7.2: Solution Documentation and Authorization for Business Process Operations (BPOps) Setup

SAP Solution Manager 7.2 SP3, SAP SE, November 2016
Objective

After reading the slides you will:

• Understand how you can use Authorizations to ensure that in the Operation Branch in your Solution Documentation only Business Process Operations relevant changes are done.
Content

- Introduction to BPOps Integration with Solution Documentation
- Usage of the Operation Branch for setting up BPOps (Alerting and Analytics Objects) in Solution Documentation
- Template User for Setup of Business Process Operations – without restrictions in Solution Documentation
- How to restrict activities in Solution Documentation via Authorization Areas and Groups to those relevant for Business Process Operations
Introduction

Introduction to BPOps Integration with Solution Documentation
In Solution Manager 7.2 the setup of Business Process Operations is done in the Solution Documentation, meaning alerting objects and analytical key figures are added to the implemented processes in the solution documentation.

By setting up monitoring, the implemented processes are not changed (e.g. regarding their configuration), but data is collected, which enriches the documented process with monitoring information.
Usage of the Operation Branch

Adding Alerting and Analytics Objects to Solution Documentation via the Operation Branch
Solution Documentation: Version Management via Branches

Solution Documentation manages different versions of documentation using a branch concept, where the **production branch** contains the documentation of the currently productive processes, points to production systems and is **not changeable**.

The **maintenance branch** shall be used for minor changes. It points to the maintenance and test systems and changes can be (but do not have to be) controlled by ChaRM. For major changes, development branches can be defined, e.g. for implementation projects.

Business Process Monitoring usually focuses on productive business processes. It does not change the implemented business processes, but only collects monitoring information using the Monitoring and Alerting Infrastructure (MAI) which is not ChaRM enabled. Best practice is to change the monitoring configuration in the **operation branch**.

→ By defining an **operation branch** and restricting the actions within the **operation branch** to those needed for monitoring setup, the Operations team will be able to configure monitoring for productive processes, but not be able to change the process documentation.
Solution Documentation – Example for Branch Setup

Figure 19: Branch setup for S/4HANA and major release development
SAP recommends the creation of an Operation branch (branch type “Operation”) in the Solution Administration for the configuration and consumption of BPMon and BPAnalytics.
Template User for Setup of Monitoring Objects

Template User for Setup of Business Process Operations – without restrictions in Solution Documentation
In Solution Manager Configuration a template BPO Admin User can be found that has all necessary roles, including SAP_SM_SL_ADMIN, i.e. the user is not restricted regarding solution documentation activities.
Authorizations in Solution Documentation and Monitoring Setup

• Monitoring focuses on core business processes, thus only a part of the solution documentation is relevant for BPOps and in solution documentation only some activities are needed for setting up monitoring.

• Solution Documentation offers to use **Authorization Areas** in order to restrict the visibility of structures (e.g. business processes, folders) and to use **Authorization Groups** in order to restrict the creation and change of objects.

• Process Monitoring is usually set up by **Business Process Operations experts** (i.e. not by Solution Documentation experts). BPMon information (alerts and metrics) are consumed by members of the business process operations or **Operations Control team**.

Thus, these users need to have only special Solution Documentation authorizations, not the full range of Solution Documentation authorizations.
Authorization Areas and Groups

Restriction of activities in Solution Documentation via Authorization Areas and Groups to those relevant for Business Process Operations
Authorization Areas

Authorization areas can protect sub trees of the solution structure. An administrator can define an authorization area and assign it to a structure (e.g. a folder). In this case only users are allowed to perform activities on the structures and sub-elements that have authorization object Solution Documentation (SM_SDOC) assigned with field Authorization Area (SMUDAREA) filled with the name of the authorization area (or filled with ‘*’).

Authorization areas are defined solution-specific. An authorization area has a 30 character long technical name and a description. The default authorization area does not need to be defined. The Solution Documentation root element and all elements without assignment have the implicit authorization area assignment Default by definition.

