Cross domains

ad, provisioning, system

What are cross-domains?

By **cross-domains**, we mean a **set of external systems** that are linked and share, for example, the same **permissions**.

A typical example of a cross-domains group might be the linking of multiple domains in **MS Active Directory**. In this case, we can have several **AD domains that share groups with each other**. That is, within one AD domain it is possible to assign users to groups from another AD domain. The groups are thus shared across the entire group of domains (cross-domains). From the end user's perspective, **the systems thus appear to have the same set of groups**.

The goal of cross-domains in **CzechIdM** is to connect systems as described in the example above and to allow to simulate the same property, i.e. that individual group can be assigned to any system in the same cross-domain group.

A user in CzechIdM can assign a role to all or only one system **in the cross-domain group**.

How to use cross-domains in CzechIdM?

To properly use cross-domains in **CzechIdM**, we need three basic things:

1. **Create systems** connecting systems in each domain.
2. Configure the **cross-domain group of systems**.
3. Create and configure **no-login roles**.

Create systems

The first step is to create systems and connect them to individual domains. If we have a group consisting of **three domains**, then we need to create **three systems** that will provision user accounts to each of the domains (each system will connect users from one domain).

Currently, **CzechIdM supports cross-domains only for MS AD**. For proper connection, it is necessary to use the **WIN-RM connector** in the correct version and setup.

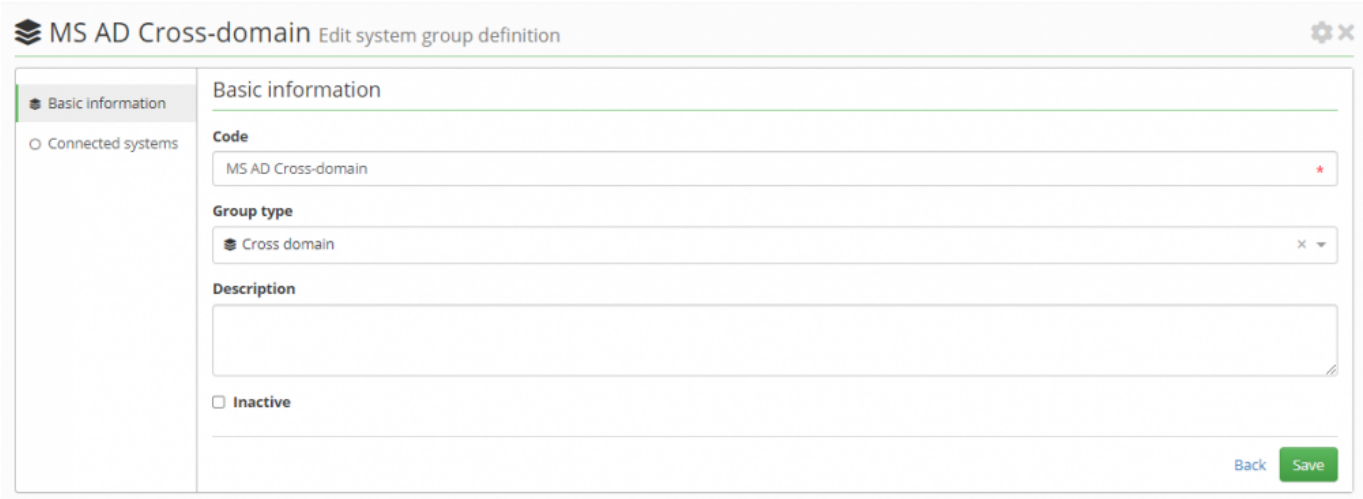
The detailed configuration of the connector and its scripts is described here: WinRM + AD Connector

