

# 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).



This tutorial is for IdM 9 and 10. In version 11 you can use a wizard for groups synchronization configuration - [wizard tutorial](#)

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

### Adding Active Directory connector


Since CzechIdM 9.2, the [forked ConnId AD connector](#) is bundled inside CzechIdM by default. You can use it out of hand.

### System for managing AD users

Loading AD groups to IdM is usually done when you want to manage the group membership of the AD users by IdM. So connecting the system for managing AD users is a logical step before you start to synchronize the groups.

If you followed the [tutorial for managing AD users](#), you have the necessary configuration of the **AD users** system mostly prepared. Specifically:

- the attribute Base contexts for group entry searches contains all containers in AD where the groups are located. (Or it's empty and Root suffixes cover all those containers.)
- the attribute ldapGroups is set in the connector configuration, in the schema and in the provisioning mapping with the MERGE strategy

However, it's a common request to do **initial** loading of the group membership from AD. This topic will be covered later.  synchronization of AD users with mapped distinguishedName to EAV of identity, so the [groups synchronization workflow](#) can resolve membership.

### Automatic creation of automatic roles

The synchronization of AD groups can also create some automatic roles based on the position of the groups in AD. These are specific options of the [groups synchronization workflow](#) and it's not often

used for typical setup. However, if you want to use it, make sure to 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**.

Profile

Tasks

Users

Organization

Roles

**Systems**

Virtual systems

Certificates

Reports

Audit

Notifications

Settings

Development

admin

Systems

+ Add

Filter

System name

Cancel filter

Filter

	System name	Description	Asynchronous provisioning	Read-only	Inactive	Blocked operations	Id
<input type="checkbox"/>	<input type="text" value="table - organizace"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		4eca52b
<input type="checkbox"/>	<input type="text" value="table role test"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		1ea5dc9
<input type="checkbox"/>	<input type="text" value="table test"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		724a1ad

1 - 3 of 3 records

BCV solutions s.r.o.

Help

ServiceDesk

About app

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

## table role test System details

Basic information

Configuration

Provisioning brake

Accounts

Entities

Scheme

Mapping

Roles

Synchronization

Provisioning

### Connector configuration

net.tirasa.connid.bundles.ad.ADConnector (connId)

Test connector

SSL

Yes

User SSL to perform password provisioning

Memberships (multi)

Specify memberships

Server hostname

Insert hostname

☒ Retrieve deleted users  
Specify TRUE to retrieve deleted users also. The default is "true".

Server port

636

Insert port. The default is 636.

☒ Retrieve deleted groups  
Specify TRUE to retrieve deleted groups also

☐ Trust all certs  
Specify TRUE to trust all certs. The default is "false".


Failover (multi)

Failover host:port

## 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. Usual values: top, group (every value on a single line)
- **Group search scope** - Default subtree. Options: object, onelevel 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.  All behave the same on the current version, so other options can't be used: **onelevel** ("onlevel" is a typo) 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\*))). However, you can't use a filter with wildcards by whole distinguishedName attributes (distinguishedName, member, manager etc.). If you want to for example exclude a certain OU from searches use msDS-parentdistname attribute instead (available since Windows Server 2012), e.g. (! (msDS-parentdistname=OU=Excluded,DC=example,DC=tl)).
- **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. **DO NOT** use **distinguishedName** or any other unindexed attribute or you'll end up with "[LDAP: error code 12 - 0000217A: SvcErr: DSID-03140414, problem 5010 (UNAVAIL\_EXTENSION), data 0];" error!
- **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**



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 there are more than 10000 groups in AD and "Base contexts for group entry searches" is set for DC=AD,DC=FIRMA,DC=CZ(root OU). LDAP: error code 12 - 000020EF: SvcErr: DSID-03140552, problem 5010 (UNAVAIL\_EXTENSION), data 0



workaround/solution: separate ldap search with "Base context for group entry searches" and divide it into smaller searches(each line with one OU):

- OU=001OU,OU=FIRMA,DC=ad,DC=FIRMA,DC=cz
- OU=002OU,OU=FIRMA,DC=ad,DC=FIRMA,DC=cz
- OU=003OU,OU=FIRMA,DC=ad,DC=FIRMA,DC=cz
- OU=004OU,OU=FIRMA,DC=ad,DC=FIRMA,DC=cz

- OU=005OU,OU=FIRMA,DC=ad,DC=FIRMA,DC=cz



Another way to solve this problem is by using "Custom group search filter" in the system configuration.

## 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.

table role test System details

- Basic Information
- Configuration
- Provisioning brake
- Accounts
- Entities
- Scheme**
- Mapping
- Roles
- Synchronization
- Provisioning

### System scheme

**Generate the scheme**

### Object types in system

**+ Add** **Filter** **Refresh**

<input type="checkbox"/>	Object name	Auxiliary	Container
<input type="checkbox"/>	<input type="checkbox"/> <b>_ACCOUNT_</b>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/> <b>_ALL_</b>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/> <b>_GROUP_</b>	<input type="checkbox"/>	<input type="checkbox"/>

1 - 3 of 3 records

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

table role test

System details

Basic Information

Configuration

Provisioning brake

Accounts

Entities

Scheme

Mapping

Roles

Synchronization

Provisioning

Attributes mapping attribute groups for operation and entity type

+ Add

<input type="checkbox"/>	Operation type	Mapping name	Object name	Entity type
<input type="checkbox"/>	<div>Synchronization</div>	sync of groups	__GROUP__	<div>Role</div>

1 - 1 of 1 records

- Now we will map just 4 attributes. Click on green add button like on picture below and this fill in:

