SailPoint

Developer Days2023

</title>

Impact of an assignment rule change

</title>

speaker: Ünsal Ilhan;
title: Senior IAM Consultant;
company: iC Consult Switzerland;

Agenda

- About me — Ünsal Ilhan, Senior IAM Consultant
- Motivation
- Required Configurations
- Artefacts (XML, Java)
- Live Demo
- Possible Improvements
- Topics to keep in mind
- Q/A & Comments

About me

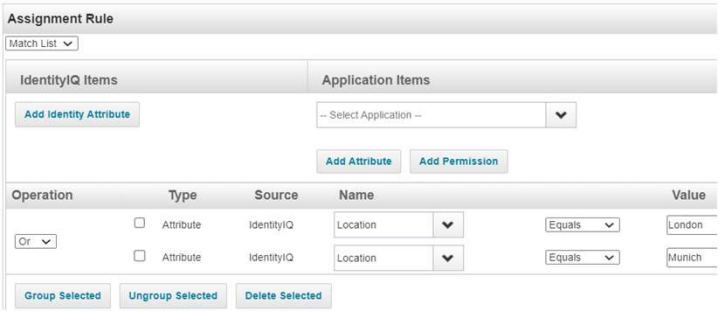
- Since 8 years at iC Consult Switzerland
- Identity IQ & IdentityNow, (FAM)
- Role: Solution Architect, Project Lead & CoE for SailPoint in Switzerland.
- Married, 44 years old.
- Love Basketball and Travelling

- **iC Consult** Headquarter in Germany, 25+ years experience
- Vendor-independent consultancy and system integrator for IAM solutions
- Portfolio covers from advisory, design to implementation/integration & managed services
- 800+ employees in more than 12 countries

Motivation

- **Customer changed the logic and used „and“ operation instead of „or“**

  -> So role was deprovisioned for hunderts of accounts.



- Changing an assignment rule on production could be fatal
  - Typcial mistakes: typo, missing brackets/quote, incorrect use of and or operations, ...

- No motivation to test it on lower environments.
  - Time pressure: changes are sometimes required immediately

- Lower environments seldom have production data or same state

„RoleAssignmentImpact“ Feature (as Plugin)

Done as Plugin for a fast delivery as showcase.

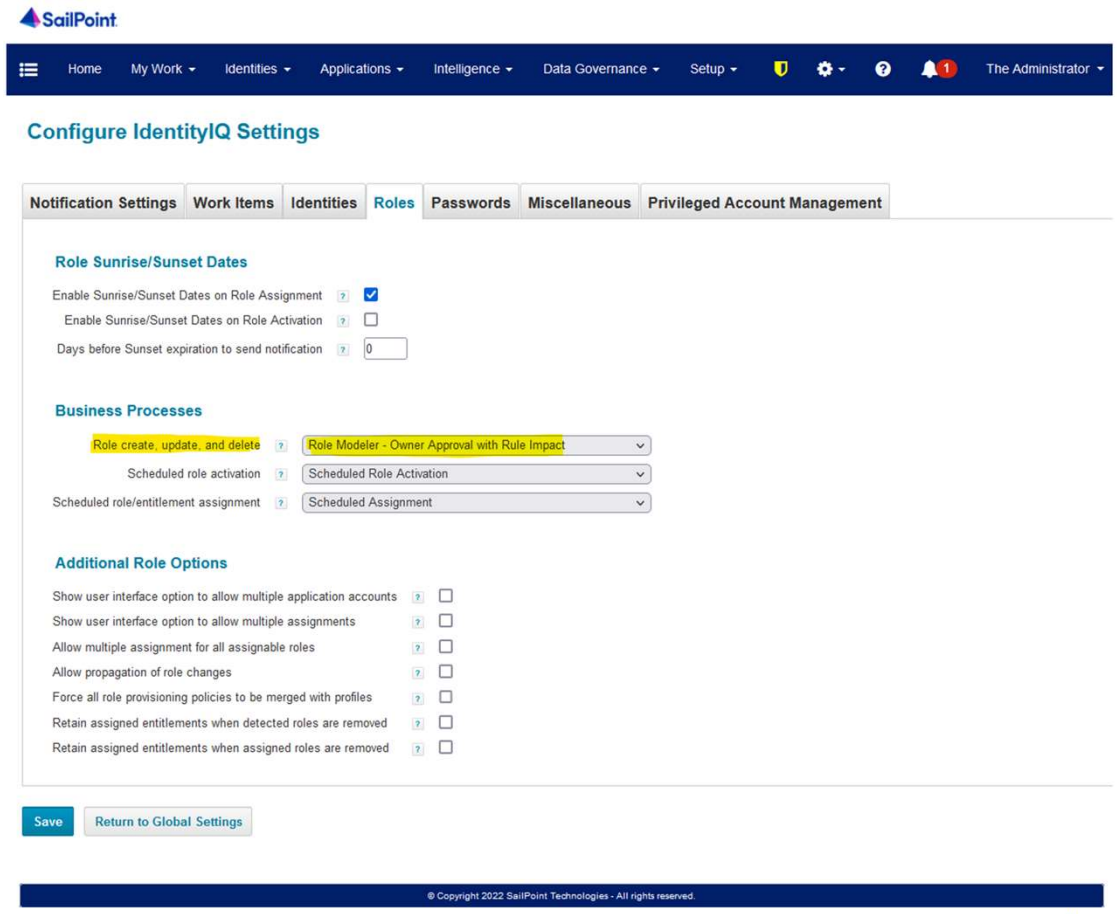
- Tested on IIQ 8.2 and 8.3
- Deinstallation -> Removal of extensions (Workflow)
- Reinstallation -> Requires reconfiguration (setting Workflow)

