SAP NetWeaver® Identity Management

Compliant provisioning using SAP Access Control

Architectural overview

Version 7.2 Rev 8

Preface

The product

The SAP NetWeaver Identity Management GRC integration consists of a set of tasks in the Identity Center and a configuration in the Virtual Directory Server that enables the use of SAP Access Control for risk validation before user provisioning. Using this solution, SAP NetWeaver Identity Management can execute provisioning to multiple target systems which are controlled by SAP Access Control to ensure compliance according to the rules implemented here.

When business requirements imply compliancy and Segregation of Duties checks, SAP NetWeaver Identity Management performs risk validation on SAP Access Control before assigning permissions, in order to achieve the compliant provisioning.

The reader

This manual is intended for people who need an overview of provisioning from SAP NetWeaver Identity Management 7.2 using SAP Access Control 10.0.

Prerequisites

To get the most benefit from this manual, you should have the following knowledge and software:

- Knowledge of the Identity Center.
- Knowledge of the Virtual Directory Server.
- Knowledge of and access to SAP Access Control 10.0 SP4 or newer.
- SAP NetWeaver Identity Management Virtual Directory Server 7.2 SP5 or newer is correctly installed and licensed.
- SAP NetWeaver Identity Management Identity Center 7.2 SP5 or newer is correctly installed and licensed.
- The Provisioning Framework for SAP Systems is correctly installed and configured.

The manual

This document gives an overview of provisioning from SAP NetWeaver Identity Management 7.2 using SAP Access Control 10.0.

Related documents

You can find useful information in the following documents (all SAP NetWeaver Identity Management 7.2 relevant documentation is available on SAP Community Network, http://scn.sap.com/docs/DOC-8397):

- The install guides for the SAP NetWeaver Identity Management.
- *SAP NetWeaver Identity Management Compliant provisioning using SAP Access Control - Configuration guide.*
- *SAP NetWeaver Identity Management Identity Services Architectural overview*.
- *SAP NetWeaver Identity Management Identity Services Configuration guide.*
- The tutorials for the Identity Center.
- The tutorials for the Virtual Directory Server.
- Relevant documentation for SAP Access Control 10.0.
- The documents *SAP NetWeaver Identity Management Identity Management for SAP System Landscapes: Architectural Overview* and *SAP NetWeaver Identity Management Identity Management for SAP System Landscapes: Configuration Guide* (describing the Provisioning Framework for SAP Systems).
- *SAP Access Control 10.0 Interface for Identity Management* available on http://scn.sap.com/docs/DOC-26208

Table of contents

Introduction

This document gives an overview of the integration between SAP NetWeaver Identity Management 7.2 and SAP Access Control (for SAP Governance, Risk and Compliance (GRC) Solutions) 10.0.

Integration scenarios

Several integration scenarios exist, depending on two factors:

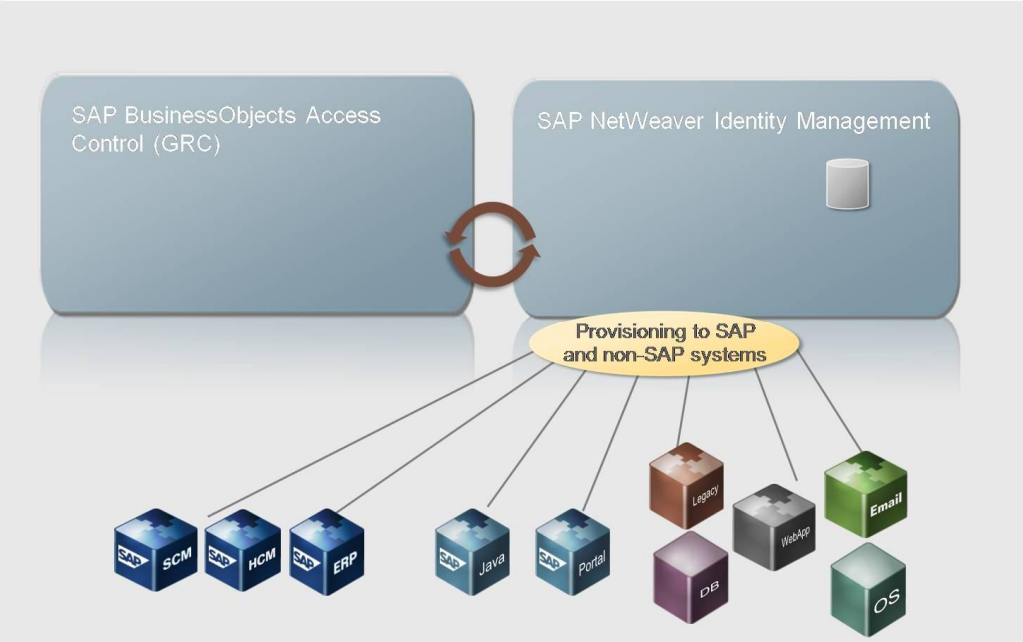
- Landscape configuration
- Result handling