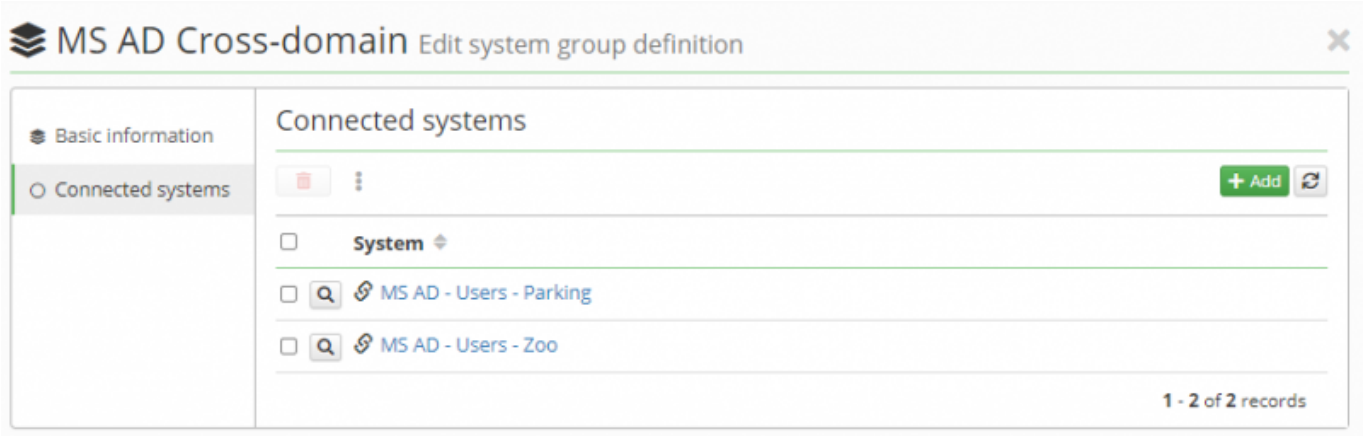
Groups of systems

After you create a domain system, you must create a **cross-domain group of these systems in IdM**.

You can create a **new group in the system group management agenda**. The group must be of type '**Cross-domain**'.

You can then add the systems you created to this group. For each system, you must select the **attribute that manages the group**. In an **MS AD** environment this will typically be the '**ldapGroups**' attribute.





No login roles

The last step in setting up the cross-domain environment in IdM is to **create and set up the appropriate roles**.The goal is to **create roles that represent groups in each domain**.

It is not necessary to create the roles manually, but we can use **group synchronization** to do so. This means that for each domain that we will create a system for role/group synchronization. This synchronisation will create roles corresponding to groups, but it will also directly create a connection to that system in IdM. This connection will assign a group identifier (typically the **group DN**) within