→ See the next slides to understand how to define an Authorization Area to restrict the visibility of structure elements in solution documentation for the BPOps use case.
Example: The user setting up BPMon should not see the folder “Production” and its business processes in the solution documentation.
Example (cont.): ... in addition, the user configuring BPMon should only see those library folders, that are relevant for BPMon.
For the definition of Authorization Areas and Groups enter the view cluster maintenance SM34 for view cluster **SMUD_AUTHG**.
Usage of Authorization Areas in Solution Documentation

Select the solution for which you want to create authorization areas.
Select view Define Authorization Areas. In case of BPOs define ALERTING_LIB, ANALYTICS_LIB, INTERFACE_LIB and the relevant structures from the Business Processes section.
Select View Assign Authorization Areas and via the New Entries button select an Authorization Area and assign the element of your solution to the respective authorization areas.
Usage of Authorization Areas in Solution Documentation

The business processes and libraries that the user should be authorized to see are assigned to the authorization areas.
Authorization Groups

The concept of authorization groups in Solution Documentation is known from data dictionary tables and views. In transaction SE54, you can create and assign authorization groups to tables and views to provide the option to protect these objects in generic table and view maintenance tools. The grouping of multiple objects makes it easier for an administrator to maintain authorization profiles. With a single entry, he can allow or forbid the maintenance for example of all service desk configuration tables and views using the authorization group SDCO.

In Solution Documentation, a similar concept is used to allow authorization checks on object or attribute type level without the need of listing hundreds of object or attribute types in a special authorization role. Authorization groups are defined solution-dependent. They have a technical name that is checked in authorization object SM_SDOC in field SMUDAUTHGR.

See next slides for an example how to define an Authorization Group to restrict the visibility of object types in solution documentation for the BPOps use case.
Objects in Solution Documentation are visible in tab “Elements” and can be created via the context menu. Example: The user configuring BPMon or BPAnalytics shall see only those objects, that are relevant for his setup.
Usage of Authorization Groups in Solution Documentation

Access the view cluster maintenance SM34 for view cluster SMUD_AUTHG and select the solution for which you want to create authorization areas first. Select View Define Authorization Groups …
Usage of Authorization Groups in Solution Documentation

… and via New Entries define an Authorization Group, e.g. in case of BPOs the group OPERATIONS.
Usage of Authorization Groups in Solution Documentation

Select View "Authorization Groups for Objects": Overview

Select View Authorization Groups for Objects and via New Entries assign Group Types to the authorization groups, i.e. in case of BPOs:
- ALAGROUP
- DIAGRAMGRP
- MONOBJGRP.
Maintenance of Role for BPOps Users

Via PFCG, copy role SAP_SM_SL_ADMIN. Change your copied role by entering the values you defined for the authorization areas and authorization groups (and the branches, if you want). In our example, the user shall be allowed to execute the following activities (field ACTVT):

1. in the Alerting Library and the Analytics Library
   - Add
   - Delete
   - Release
   all objects
2. in the Business Processes Library and the Interfaces Library
   - Add
   - Delete
   - Release
   alerting objects, analytics objects and process diagrams. The user should also be authorized to change process diagrams.

In the Business Processes Library and the Interfaces Library the user should not be authorized the to change process structures (display only).

Authorizations of other users are not impacted.
Maintenance of SMUDAREA Authorization for User

1. within the Alerting and Analytics Library add, delete and release all objects
2. within Business Processes and Interfaces Library
   a) not change process structures (i.e. display only)
   b) add, delete and release alerting and analytics objects wherever possible (at process, step or interface level) and add or change process diagrams

Note: You can use field SBRA field to restrict to the branches OPERATION and PRODUCTION.
Structure Elements in Solution Documentation

Now the BPO setup user only sees those processes that are relevant for his configuration...
Structure Elements in Solution Documentation

... and only those library folders, that are relevant for his configuration.
In addition, the user can only add those objects in Solution Documentation that are relevant for his configuration...
Objects in Solution Documentation: Relevant for BPOps

... and switch between the Production and Operation branch.