The GRC provisioning framework can be configured to deal with any combination of these two.

Landscape configuration scenarios

There are two landscape configuration scenarios for the integration:

- Centralized provisioning: The centralized provisioning is recommended as a default solution. This is a scenario where SAP NetWeaver Identity Management is the only provisioning system, responsible for provisioning both the assignments that require and do not require compliance checks to the back-end systems (both SAP and non-SAP). The SAP NetWeaver Identity Management uses SAP Access Control to execute risk analysis.



- Distributed provisioning: This solution is recommended to use in exceptional cases only. The provisioning is performed both by SAP NetWeaver Identity Management and SAP Access Control.

Result handling scenarios

Whenever a request to SAP Access Control is sent by the SAP NetWeaver Identity Management, further action depends on the results of SAP Access Control's request processing, i.e. which privileges are approved and which are not.

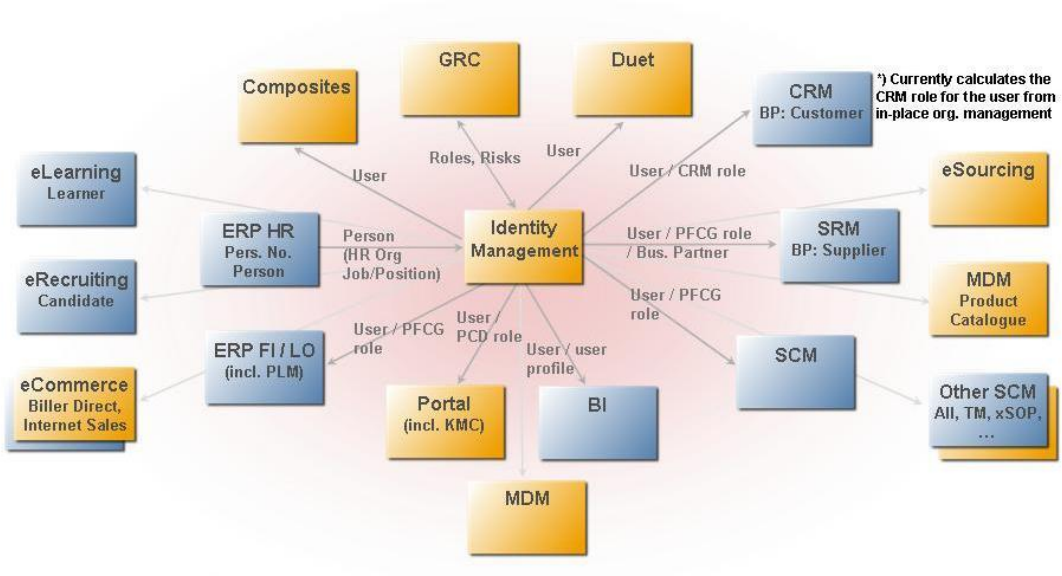
Two different approaches to handling a request processing result exist:

- Polling: The Identity Management performs the appropriate web service request, polling the SAP Access Control for the result.
- Event based (AC Callback Service): Instead of polling for the result, the Identity Management is informed about the status of the request when the processing is done. The information about this is sent by GRC, by executing its *Exit service WS* call to Identity Services.

