ESPRESSO TUTORIALS

Julian Harfmann | Sabrina Heim | Andreas Dietrich

Compliant Identity Management mit SAP® IdM und GRC AC

- Vorteile eines Compliant Identity Managements
- Stärken und Schwächen von SAP IdM und GRC AC
- integrierte Rollen- und Berechtigungsverwaltung
- gemeinsame Benutzeroberfläche über SAP Enterprise Portal

Inhaltsverzeichnis

2 Produkte im SAP-CIM-Kontext

In diesem Kapitel stellen wir Ihnen zunächst die beiden Produkte SAP GRC Access Control und SAP Identity Management vor, die zur Realisierung unseres Compliant-Identity-Management(CIM)-Szenarios dienen. Im Anschluss daran gehen wir kurz auf die Grundkonfiguration der beiden Produkte im Hinblick auf die CIM-Integration ein, bevor das Kapitel mit einem Vergleich der beiden Identity-Management-Versionen endet, die sich momentan auf dem Markt befinden.

2.1 SAP GRC Access Control

Bevor wir mit der eigentlichen Vorstellung von SAP GRC Access Control beginnen, wollen wir im ersten Schritt ein paar Worte zur Architektur des Systems sowie zu den technischen Voraussetzungen verlieren, die notwendig sind, um die Anbindung von Zielsystemen zu ermöglichen.

Prinzipiell erfolgt die Anbindung von SAP-Systemen an das AC-System per *Remote Function Call (RFC)* über die Transaktion *SM59*. Eine Ausnahme stellt das SAP Identity Management dar, das per HTTP (Hypertext Transfer Protocol) und SPML (Service Provisioning Markup Language) mit dem GRC verbunden wird. Zusätzlich dazu ist eine Aktivierung der *Webservices* notwendig, um später die Integration zwischen SAP IdM und SAP GRC AC erfolgreich durchführen zu können. Die Aktivierung der relevanten GRC-Webservices erfolgt mithilfe der Transaktion *SOAMANAGER*.

Auf die einzelnen Schritte, die zur Konfiguration des Compliant Identity Managements notwendig sind, werden wir in Abschnitt 4.3 noch zu sprechen kommen. Einen prinzipiellen Überblick über die GRC-Architektur bietet Ihnen Abbildung 2.1.

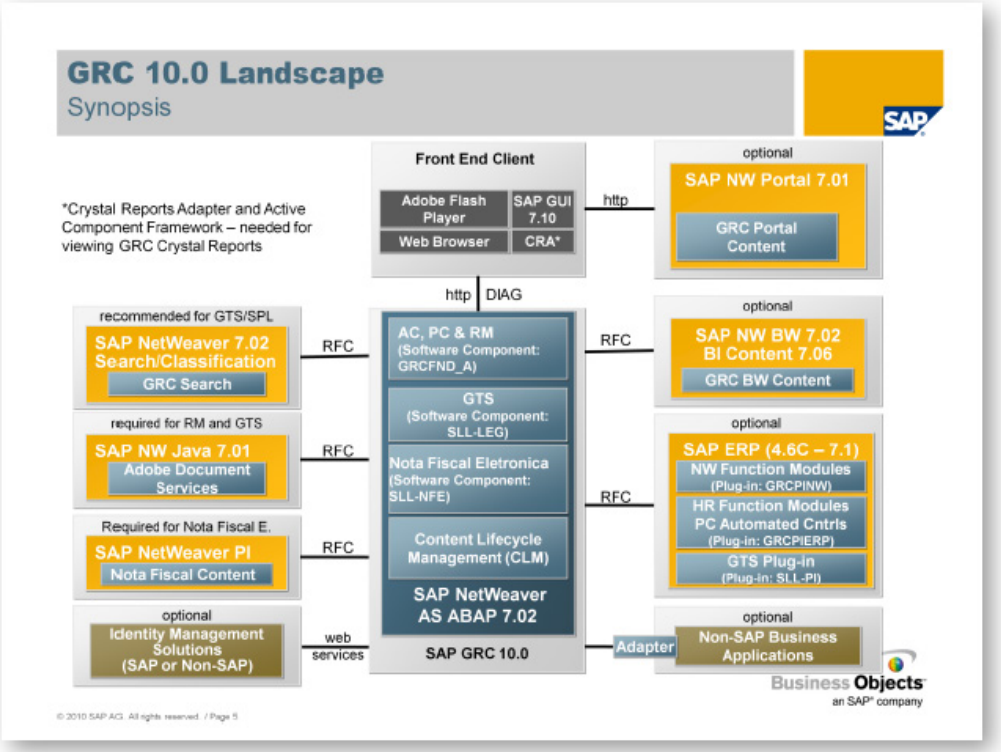
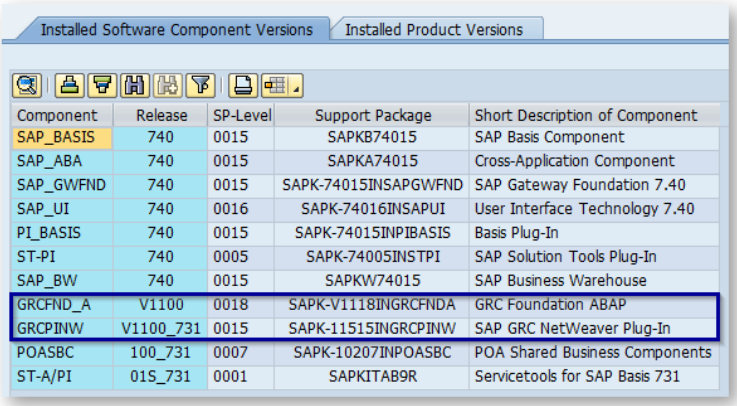


