

# Systems - Ldap: Roles provisioning

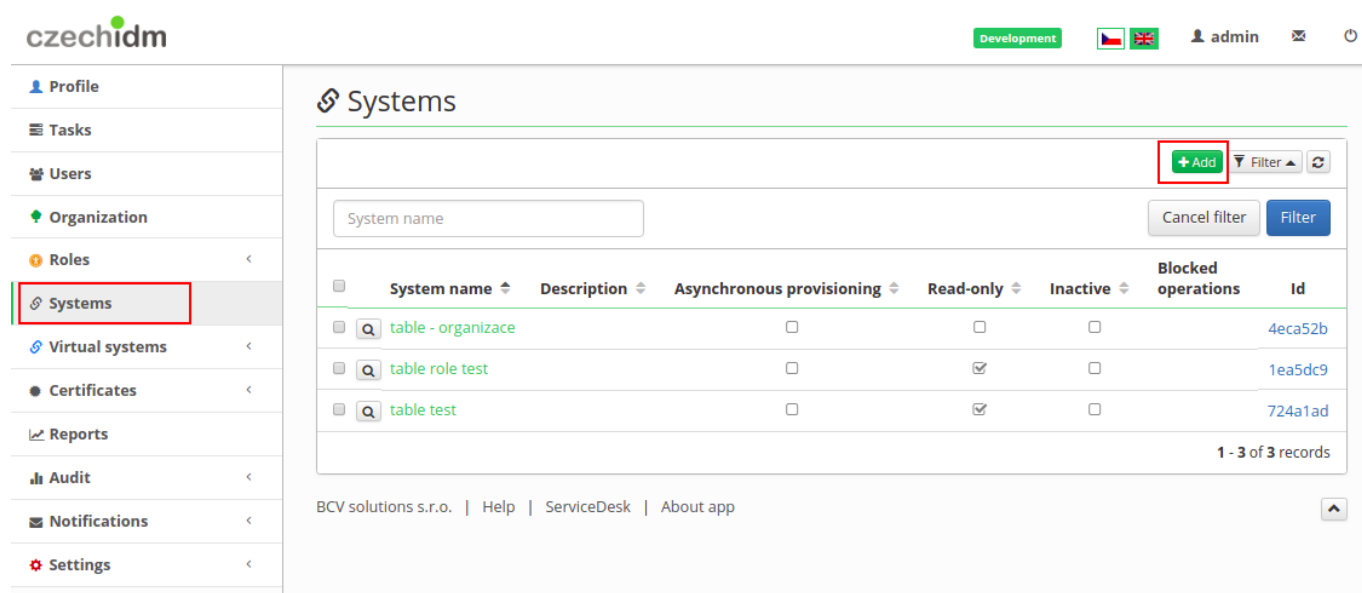
This tutorial is intended as a guide for administrators that want to provision roles from CzechIdM to Ldap.

You will learn

- how to connect an Ldap system for role provisioning
- how to propagate just those roles we want

## Create system

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



The screenshot shows the CzechIdM web interface. On the left, a sidebar contains navigation links: Profile, Tasks, Users, Organization, Roles, **Systems** (highlighted with a red box), Virtual systems, Certificates, Reports, Audit, Notifications, and Settings. The main area is titled 'Systems' and features a '+ Add' button (highlighted with a red box) and a 'Filter' button. Below the button is a search bar labeled 'System name'. A table lists three existing systems:

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

At the bottom right of the table, it says '1 - 3 of 3 records'. The footer of the interface includes '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 LdapConnector

Základní informace

Konfigurace

Brzda provisioningu

Účty na systému

Entity na systému

Schéma systému

Mapování atributů

Role

Synchronizace

Provisioning

## Nastavení konektoru

net.tirasa.connid.bundles.ldap.LdapConnector (connid)

Test konektoru

**Host**

localhost

The name or IP address of the host where the LDAP server is running.

**TCP Port**

1389

TCP/IP port number used to communicate with the LDAP server. The default is 389.

☒ SSL

Select the check box to connect to the LDAP server using SSL. The default is "false".

**Failover Servers (multi)**

List all servers that should be used for failover in case the preferred server fails. If the preferred server fails, JNDI will connect to the next available server in the list. List all servers in the form of "ldap://ldap.example.com:389/", which follows the standard LDAP v3 URLs described in RFC 2255. Only the host and port parts of the URL are relevant in this setting.

**Principal**

uid=admin,ou=system

The distinguished name with which to authenticate to the LDAP server.

**Password**

\*\*\*\*\*

Password for the principal.