SAP NetWeaver Identity Management

SAP NetWeaver Identity Management acts as an identity hub in a heterogeneous SAP landscape and enables efficient and secure management of identities. The Identity Center is the *authoritative source* of identity information in the whole SAP environment.

Typically, SAP NetWeaver Identity Management accepts provisioning requests from any of the systems/applications in the landscape, acts upon them and, based on the properties of the accepted requests, performs rule-based provisioning to other managed system in the SAP landscape (both non-SAP and SAP).



What kind of provisioning processes are started (e.g. which back-end systems will be the target for provisioning requests started by SAP NetWeaver Identity Management) depends on several criteria:

- The roles and privileges assigned to the entries in the Identity Center.
- The business requirements (Segregation of Duties and compliance checks).

To be able to process the provisioning requests to the back-end systems, the Identity Center must know which roles/systems/privileges are available for each of its managed systems. Each of the managed systems has its own way to expose this information to the Identity Center.

SAP Access Control

When business requirements imply compliant provisioning, SAP NetWeaver Identity Management submits the risk validation requests to SAP Access Control. The SAP Access Control carries out Segregation of Duties and then the SAP NetWeaver Identity Management performs provisioning to managed target systems.

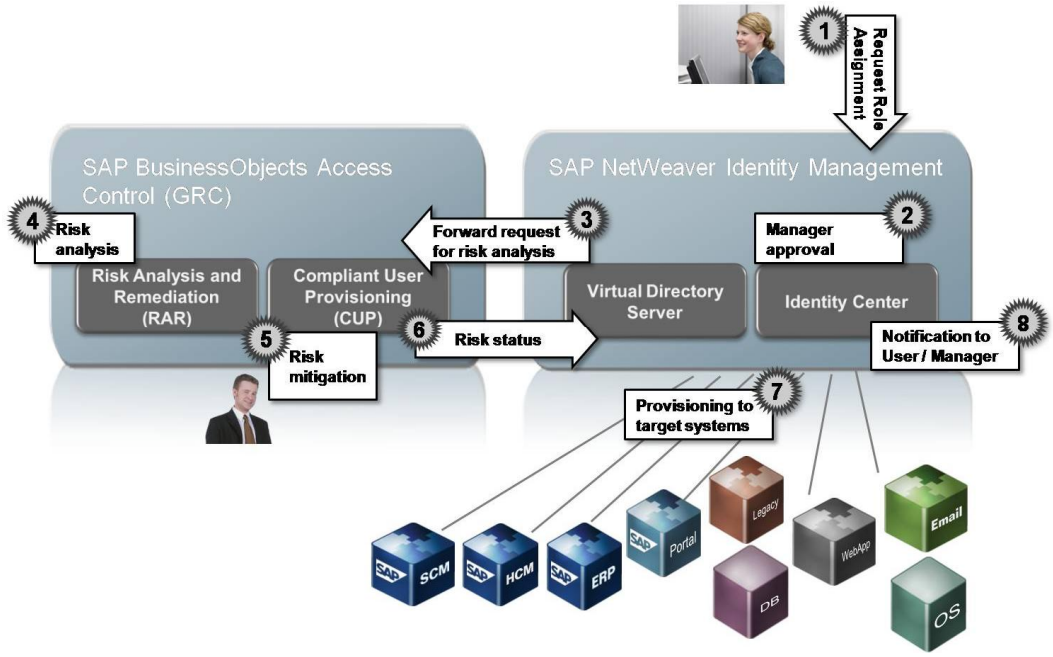
SAP Access Control exposes its functionality through a Web Service API, among others the following:

- Application
- Search Role
- Request Status
- Request Details
- Audit Log
- Provision Log
- Submit User Access Request

These web service calls are integrated in SAP NetWeaver Identity Management. For more information, see the document *SAP Access Control 10.0 Interface for Identity Management* available on http://scn.sap.com/docs/DOC-26208.