Abbildung 2.1: GRC-Architektur

Vor dem Anschluss der Zielsysteme sind auf deren Seite sowie im GRC noch einige Voraussetzungen zu erfüllen. Für den erfolgreichen Austausch von Daten zwischen SAP GRC AC und dem jeweiligen Satellitensystem müssen zunächst verschiedene Plug-ins installiert werden. Dazu gehören:

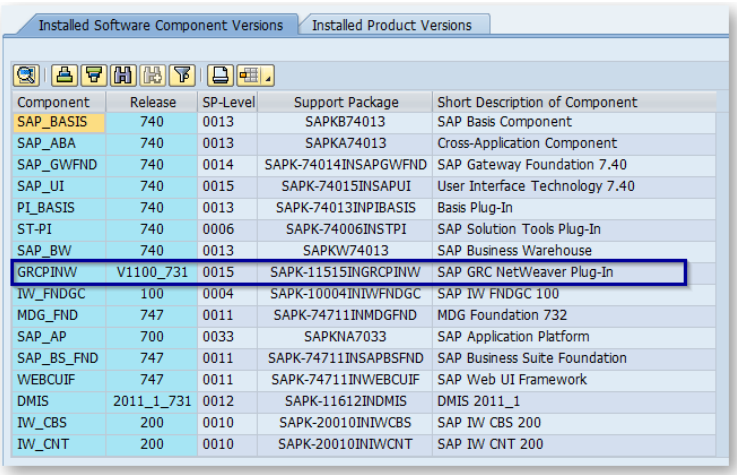
- für GRC Access Control die in Abbildung 2.2 umrahmten Plug-ins,
- sowie für das Zielsystem das in Abbildung 2.3 markierte Plug-in.



Installed Software Component Versions | Installed Product Versions

Component	Release	SP-Level	Support Package	Short Description of Component
SAP_BASIS	740	0015	SAPKB74015	SAP Basis Component
SAP_ABA	740	0015	SAPKA74015	Cross-Application Component
SAP_GWFND	740	0015	SAPK-74015INSAPGWFND	SAP Gateway Foundation 7.40
SAP_UI	740	0016	SAPK-74016INSAPUI	User Interface Technology 7.40
PI_BASIS	740	0015	SAPK-74015INPIBASIS	Basis Plug-In
ST-PI	740	0005	SAPK-74005INSTPI	SAP Solution Tools Plug-In
SAP_BW	740	0015	SAPKW74015	SAP Business Warehouse
GRCFND_A	V1100	0018	SAPK-V1118INGRCFNDA	GRC Foundation ABAP
GRCPINW	V1100_731	0015	SAPK-11515INGRCPINW	SAP GRC NetWeaver Plug-In
POASBC	100_731	0007	SAPK-10207INPOASBC	POA Shared Business Components
ST-A/PI	01S_731	0001	SAPKITAB9R	Servicetools for SAP Basis 731

Abbildung 2.2: Plug-ins für GRC Access Control



Installed Software Component Versions | Installed Product Versions

Component	Release	SP-Level	Support Package	Short Description of Component
SAP_BASIS	740	0013	SAPKB74013	SAP Basis Component
SAP_ABA	740	0013	SAPKA74013	Cross-Application Component
SAP_GWFND	740	0014	SAPK-74014INSAPGWFND	SAP Gateway Foundation 7.40
SAP_UI	740	0015	SAPK-74015INSAPUI	User Interface Technology 7.40
PI_BASIS	740	0013	SAPK-74013INPIBASIS	Basis Plug-In
ST-PI	740	0006	SAPK-74006INSTPI	SAP Solution Tools Plug-In
SAP_BW	740	0013	SAPKW74013	SAP Business Warehouse
GRCPINW	V1100_731	0015	SAPK-11515INGRCPINW	SAP GRC NetWeaver Plug-In
IW_FNDGC	100	0004	SAPK-10004INIWFNDGC	SAP IW FNDGC 100
MDG_FND	747	0011	SAPK-74711INMDGFND	MDG Foundation 732
SAP_AP	700	0033	SAPKNA7033	SAP Application Platform
SAP_BS_FND	747	0011	SAPK-74711INSAPBSFND	SAP Business Suite Foundation
WEBCUIF	747	0011	SAPK-74711INWEBCUIF	SAP Web UI Framework
DMIS	2011_1_731	0012	SAPK-11612INDMIS	DMIS 2011_1
IW_CBS	200	0010	SAPK-20010INIWCBS	SAP IW CBS 200
IW_CNT	200	0010	SAPK-20010INIWCNT	SAP IW CNT 200