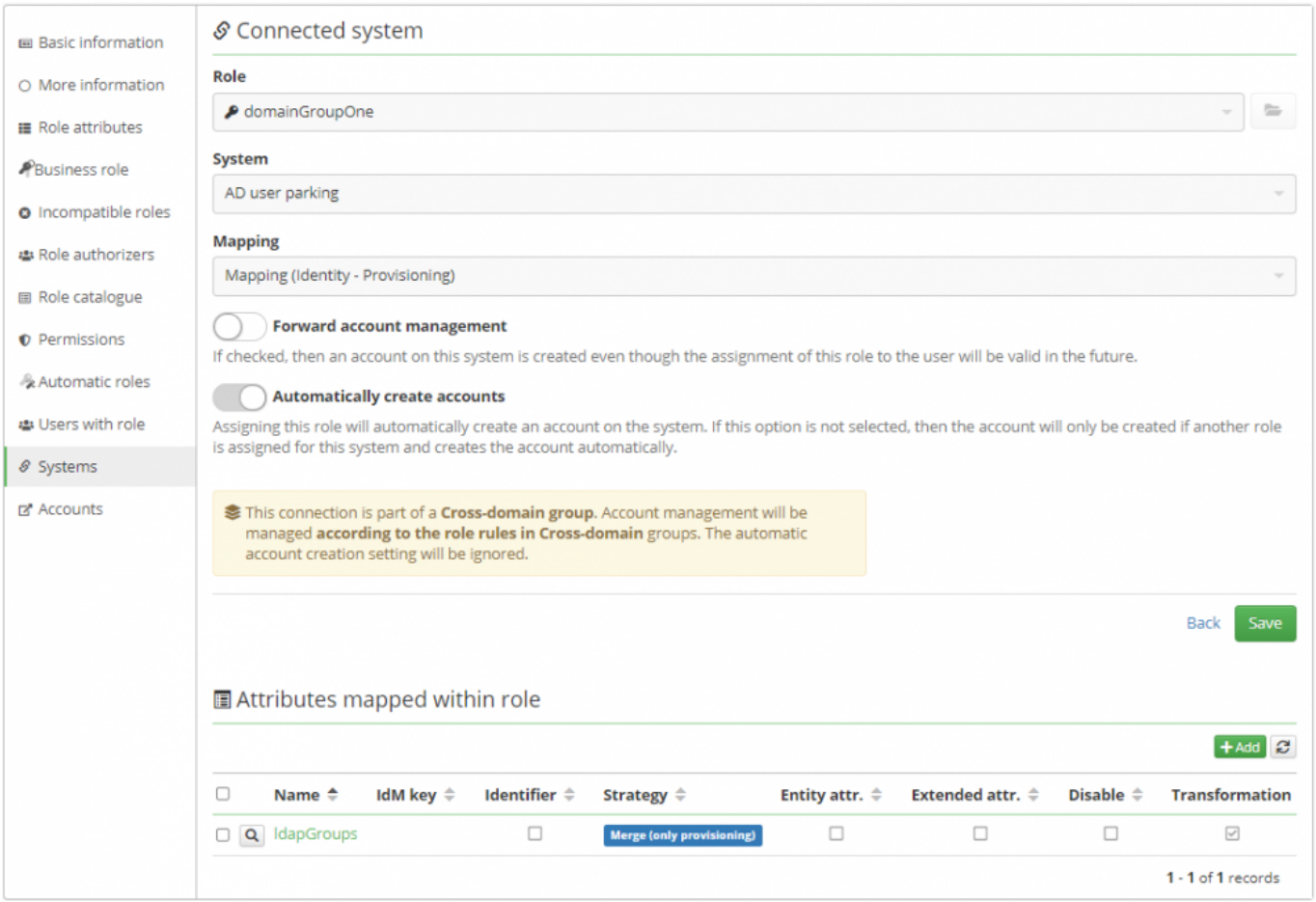
the attribute that manages the groups in the domain (typically '**ldapGroups**').

Roles created in this way will contain a link to the domain from which the group originates. However, to function properly within a cross-domain, we need to create links to other domains as well. So the goal is for each role to link to all domains while assigning an **identifier (DN)** to the group's managing attribute (**ldapGroups**). The value of the group identifier (DN) **will be the same in all connections to that role**!

If you make the settings described above, the role should switch to **no-login mode**. No-login mode means that assigning such a role to a user will **not create an account** on the system. An account will only be created if the user has another role assigning an account. Such a role is then called a **login-role**, which is a common system-assigning role from the IdM perspective.

The prerequisite for a role to become a no-login role is that the connected system must be part of some **active group of systems with a cross-domain type**, and also that this role **overloads the same merge attribute** as is used in the group.

If the role is in **no-login mode** for cross-domains, then the **information box is displayed on that system connection**:



Assing no-login role to only one domain

In the previous step, we described what cross-domain **no-login** roles are. We already know that if we assign such a role to a user, then no account will be created on the end system.