So better to implement it as WorkflowLibrary and Workflow extension

Role Configuration

- Custom Business Process:
- “Role Modeler - Owner Approval with Rule Impact”

- Extends the original Workflow
- “Role Modeler - Owner Approval”
- with 2 additional steps.



Artefacts: Workflow extension

1. Step „prepareRuleImpact“

```
    <Transition to="prepareRuleImpact"
                when="script:new customer.iiq.RuleOfRoleImpactLibrary().isDisplayImpactRequired(wfcontext)"/>
    <Transition to="Check Approvals" when="impactAnalysisOwner == unbound || impactAnalysisOwner == null"/>
    <Transition to="Impact Analysis"/>
</Step>

<Step name="prepareRuleImpact"
      action="script:new customer.iiq.RuleOfRoleImpactLibrary().getImpactRendered(wfcontext)"
      resultVariable="impactOfRoleChangeRendered">
    <Arg name="headerNames">
        <value>
            <List>
                <String>Name</String>
                <String>Location</String>
                <String>State</String>
            </List>
        </value>
    </Arg>
    <Arg name="attributeNames">
        <value>
            <List>
                <String>name</String>
                <String>location</String>
                <String>lifecycleState</String>

            </List>
        </value>
    </Arg>
    <Arg name="sortAttributes">
        <value>
            <List>
                <String>location</String>
                <String>lifecycleState</String>

            </List>
        </value>
    </Arg>
    <Transition to="Rule change approval"/>
</Step>
```

