Role Autoassignment

MidPoint 3.7 and later

This feature is available only in midPoint 3.7 and later. Partial implementation by using object template was available since midPoint 3.2.

Introduction

There are many ways how to assign roles, orgs and services. Many roles are assigned using a manual or partially-manual process. But there is almost always some degree of automation when at least some roles are assigned to users according to fixed rules. This page describes the mechanism to automatically assign roles in midPoint.

Autoassignment Conditions in Roles

Perhaps the most convenient way to automatically assign a role is to use autoassignment condition in a role:

Autoassignment mapping in a role

```
<role>
    <name>Intern</name>
    ...
    <autoassign>
        <enabled>true</enabled>
        <focus>
                        <selector>. <!-- Since 4.2 -->
                                <type>UserType</type>
                        </selector>
            <mapping>
                <source>
                    <path>employeeType</path>
                </source>
                <condition>
                    <script>
                        <code>employeeType == 'intern'</code>
                    </script>
                </condition>
            </mapping>
        </focus>
    </autoassign>
</role>
```

The role above will be automatically assigned to any user that has property `employeeType` set to `intern`. As all midPoint mapping even this mapping is relativistic. If user becomes an intern (the `employeeType` property is changed) then the role is automatically assigned. When the user stops being an intern the role is unassigned.

See Role Autoassign Configuration page for more details.

Autoassignment in Object Template

Autoassignment in roles is simple and elegant, but it has several disadvantages. However, even complex role autoassignment cases can be handled by using object template. The roles can be automatically assigned by using object template mappings:

Autoassignment in object template

```
<objectTemplate>
    <name>User Template</name>
    ...
    <mapping>
        <authoritative>true</authoritative>
        <source>
            <path>organization</path>
        </source>
        <expression>
            <assignmentTargetSearch>
                <targetType>RoleType</targetType>
                <filter>
                    <q:equal>
                        <q:path>name</q:path>
                        <expression>
                            <path>$organization</path>
                        </expression>
                    </q:equal>
                </filter>
            </assignmentTargetSearch>
        </expression>
        <target>
            <path>assignment</path>
        </target>
    </mapping>
    ...
<objectTemplate>
```

The mapping above will create assignment for any role which name matches with a value of `organization` user property. Therefore a single mapping can be used to assign a wide range of roles.

See Object Template page for more details about object template mechanism. The Expression page describes the details of `assignmentTargetSearch` expression evaluator that is frequently used for this purpose.

Roles Within Roles

There is sometimes a need to assign one role when another role is assigned. As midPoint has full support for role hierarchy this is easily done by nesting the roles inside. If there is additional condition when the nested role is to be applied then the conditional role approach can be used. There are many ways how to implement this functionality.

Sometimes there is a need to unassign a role when another role is assigned. Role exclusion mechanism may be used to implement this approach, as illustrated by Radio Button Roles example. However, care must be taken if this is to be combined with role autoassignment as it is easy to set up a conflicting policies. MidPoint is a thorough system and it does not like conflicting policies.

See Also

- Role Autoassign Configuration
- Object Template
- Expression
- Advanced Hybrid RBAC