

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

Vorwort	7
1 Einführung in das Compliant Identity Management (CIM)	11
1.1 Motivation für die Einführung von Compliant-Identity- Management-Prozessen	11
1.2 CIM: eine Aufgabe des Unternehmens – nicht ausschließlich der IT	17
2 Produkte im SAP-CIM-Kontext	27
2.1 SAP GRC Access Control	27
2.2 SAP Identity Management	46
3 Zwei Produkte für einen Prozess – ergibt das einen Sinn?	81
3.1 Stärken und Schwächen von SAP Identity Management	81
3.2 Stärken und Schwächen von SAP GRC Access Control	92
3.3 Unterschiedliche Arten der Integration von SAP IdM und GRC in die Unternehmensarchitektur	96
4 Compliant Identity Management	101
4.1 Zusammenspiel der Produkte SAP IdM und GRC AC	101
4.2 Integrierte Rollen- und Berechtigungsverwaltung	107
4.3 Konfiguration eines integrierten Szenarios	111
4.4 Aus zwei mach eins – Integration in ein Unternehmensportal	145

5 Fazit/Ausblick	157
A Die Autoren	161
B Index	165
C Disclaimer	169

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.

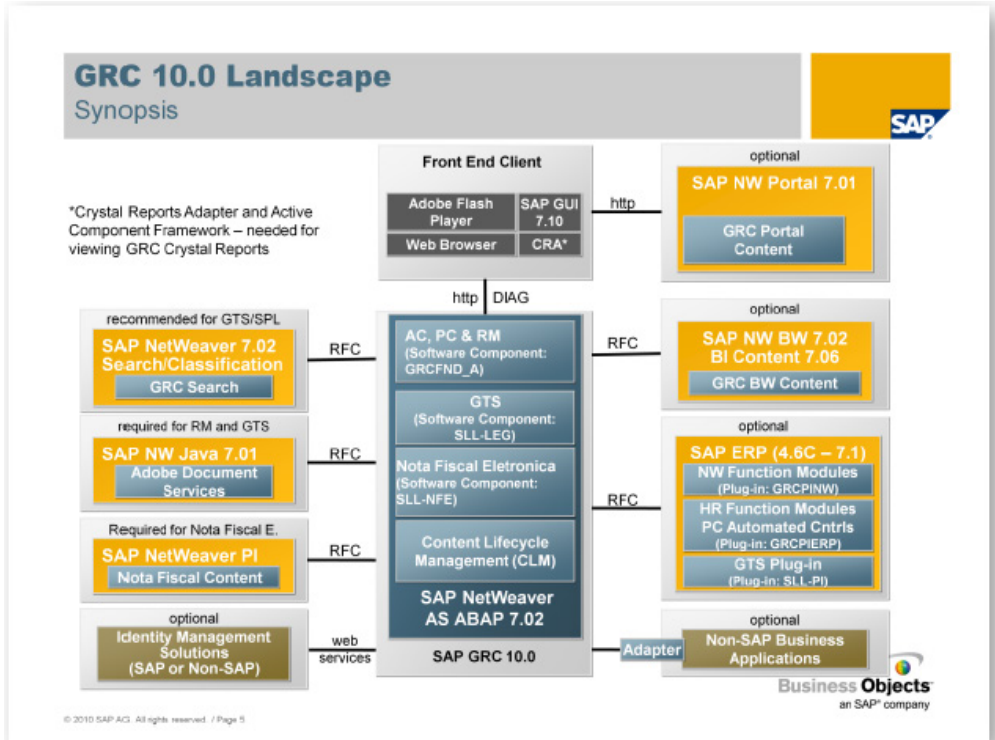


Abbildung 2.1: GRC-Architektur

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.