2. Step „Rule change approval“

```
<Step icon="Approval" name="Rule change approval">
    <Approval mode="any" name="Rule change approval" owner="ref:launcher"
              send="impactOfRoleChangeRendered, approvalObject">
        <Arg name="launcher" value="ref:launcher"/>
        <Arg name="approvalObject" value="ref:approvalObject"/>
        <Arg name="impactOfRoleChangeRendered" value="ref:impactOfRoleChangeRendered"/>
        <Arg name="workItemName" value="ref:workitemName"/>
        <Arg name="workItemDescription" value="ref:workItemName"/>
        <Form name="Rule change approval">
            <Attributes>
                <Map>
                    <entry key="pageTitle" value="$(workItemName)"/>
                </Map>
            </Attributes>
            <Section label="Rule" type="datatable">
                <Field name="Actual Rule">
                    <Script>
                        <Source><![CDATA[
                            import sailpoint.object.Bundle;
                            String summary = "";
                            if (approvalObject.getId() != null) {
                                Bundle bundle = context.getObjectById(Bundle.class, approvalObject.getId());
                                if (bundle != null && bundle.getSelector() != null) {
                                    summary = bundle.getSelector().generateSummary();
                                }
                            }
                            return summary;
                        ]]></Source>
                    </Script>
                </Field>
                <Field name="New Rule">
                    <Script>
                        <Source><![CDATA[
                            String summary = "";
                            if (approvalObject.getSelector() != null) {
                                summary = approvalObject.getSelector().generateSummary();
                            }
                            return summary;
                        ]]></Source>
                    </Script>
                </Field>
            </Section>
            <Section label="Impact" type="text">
                <Field>
                    <Attributes>
                        <Map>
                            <entry key="contentIsEscaped" value="true"/>
                        </Map>
                    </Attributes>
                    <Script>
                        <Source><![CDATA[
                            return impactOfRoleChangeRendered;
                        ]]></Source>
                    </Script>
                </Field>
            </Section>
            <Button action="next" label="Apply Impact"/>
            <Button action="back" label="Reject Impact"/>
        </Form>
    </Approval>
    <Arg name="workitemName"
         value="script:&amp;quot;Rule confirmation for Role: &amp;quot; + approvalObject.getDisplayableName()"/>
    <Transition to="stop" when="!approved"/>
    <Transition to="Check Approvals" when="impactAnalysisOwner == unbound || impactAnalysisOwner == null"/>
    <Transition to="Impact Analysis"/>
</Step>
```

Artefacts: Java Code

Step Transition check

```
public boolean isDisplayImpactRequired(WorkflowContext wfc) {

                ...

    if (existingBundle != null) {

        RoleLifecycler cycler = new RoleLifecycler(context);

        BundleDifference diffs = cycler.diff(existingBundle, newBundle);

        if (diffs.getSelectorDifference() != null) {

            return true;

        }

    }

                ...
}
```