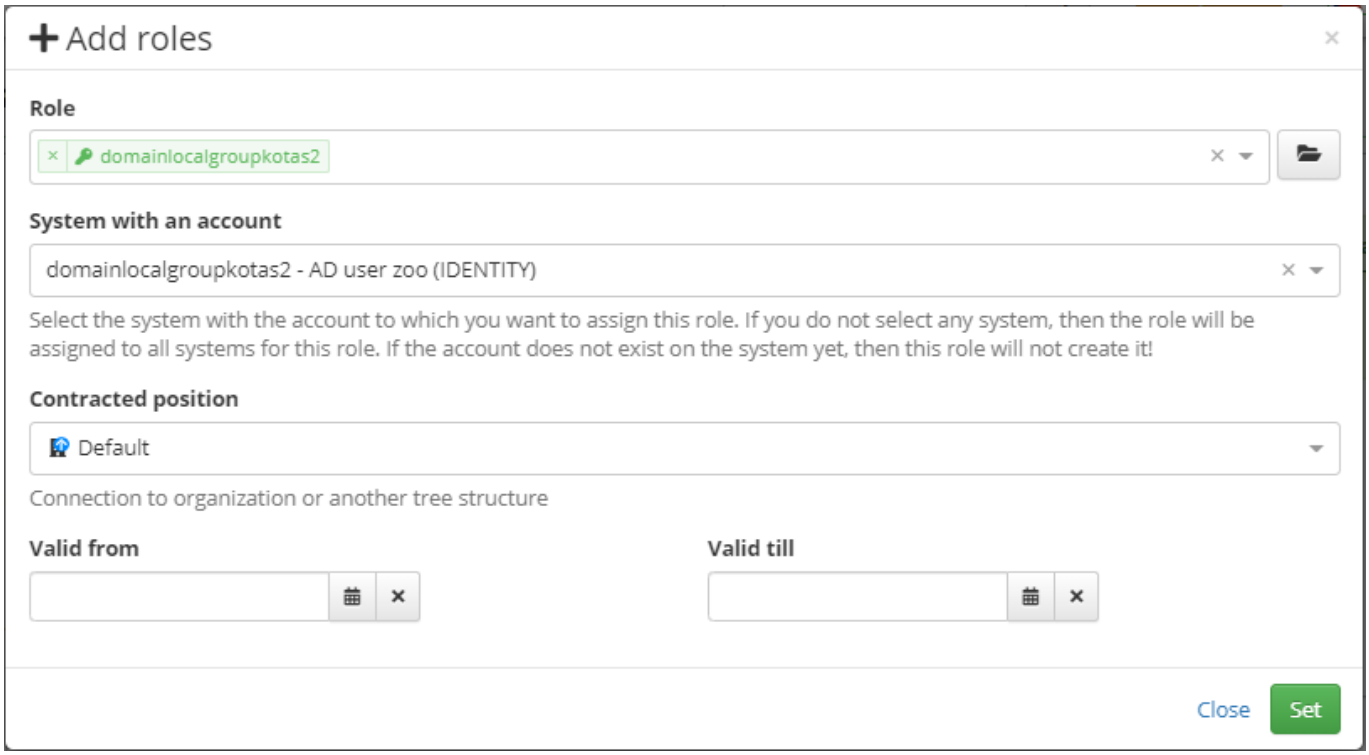
Now let's have a situation where we have a no-login role that assigns a group to **three domains**. If

we assign this role to a user who also has login roles for all three domains, then the group will be assigned to all existing accounts.

This behavior can be a problem when we want to assign a group to only one account on one of the domains.

As a workaround for this situation, a **selection of available systems** (domains) that the role connects to has been added to the details of the new role request. This selection basically acts as a filter. That is, if nothing is selected (the default state), the group will be assigned to all of the user's domains. If we select only one domain, then the group will only be assigned to that domain's account.

This selection will only be displayed for no-login roles in a cross-domain group and if the role contains more than one linked domain.



Future improvements

Group synchronization **could create a merge attribute connection not only to the system from which it is synchronized, but also** to all other systems in the cross-domain group.

Group synchronization **could assign roles to users not only according to the state on the system from which**

the group originates, but also from all other systems in the cross-domain group.

Limitations

No-login connections cannot overload the primary mapping attribute (UID)!

Adding or removing too many groups at once is not supported. Lenght limitation of environment variable on Windows is 8 191 characters so if combination of all added and removed group's DNs plus comas, doublequotas and the script itself is longer than that cmd.exe just ignores it. The result is no script is being run and no error or exception ocures. Relatively safe is to add or remove about 50-100 groups at once.