Abbildung 2.3: Plug-in für Zielsystem

Bei der Installation der Plug-ins ist darauf zu achten, dass diese vom Releasestand auch zu den anderen Komponenten des jeweiligen Systems passen. Dies gilt im Speziellen für das GRCPINW auf dem Zielsystem. Überdies bestehen gewisse Abhängigkeiten zum SAP GRC AC (z. B. Fiori UI zur Nutzung der GRC-Genehmiger-App), auf die an dieser Stelle nicht im Einzelnen eingegangen werden soll, die

aber im SAP-Konfigurationsleitfaden für GRC nachgelesen werden können.

Nach diesem kurzen Abriss zur Architektur und zu den technischen Voraussetzungen können wir an dieser Stelle mit der Kurzvorstellung der Komponenten von SAP GRC Access Control beginnen, bevor wir im Verlauf des Kapitels einen detaillierteren Einblick in die vielfältigen Konfigurationsmöglichkeiten der Workflows im Kontext von SAP GRC AC geben. Diese Workflows sind für die Benutzeradministration hinsichtlich der Antrags- und Genehmigungsprozesse sowie einer integrierten Risikoprüfung für das SAP GRC Access Control unerlässlich.

Neben den von SAP standardmäßig ausgelieferten werden unternehmensspezifisch eingerichtete Workflows vorgestellt und deren Konfiguration wird im Kontext der Workflowinstrumente MSMP (Multi-Stage-Multi-Path) und BRF+ (Business Rule Framework) näher betrachtet.

Ein besonderer Stellenwert kommt hier den einzelnen Prozessschritten der Provisionierung im Kontext des Compliant Identity Managements zu.

2.1.1 Kurzvorstellung der Komponenten im AC-Kontext

Access Risk Analysis (ARA)

Access Risk Analysis (ARA), zu Deutsch »Analyse der Zugriffsrisiken«, ist die zentrale Komponente von SAP GRC Access Control. Sie ermöglicht es, teilautomatisierte Analysen auf Benutzer-, Rollen- und Profilebene durchzuführen und so ein Echtzeitbild der Risiken in der Systemlandschaft zu erhalten. Aus den gewonnen Erkenntnissen können Maßnahmen zur Bereinigung oder Mitigierung der identifizierten Risiken abgeleitet werden. Die Risiken werden in der sogenannten *Segregation-of-Duties(SoD)-Matrix* abgebildet und so dem Anwender für Analysen zugänglich gemacht.

Business Role Management (BRM)

Das Business Role Management (BRM) ist der Bestandteil von AC, der sich mit der Pflege und Weiterentwicklung von Rollen bzw. Privilegien in der Systemlandschaft beschäftigt. Mithilfe des BRM lassen sich sämtliche Änderungen an den Berechtigungen dokumentieren und revisionssicher nachvollziehen. Des Weiteren ist es möglich, dedizierte und unternehmensspezifische Workflows zu hinterlegen, die bei Modifikationen an den Berechtigungen zu durchlaufen sind. Die Funktionen des Business Role Managements ermöglichen es, den gesamten Prozess der Pflege und Weiterentwicklung von Berechtigungen innerhalb eines Tools zu steuern und abzubilden.

User Access Management (UAM)

Die Komponente User Access Management (UAM) wird für die Erstellung und Änderung von Benutzern verwendet. Hierzu stehen im UAM Genehmigungsworkflows bereit, sodass die Prozesse revisionssicher dokumentiert sind und zu jedem Zeitpunkt nachvollzogen werden können. Für einzelne Workflows sind Risikoprüfungen etabliert, die Berechtigungskonflikte zur Laufzeit sichtbar machen.

In Abschnitt 1.2 werden wir uns detaillierter die einzelnen Möglichkeiten im Kontext der verschiedenen Provisionierungsfunktionen ansehen.

Emergency Access Management (EAM)

Das Emergency Access Management (EAM), besser bekannt unter den Namen »Firefighter«, ermöglicht es, kritische (z. B. Replace und Debug) sowie nicht häufig verwendete Berechtigungen (z. B. Jahresabschluss) aus dem gewöhnlichen Benutzerstammsatz auszulagern. Diese werden einem Benutzer mit weiter reichenden Berechtigungen zugeordnet, genannt *Firefighter*. Der Vorteil des EAM liegt in der Protokollierung sämtlicher Tätigkeiten, die mit dem Firefighter ausgeführt werden. Durch die Protokollierung und spätere Prüfung der erzeugten Firefighter-Protokolle ist den Audit-Anforderungen genüge getan

B Index

G

I

J

K

M

N

P

Q

R

S

T

U

V

W

Z