

# Systems - DB: Roles provisioning

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

You will learn

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

## DB's Table

For this example I created simple table with just one column 'name' as varchar, which will be name of role and identifier.

## 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 a menu with items like Profile, Tasks, Users, Organization, Roles, and Systems. The 'Systems' item is highlighted with a red rectangle. The main content area is titled 'Systems' and features a table of existing systems. Above the table, there is a search bar and a '+ Add' button, which is also highlighted with a red rectangle. The table has columns for System name, Description, Asynchronous provisioning, Read-only, Inactive, Blocked operations, and Id. Three systems are listed: 'table - organize', 'table role test', and 'table test'. At the bottom of the table, it says '1 - 3 of 3 records'.

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

- Fill in name of a system. And click on **Save and continue**.
- In tab **Configuration** choose Database table connector

roles\_a detail napojeného systému

Základní informace

Konfigurace

Brzda provisioningu

Účty na systému

Entity na systému

Schéma systému

Mapování atributů

Role

Synchronizace

Provisioning

### Nastavení konektoru

Database Table Connector (connId) Test konektoru

**Name Quoting**

Select whether database column names for this resource should be quoted, and the quoting characters. By default, database column names are not quoted (None). For other selections (Single, Double, Back, or Brackets), column names will appear between single quotes, double quotes, back quotes, or brackets in the SQL generated to access the database.

**Host**

localhost

Enter the name of the host where the database is running.

**Port**

5432

Enter the TCP port number the database server is listening on.

**User**

ldmadmin

Enter the name of the mandatory Database user with permission to account table.

**User Password**

\*\*\*\*\*

Enter a user account password that has permission to access accounts table.

**Database**

jdbCTest

Enter the name of the database on the database server that contains the table.

**Table**

roles\_a

Enter the name of the table in the database that contains the accounts.

**Key Column**

name

This mandatory column value will be used as the unique identifier for rows in the table.

## Connector configuration

On this page fill in these important values:

- **Host** - IP address of ad server or hostname
- **Port** - on this port will server listen
- **User** - with this username connector will connect to the DB system, this user has to have enough rights to write.
- **User password** - password of the "user" account
- **Database** - name of database, we want to connect
- **Table** - name of table
- **Key column** - column as an identifier in table
- **JDBC Driver** - it is based on type of database, e.g. for Postgres it is "org.postgresql.Driver"
- **JDBC Connection URL** - it is based on type of database

## 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.

roles\_a System details

Basic information

Configuration

Provisioning brake

Accounts

Entities

Scheme

Mapping

Roles

Synchronization

Provisioning

System scheme

Generate scheme

Object types in system

+ Add

Filter

Object name	Auxiliary	Container	Id
__ACCOUNT__			d792d21

1 - 1 of 1 records

- Then in **Mapping** tab create new mapping - provisioning (\\\_\\\_ACCOUNT\\\_\\\_ (Object name), Role (Entity type)). {If you are using Active Directory, select \\\_\\\_GROUP\\\_\\\_ as Object name }
- Now we will map just 1 attribute. Click on green add button like on picture below and this fill in:

Attribute in schema	Name	Attribute	IdM key
__NAME__ (__ACCOUNT__)	name	identifier, entity	name

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

Operation type

Provisioning

Mapping name

prov

Object name

\_\_ACCOUNT\_\_

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	Id
__NAME__	name						b1e6e66

1 - 1 of 1 records

# 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 provisioning 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)

roles\_aSystem details

Basic information

Configuration

Provisioning brake

Accounts

Entities

Scheme

Mapping

Roles

Synchronization

Provisioning

Mapping of attributes for IdM entity and operation type

DetailAccount management

Can an account be created?

String SYSTEM\_NAME = "role\_a";

// Inserted script: scShouldBeProvisioned

/\* Description:

null

\*/

scriptEvaluator.evaluate(

scriptEvaluator.newBuilder()

.setScriptCode('scShouldBeProvisioned')

.addParameter('scriptEvaluator', scriptEvaluator)

.addParameter('entity', entity)

.addParameter('uid', uid)

)

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!

BackSave and continue

or if role is in specified role catalogue (roles\\_a catalogue).

```
// Inserted script: IsRoleInCatalogue
/* Description:
Is role in the catalogue? Script return "true" if given (input parameter
"role") IdmRoleDto is in supported catalogue (given in the parameter
"catalogueCode"). Search is recursively.
*/
scriptEvaluator.evaluate(
    scriptEvaluator.newBuilder()
        .setScriptCode('IsRoleInCatalogue')
        .addParameter('scriptEvaluator', scriptEvaluator)
        .addParameter('uid', uid)
        .addParameter('entity', entity)
        .addParameter('system', system)
        .addParameter('role', entity)
        .addParameter('catalogueCode', '123') // '123' represents a catalog
code
        .build());
```

Beware: If you add first (roles\\_a:roleToBeProvisioned) 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:dvereRole 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

https://wiki.czechidm.com/

Printed on 2024/03/07 04:51

From:

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

Permanent link:

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

Last update: **2020/08/13 15:47**