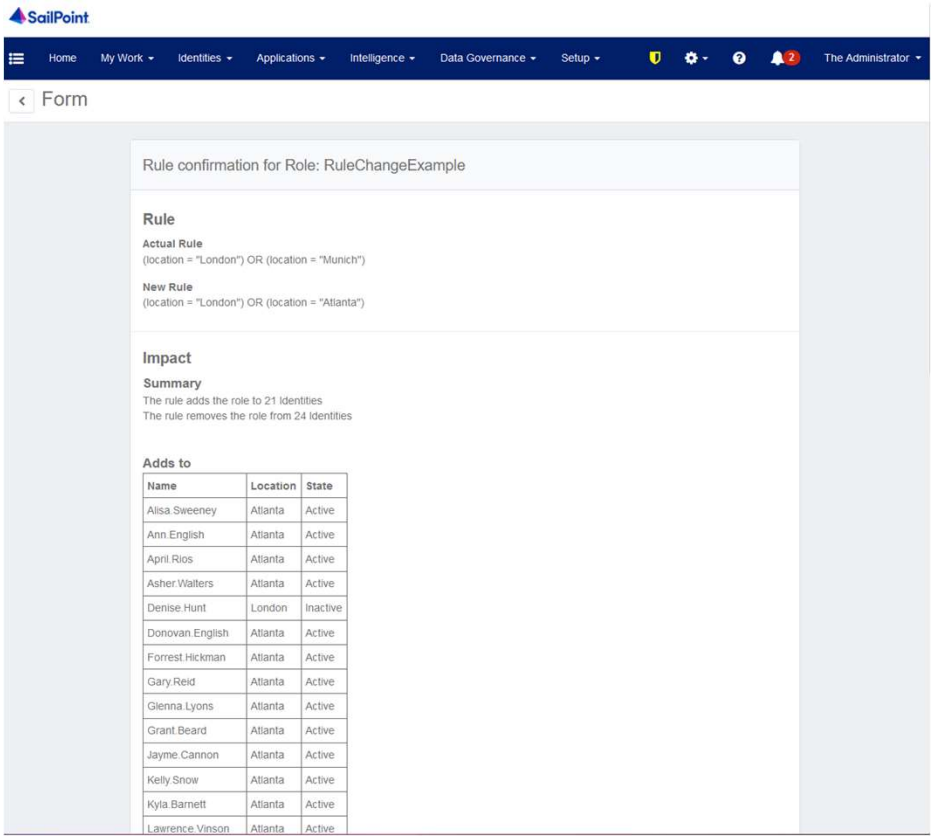
Approval rendering

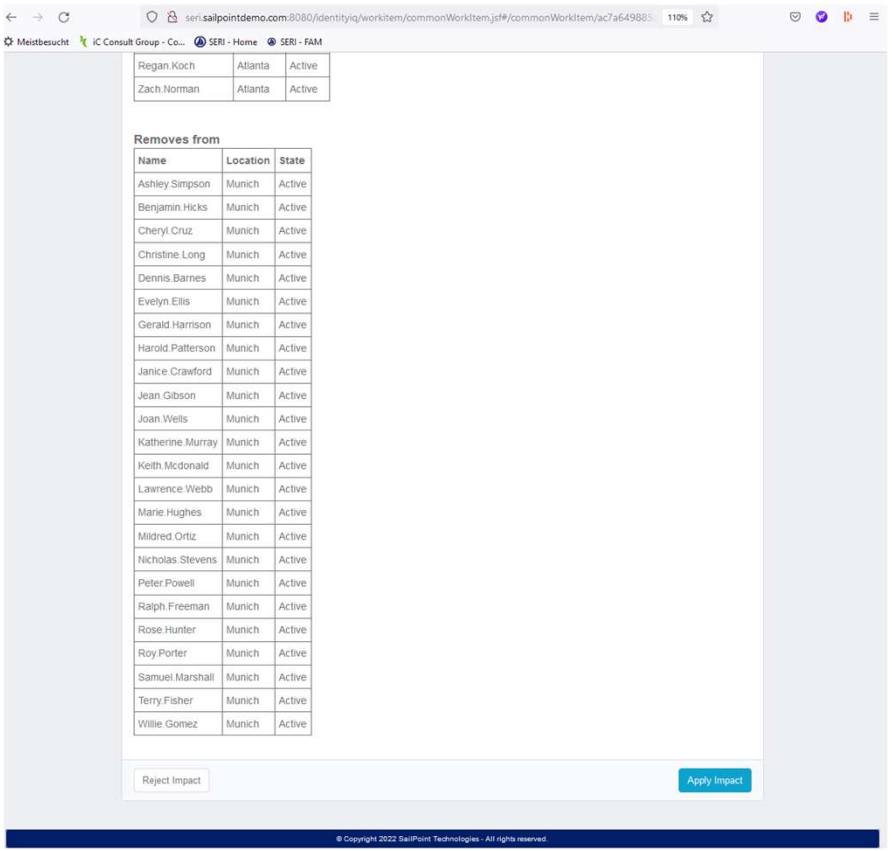
```
public String getImpactRendered(WorkflowContext wfc) throws GeneralException {
            ...
    //get Identity id's that are currently assigned based on IdentityEntitlments
    List<String> currentlyAssignedTo = getIdentityIdsThatAreCurrentlyAssigned(context, newBundle);

    //use Matchmaker to evaluate IdentitySelector for all Identities: matchmaker.isMatch(selector, identity)
    List<String> willBeAssignedTo = getIdentityIdsThatWillBeAssigned(context, newBundle);

    // returns the Impact as HTML tables: 1. role will be added to, 2.role will be removed from.
    // difference is evalueated from above 2 lists.
    // for sorting apaches ImmutablePair is used. Left side the sort values and right side the HTML table data
    return getImpactRendered(context, currentlyAssignedTo, willBeAssignedTo, headers, attributes, sortAttributes);
}
```

Demo on IdentityIQ Environment





Improvements & topics to keep in mind

- Improvements
  - Use SQL statement instead of QueryOptions in case of performance issues
  - Move Java code to Workflow Library

- Keep in mind

  Only changes made directly via the role editor triggers the impact evaluation.

  -> Any changes deployed from GIT are not detected

  -> Any changes via Debug to

  - Populations, Rules, Scripts, Filter, MachtList

  are not detected

Questions/Answers
Comments

[Thank you!]

speaker: Ünsal Ilhan;
title: Senior IAM Consultant;
company: iC Consult Switzerland;