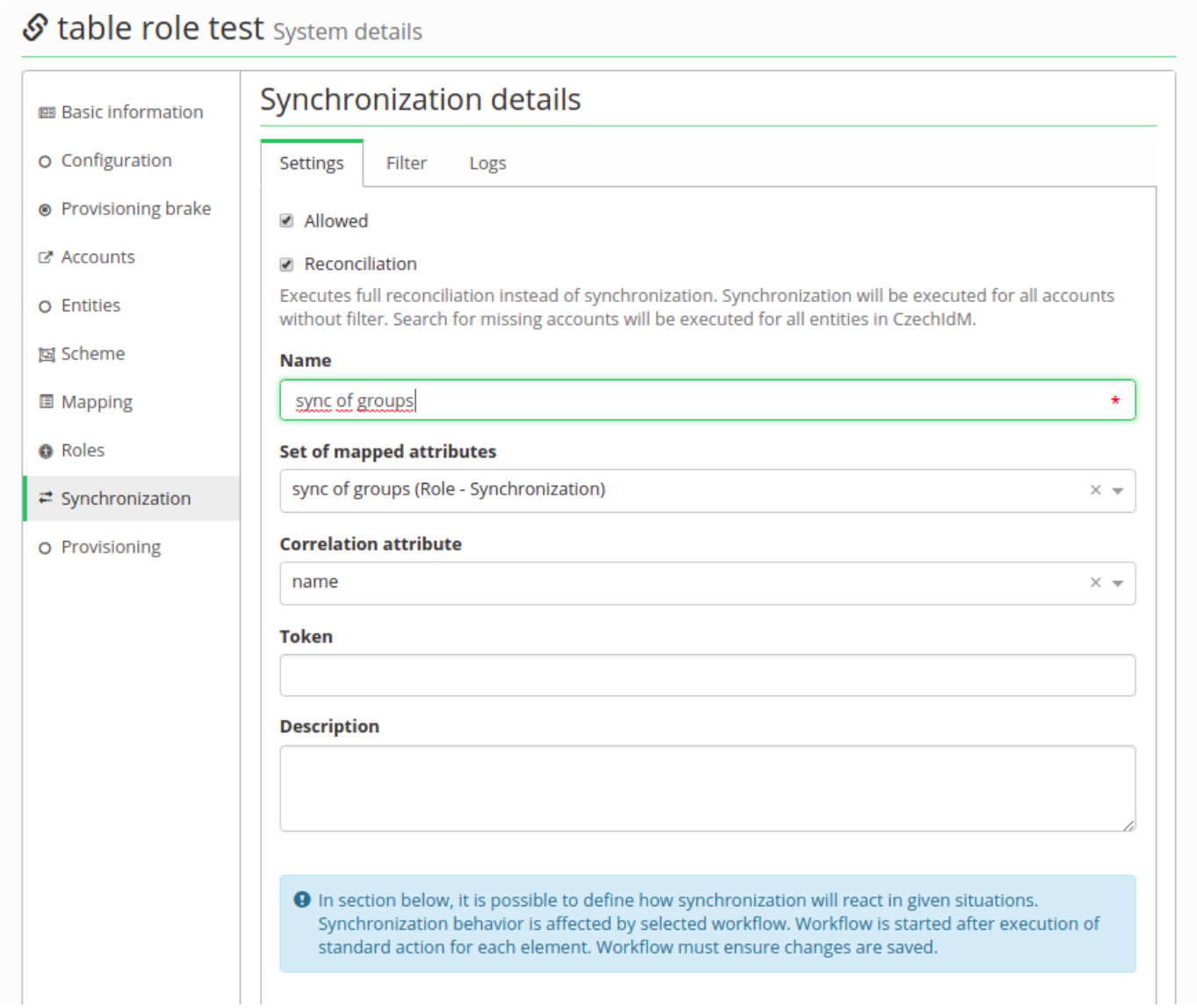