Sample scenario

A typical scenario could be like this (centralized provisioning scenario):



1. A new employee is hired. SAP Human Resources submits a role assignment request to SAP NetWeaver Identity Management, with the information about the employee and the employee's manager.
2. As a result, a workflow process is started on Identity Management side. The employee's manager will assign a set of roles and entitlements to the new employee, that are required for his/her new job. The information about these roles and entitlements is stored in the Identity Center. The information added by the manager is not stored in the new employee's entry – it waits for the outcome of the approval process.
3. This typically triggers multiple events that result in provisioning processes towards back-ends managed by the Identity Center.

   Usually, SAP NetWeaver Identity Management carries out this provisioning directly, but some assigned roles/privileges must be handed to SAP Access Control in order to execute a risk validation.

   Due to the asynchronous nature of the request process to SAP Access Control, the Identity Center starts a *pending* provision process (this means that the relevant information added by the manager is not stored in the new employee's entry – it waits for the outcome of the approval process).

   SAP NetWeaver Identity Management executes a web service call to the SAP Access Control system and submits the request for risk analysis. The status about the successful receipt of the request is sent back to SAP NetWeaver Identity Management.
4. The request is stored in the SAP Access Control request queue. The SAP Access Control carries out Segregation of Duties and compliancy checks.
5. In case a risk is detected in the request the SAP Access Control workflow will determine an approver who needs to work on the request item, otherwise it can be completed automatically.

6. SAP NetWeaver Identity Management awaits the status of the approval. It regularly polls SAP Access Control about the outcome of the request (if using polling as the result handling scenario) or waits until it receives a callback service (if using event based result handling scenario). If the request is not processed within a certain (configurable) time limit, SAP NetWeaver Identity Management will treat the request as failed.
7. When SAP NetWeaver Identity Management receives the result of the requested operation, it confirms or rejects the changes in the Identity Center. If the request is approved, the roles and entitlements assigned for the new entry (by the manager) are provisioned to the managed systems and thus become valid and enabled with the new employee's entry.
8. A notification to user and/or manager is sent.

Initialization

In order to successfully hand over the requests to SAP Access Control, the SAP NetWeaver Identity Management requires information about the environment managed by SAP Access Control.

Before it can process any provisioning request, SAP NetWeaver Identity Management executes one web service call towards SAP Access Control:

- "Search Role" which obtains information about roles available for each of the systems managed by SAP Access Control. This call will typically enrich the role information which is already available in the Identity Management. The role information will be retrieved by initial load jobs connecting directly to the target system.

These operations are normally executed during the "Initial Load" phase. The information is stored as privileges in the Identity Center.

Limitations/tuning of the framework

The following may be adjusted in the framework:

- The GRC provisioning framework is built around the smallest set of attributes that are required in a *GRAC_USER_ACCESS_WS* web service call. Submitting additional attributes must be configured as custom attributes on the SAP Access Control side and added to the relevant task(s)/pass(es) of the GRC provisioning framework.

  See section *Mandatory attributes* in the document *SAP NetWeaver Identity Management Compliant provisioning using SAP Access Control - Configuration Guide*.

- The *GRAC_USER_ACCESS_WS* web service call includes the following information: Request type, priority and employee type. The values that SAP NetWeaver Identity Management uses when executing this call has to be aligned with the values that are configured in SAP Access Control.

  See section *Setting the requestor properties* in the document *SAP NetWeaver Identity Management Compliant provisioning using SAP Access Control - Configuration Guide*.

The following limitations apply to the GRC provisioning framework:

- Obtaining information about managed systems and roles has to be done regularly – there is no automatic process for this.
- A change of the SAP NetWeaver Identity Management's request (so called remediation) is limited to removing the items. It is not possible to add new roles on SAP Access Control side.