Attribute in schema	Name	Attribute	IdM key
__NAME__ (__GROUP__)	DN(__NAME__)	extended	
distinguished_name			
name (__GROUP__)	name	entity	name
name (__GROUP__)	name-code	entity	code
__UID__ (__GROUP__)	__UID__	identifier	

table role test

System details

Basic Information

Configuration

Provisioning brake

Accounts

Entities

Scheme

Mapping

Roles

Synchronization

Provisioning

Mapping of attributes for IdM entity and operation type

Detail

Operation type

Synchronization

Mapping name

sync of groups

Object name

\_\_GROUP\_\_

Entity type

Role

Back

Save and continue

Mapped attributes

+ Add

Filter

	Name	IdM key	Identifier	Entity attr.	Extended attr.	Transform from system	Transform to system
<input type="checkbox"/>	DN(__NAME__)	distinguished_name	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	name	name	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	name-code	baseCode	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	__UID__		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

table role test

System details

Basic information

Configuration

Provisioning brake

Accounts

Entities

Scheme

Mapping

Roles

Synchronization

Provisioning

Synchronization configuration

+ Add

	Running	Name	Reconciliation	Allowed		Id
<input type="checkbox"/>	<input checked="" type="checkbox"/>	sync of groups	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	23ed9fa

1 - 1 of 1 records

- Enable **Allowed** and **Reconciliation**. Fill **Name**, **Set of mapped attributes** and then **Correlation attribute** as '\\\_\\\_UID\\\_\\\_\'.
- Below 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**

**Set of mapped attributes**

**Correlation attribute**

**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.



	<h3>Linked</h3> <p><b>Action</b></p> <p>Update entity x ▾</p> <p><b>Workflow</b></p> <p>Synchronization - Roles from AD x ▾</p>
	<h3>Not linked</h3> <p><b>Action</b></p> <p>Create link and update entity x ▾</p> <p><b>Workflow</b></p> <p>Synchronization - Roles from AD x ▾</p>
	<h3>Missing entity</h3> <p><b>Action</b></p> <p>Create entity x ▾</p> <p><b>Workflow</b></p> <p>Synchronization - Roles from AD x ▾</p>
	<h3>Missing account</h3> <p><b>Action</b></p> <p>Delete entity x ▾</p> <p><b>Workflow</b></p> <p>Synchronization - Roles from AD x ▾</p>
	<p><a href="#">Back</a> <a href="#">Save and continue</a> ▴</p>

## Synchronization of groups

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 "IdapGroups" attribute.



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.

## Editing groups in Active Directory

CzechIdM managing membership of users in Active Directory groups, editing of groups is controlled

by administrators directly in AD, you need to link these edits with IDM. If you will don't follow correct steps, you will end with following error in provisioning of users with incorrectly edited AD group:



```
org.identityconnectors.framework.common.exceptions.ConnectorException: javax.naming.NameNotFoundException:
[LDAP: error code 32 - 0000208D: NameErr: DSID-03100288, problem 2001 (NO_OBJECT), data 0, best match
of: 'OU=Groups,DC=test_company,DC=local'];
remaining name
'CN=My_test_group,OU=Groups,DC=test_company,DC=local'
```

This error means that CzechIdM can not find DistinguishedName set in assigned role for any group in Active Directory. This group could be renamed, moved or deleted. If you come across a mentioned error, just delete items in provisioning queue for users, go through the specified tutorial and resave stuck users when it's finished.

## 1) Rename or move group in Active Directory

Synchronization must be started after each time you **rename** a group or **move** group to another organization unit. Otherwise provisioning of any user who is a member of the modified group will fail with following error in provisioning queue.

## 2) Delete group in Active Directory or move group from CzechIdM scope

If you want to delete role or move it from IDM scope:

- Make sure that no users have assigned role for this group and that the role is not used as automatic role.
- Then you can remove group from AD and **remove role from managed attributes**.

If you deleted groups or moved from IDM scope and you will try provisioning of users with linked role before synchronization of roles, provisioning will not be successful.

You will recognize this situation by error mentioned in the note above and also if you will run synchronization of groups, in log of synchronization you will have some items in the state **Missing account**.

### To correctly remove group and role:

- Open synchronization item with **Missing account** state and copy **Entity ID** from item. In most cases ID is ObjectGUID of the group.
- Go to **Account on system** on system for Groups and paste Entity ID into filter. By opening found item, you can see **role** for missing group.
- Make sure that you remove this role from all users.
- Remove the role from IDM.

- Remove group from AD.
- Go to system for AD User → Attributes mapping → Mapping for provisioning and click on attribute **ldapGroups** → go to tab **Controlled values** → In section **Attributes controlled in past**, you will see the group → delete it



If you will not perform last step and role was just moved from scope of IDM, because you want to manage this role without IDM → **IDM will still remove group managed users!**

## Tips

### CREATE NEW GROUP IN ACTIVE DIRECTORY

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

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

New Entry

Attributes

Mandatory attribute [ntsecuritydescriptor, 1.2.840.113556.1.2.281] is missing, please add it. Mandatory attribute [1.2.840.113556.1.4.782,

DN: CN=TestSkupina,OU=Groups,OU=EU,OU=Organ

Attribute Description	Value
objectClass	group (structural)
objectClass	top (abstract)
groupType	-2147483646
instanceType	4
CN	TestSkupina
sAMAccountName	TestSkupina

?

< Back

Next >

Cancel

Finish

Finally, click Finish

From:

<https://wiki.czechidm.com/> - CzechIdM Identity Manager

Permanent link:

[https://wiki.czechidm.com/tutorial/adm/ad\\_groups\\_sync](https://wiki.czechidm.com/tutorial/adm/ad_groups_sync)

Last update:

2024/02/16 15:31