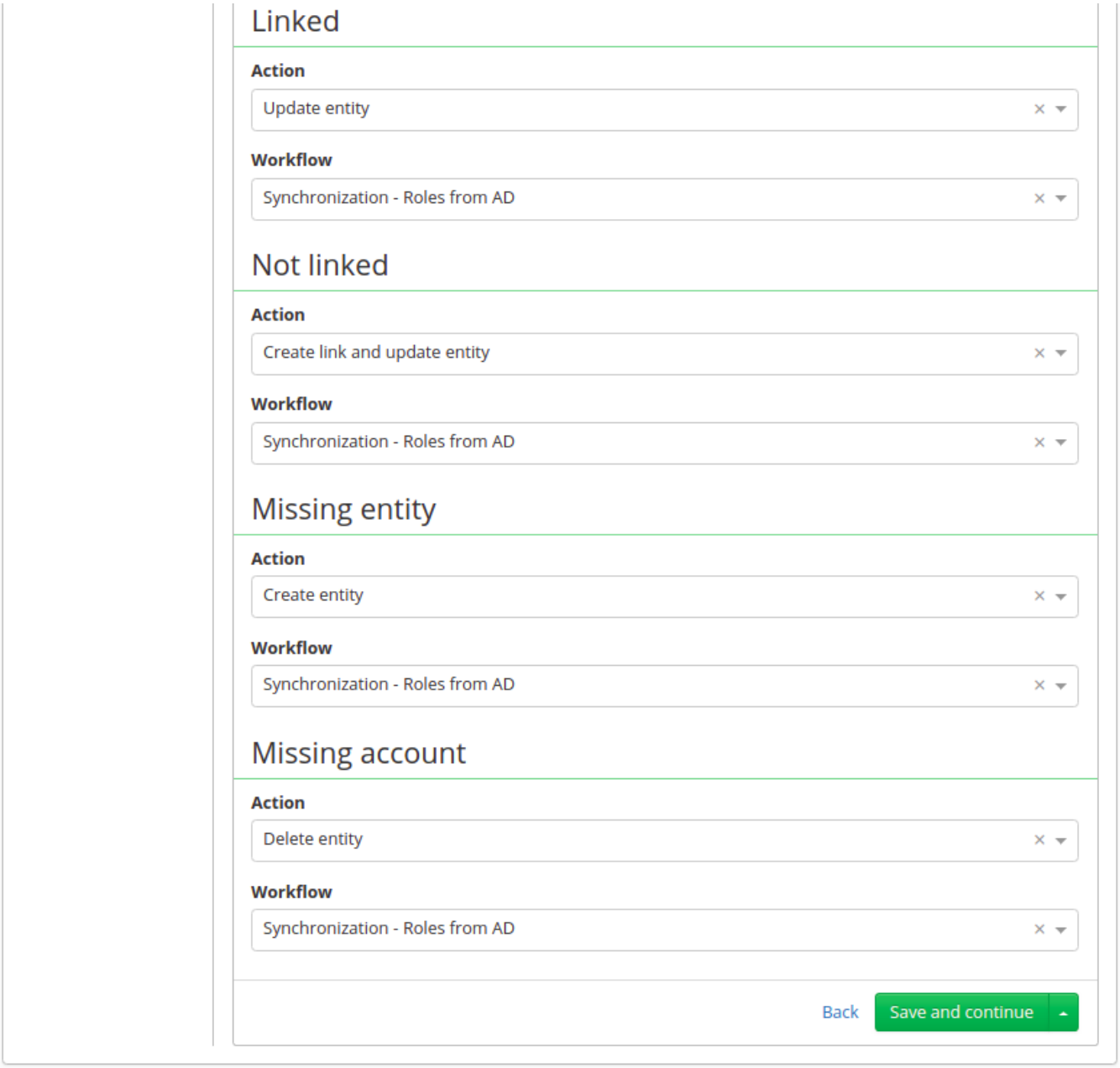