**Base Contexts (multi)**

ou=groups,ou=system

One or more starting points in the LDAP tree that will be used when searching the tree. Searches are performed when discovering users from the LDAP server or when looking for the groups of which a user is a member.

On this page fill in these important values:

- ## Connector's mapping

- Základní informace

Konfigurace

Brzda provisioningu

Účty na systému

Entity na systému

Schéma systému

Mapování atributů

Role

Synchronizace

Provisioning

Schéma systému

Generovat schéma

Typy objektů na koncovém systému

+ Přidat

▼ Filtr

↺

Název objektu ↕	Pomocný objekt ↕	Je kontejnerem ↕	Id
_ACCOUNT_	<input type="checkbox"/>	<input type="checkbox"/>	87b60b2
_GROUP_	<input type="checkbox"/>	<input type="checkbox"/>	4ca6edf

1 - 2 z 2 záznamů

- Then in **Mapping** tab create new mapping - provisioning (\\_\\_GROUP\\_\\_ (Object name), Role (Entity type)).
- Now we will map just 2 attribute. Click on green add button like on picture below and this fill in:

Attribute in schema	Name	Attribute	IdM key
Transformation to system			
cn (__GROUP__)	name	identifier, entity	name
__NAME__ (__GROUP__)	name	entity	name
"cn="+attributeValue+",ou=groups,ou=system"			

dummyLDAP-roles

detail napojeného systému

Základní informace

Konfigurace

Brzda provisioningu

Účty na systému

Entity na systému

Schéma systému

**Mapování atributů**

Role

Synchronizace

Provisioning

Mapování atributů pro IdM entitu a typ operace

Detail

Správa účtů

Typ operace

Provisioning

Název mapování

prov - roles

Název objektu

\_\_GROUP\_\_

Typ IdM entity

Role

Zpět

Uložit a pokračovat

Namapované atributy

+ Přidat

Filtr

	Název	IdM klíč	Je identifikátorem	Atribut entity	Rozšířený atribut	Transfor. ze systému	Transfor. do systému	Id
	cn	name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0eb362e
	__NAME__	name	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	eda4d46

1 z 2 záznamů

## Make a script

At this point, provisioning of roles is active and if we create a role or re-save already existing, role will be provisioned to database. But we probably do not want propagate all of roles.

Select our system and then agenda **Mapping**. Select just created provisioninig mapping. On this page there is another tab **Account Management**. Here you can write a script or add one with green button **Insert script**. For example you can specify which roles will be propagated based on role name (roles\ a:roleToBeProvisioned) or if role is in specified role catalogue (roles\ a catalogue).

roles\_a System details

Basic information

Configuration

Provisioning brake

Accounts

Entities

Scheme

Mapping

Roles

Synchronization

Provisioning

Mapping of attributes for IdM entity and operation type

Detail

Account management

Can an account be created?

1String SYSTEM\_NAME = "role\_a";

2// Inserted script: scShouldBeProvisioned

3Description:

4null

5//

6scriptEvaluator.evaluate(

7scriptEvaluator.newBuilder()

8.setScriptCode('scShouldBeProvisioned')

9.addParameter(scriptEvaluator, scriptEvaluator)

10.addParameter(entity, entity)

Insert script

Account Management - allows you to disable the account creation (for that entity) on this system. The input parameter of this Groovy script is IdM entity 'entity', generated account identifier 'uid' and IdM system 'system'. Output value must be Boolean.TRUE or Boolean.FALSE!

Back

Save and continue

Beware: If you add this script after provisioning of a role. This script will not prevent future provisioning of this role. You have to remove role's account on this system. In agenda **Roles** on left menu you can find the role, click on magnifying glass. In tab **Accounts** you can see all accounts of this role (there could be more items, if role was synchronized from system or provisioned to more systems). Here if you remove account, role will be erased on end system. Future provisioning of the role to this system based on script mentioned above.

bcv:identity\_a:dvere

Role details

Basic information

More information

Role attributes

Business role

Incompatible roles

Role authorizers

Role catalogue

Permissions

Automatic roles

Users with role

Systems

Accounts

Accounts in systems

+ Add

Account identifier	System name	Owns account	Is protected from delete	Protected until	Id
bcv:identity_a:dvere	roles_a	<input checked="" type="checkbox"/>	<input type="checkbox"/>		ba24035

1 - 1 of 1 records

From:

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

Permanent link:

[https://wiki.czechidm.com/tutorial/adm/ldap\\_roles\\_provisioning](https://wiki.czechidm.com/tutorial/adm/ldap_roles_provisioning)

Last update:

2019/05/23 07:19

