



</title>

# Impact of an assignment rule change

</title>

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



# Agenda

**About me**

Ünsal İlhan, 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 hundreds 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

Operation	Type	Source	Name	Value
Or	<input type="checkbox"/> Attribute	IdentityIQ	Location	London
	<input type="checkbox"/> Attribute	IdentityIQ	Location	Munich

# „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.



**SailPoint**

Home My Work Identities Applications Intelligence Data Governance Setup 1 The Administrator

### Configure IdentityIQ Settings

Notification Settings Work Items Identities **Roles** Passwords Miscellaneous Privileged Account Management

#### Role Sunrise/Sunset Dates

Enable Sunrise/Sunset Dates on Role Assignment ☒

Enable Sunrise/Sunset Dates on Role Activation ☐

Days before Sunset expiration to send notification

#### Business Processes

Role create, update, and delete **Role Modeler - Owner Approval with Rule Impact**

Scheduled role activation Scheduled Role Activation

Scheduled role/entitlement assignment Scheduled Assignment

#### Additional Role Options

Show user interface option to allow multiple application accounts ☐

Show user interface option to allow multiple assignments ☐

Allow multiple assignment for all assignable roles ☐

Allow propagation of role changes ☐

Force all role provisioning policies to be merged with profiles ☐

Retain assigned entitlements when detected roles are removed ☐

Retain assigned entitlements when assigned roles are removed ☐

**Save** Return to Global Settings

© Copyright 2022 SailPoint Technologies - All rights reserved.

# Artefacts: Workflow extension



## 1. Step „prepareRuleImpact“

```
<Transition to="prepareRuleImpact"
  when="script:new customer.iiq.RuleOfRoleImpactLibrary().getDisplayImpactRequired(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>
```

© 2023 SailPoint Technologies, Inc. All rights reserved.

## 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:quote;Rule confirmation for Role: {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) {  
        RoleLifecycle cyler = new RoleLifecycle(context);  
        BundleDifference diffs = cyler.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 evaluateated 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

SailPoint

Home My Work Identities Applications Intelligence Data Governance Setup The Administrator

< Form

Rule confirmation for Role: RuleChangeExample

**Rule**

**Actual Rule**  
(location = "London") OR (location = "Munich")

**New Rule**  
(location = "London") OR (location = "Atlanta")

**Impact**

**Summary**  
The rule adds the role to 21 Identities  
The rule removes the role from 24 Identities

**Adds to**

Name	Location	State
Alisa Sweeney	Atlanta	Active
Ann English	Atlanta	Active
April Rios	Atlanta	Active
Asher Walters	Atlanta	Active
Denise Hunt	London	Inactive
Donovan English	Atlanta	Active
Forrest Hickman	Atlanta	Active
Gary Reid	Atlanta	Active
Glenna Lyons	Atlanta	Active
Grant Beard	Atlanta	Active
Jayne Cannon	Atlanta	Active
Kelly Snow	Atlanta	Active
Kyla Barnett	Atlanta	Active
Lawrence Vinson	Atlanta	Active

ser.sailpointdemo.com:8080/identityiq/workitem/commonWorkItem.jsf#/commonWorkItem/ac7a649885 110%

Meistbesucht IC Consult Group - Co... SERI - Home SERI - FAM

Regan Koch	Atlanta	Active
Zach Norman	Atlanta	Active

**Removes from**

Name	Location	State
Ashley Simpson	Munich	Active
Benjamin Hicks	Munich	Active
Cheryl Cruz	Munich	Active
Christine Long	Munich	Active
Dennis Barnes	Munich	Active
Evelyn Ellis	Munich	Active
Gerald Harrison	Munich	Active
Harold Patterson	Munich	Active
Janice Crawford	Munich	Active
Jean Gibson	Munich	Active
Joan Wells	Munich	Active
Katherine Murray	Munich	Active
Keith McDonald	Munich	Active
Lawrence Webb	Munich	Active
Marie Hughes	Munich	Active
Mildred Ortiz	Munich	Active
Nicholas Stevens	Munich	Active
Peter Powell	Munich	Active
Ralph Freeman	Munich	Active
Rose Hunter	Munich	Active
Roy Porter	Munich	Active
Samuel Marshall	Munich	Active
Terry Fisher	Munich	Active
Willie Gomez	Munich	Active

Reject Impact Apply Impact

© Copyright 2022 SailPoint Technologies - All rights reserved.



# 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



```
if localVarHTTPResponse.StatusCode >= 300 {  
    newErr := &GenericOpenAPIError{  
        body: localVarBody,  
        error: localVarHTTPResponse.Status,  
    }  
}
```

# Questions/Answers Comments

```
if localVarHTTPResponse.StatusCode == 400 {  
    var v ErrorResponseDto  
    err = a.client.decode(&v, localVarBody, localVarHTT  
    if err != nil {  
        newErr.error = err.Error()  
        return localVarReturnValue, localVarHTTPResp  
    }  
}
```



**[Thank you!]**

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