table role test System details
Basic information
Configuration
Provisioning brake
Accounts
Entities
Scheme
Mapping
Roles
Synchronization
Provisioning
Synchronization details
Settings
Filter
Logs
Allowed
Reconciliation
Executes full reconciliation instead of synchronization. Synchronization will be executed for all accounts without filter. Search for missing accounts will be executed for all entities in CzechIdM.
Name
sync of groups
Set of mapped attributes
sync of groups (Role - Synchronization)
Correlation attribute
name
Token
Description
In section below, it is possible to define how synchronization will react in given situations. Synchronization behavior is affected by selected workflow. Workflow is started after execution of standard action for each element. Workflow must ensure changes are saved.



Synchronization

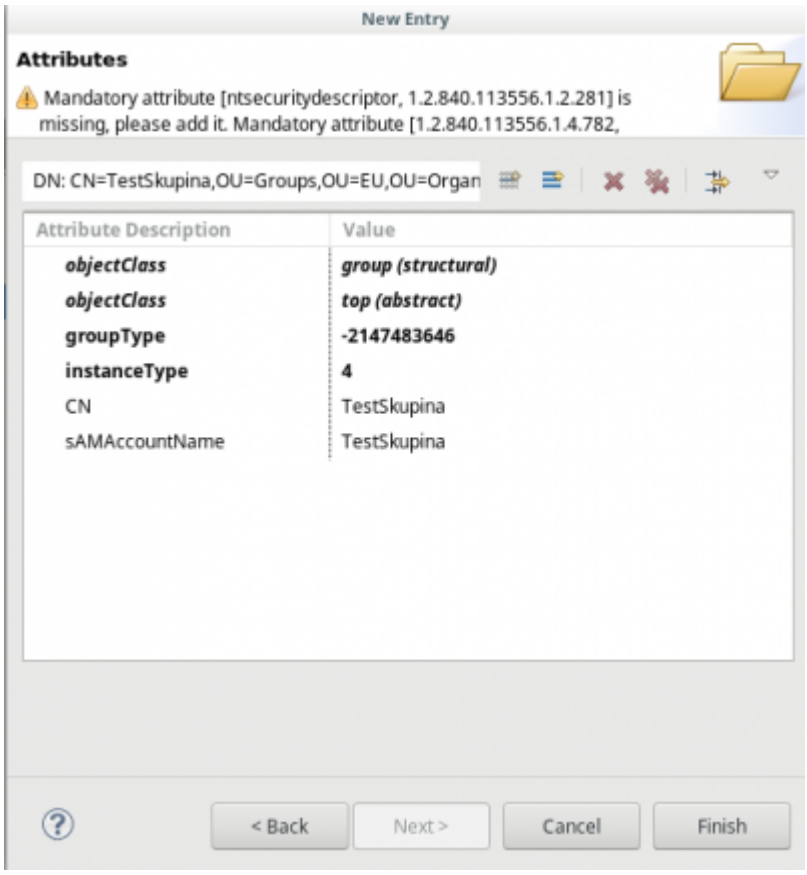
At this point configuring of synchronization is complete. Save this synchronization and run it. It should smoothly create a catalog, new roles and maybe even some automatic roles. If provisioning of memberships will fail do not forget to try "ldapGroups" attribute.

In user provisioning system's configuration **Base context of groups** should be filled too, for correctly provisioning memberships
In user provisioning system's schema and mapping should have attribute memberOf/ldapGroups and **Strategy** as "Merge".
If you synchronize groups with resolving users membership, the connector doesn't support groups with more than 1000 members (by default). If you need more, you must (temporarily) increase MaxPageSize in the AD configuration.

Tips

You can create a new security group in Active Directory with the Apache Directory Studio by following these steps:

- Select an existing group
- Right click on the group name → New → New entry
- Check the "Use existing entry as template" and click Next
- Object classes: Write "group" and click Add → group and top are added to "Selected object classes" → Next
- Distinguished Name: Set the value of RDN to your choice → Next
- A warning is displayed - click Cancel
- Set instanceType = 4
- Set sAMAccountName to your choice (right click → Edit values)
- Delete values (right click → Delete values) of these attributes:
  - nTSecurityDescriptor
  - objectCategory
  - member (if you don't want to copy members)
  - sAMAccountType



Finally, click Finish