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-V1118INGRCFND	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

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

A

ABAP-Stack 47
Access Management 82
Access Risk Analysis (ARA) 30
Account Management 13, 81
Account-Mapping 19
Active Directory 84

B

Benutzer-Identifikation 20
Benutzerkonto 19, 23
Berechtigung 21
 Arbeitsplatzrolle 22
 Berechtigungskonzept 21, 22,
 24, 98
 Businessrolle 24
 Rollenlimit 24
Berechtigungskonzept 14
Berechtigungswesen 92
BRF+ 30, 43
Business Role Management 31,
91

C

Callback-Webservice 100, 105,
106, 119, 121, 124, 125, 144
Deployment 127
Konfiguration AS JAVA 127
Prozess-ID 122
Centralized Provisioning 97

CIM *Siehe* Compliant Identity
Management
Compliance 12, 13, 98
Compliant Identity Management
(CIM) 11, 13, 14, 15, 96, 107
Vorteile 13

D

Datenbank 47, 52
Datenbankschema 48
Directory 52
Dispatcher 49, 50
Dispatcher Utility 57
Distributed Provisioning 97
Dynamische Gruppe 87, 88, 91

E

Eclipse 53
Emergency Access
Management (EAM) 13, 31
Employee Self Service (ESS)
22
Entwicklungsumgebung 85

F

Fachkompetenz 21
Firefighter 31
Forms 72
Form Type 73

G

- GRC Business Role Management 94
- GRC Provisioning Framework 68, 112, 118, 129, 130

I

- IAM 18, 98
 - Dokumentation 49
 - IAM-Infrastruktur 18
 - Identity and Access Management 47
- Identity Store 47, 67
- IdM
 - Prozess 87
- IdM Developer Studio 53
 - Forms 50
- IKS-Verantwortlicher 109
- Integration 52, 81, 96
- integriertes Szenario 131

J

- Java Virtual Machine 50
- JavaScript 83
- Jobs 49

K

- Keys.ini-Datei 60, 112, 122, 127
 - KeysIniUtility 55
- Key-User 22
- Konfiguration 131
- Konnektor 82, 83
- Kosten 22, 47

M

- Microsoft Management Console 53
- MSMP 30, 33

N

- Namenskonvention 23
- NWA Siehe SAP NetWeaver Administrator

P

- Packaging-Konzept 71
 - Import 67
 - Versionsverwaltung 72
- Performance 24, 49
- Polling 98, 100
- Portal 50
- Processes 72
 - Process Flow Diagram 75
 - Public Process 76
- Provisionierung 47

Q

- Queue 49

R

- Reconciliation 91
- Repository 117
 - GRC Repository 117, 118, 122, 130
 - Jobs 77
 - Konstanten 77
 - Type 76
- REST-Interface 51, 83
- Risikoanalyse 92
- Risikoverantwortlicher 109

Risk Terminator 93
 Rollenmanagement 93
 Rollenmodell 22, 90
 -Update 91
 Runtime 49

S

SAP Enterprise Portal 145
 SAP-GRC-Anbindung 148
 SAP-IdM-Anbindung 147
 SAP Gateway 51
 SAP GRC Access Control 11,
 27, 46
 SAP Identity Management (IdM)
 11, 46
 SAP IdM Siehe *SAP Identity
 Management*
 Datenbankverbindung 59
 SAP IdM Admin WebUI 77
 Repository-Verwaltung 78, 117
 SAP IdM Developer Studio 63,
 70, 129
 Berechtigungen 70
 Berechtigungen auf Paketen 71
 Datenbankverbindung 59
 Installation 62
 Rolle für IdM-Administrator 66
 SAP NetWeaver 50, 52
 Application Server Java 50
 SAP NetWeaver Administrator
 59, 127
 Anwendung starten & stoppen
 62, 128
 Anwendungsressourcen 59
 Java-Systemeigenschaften 60
 SAP NetWeaver Business Client
 140

SAP NetWeaver Developer
 Studio 126
 SAP Provisioning Framework
 66, 68, 72
 SAP Software Provisioning
 Manager 54
 SAP-IdM
 Benutzeroberfläche 138
 Identität ändern 139
 SAP-Standardworkflow 41
 SAPUI5 51
 Segregation of Duties 30
 stored procedure 48
 Systemlandschaft 48

T

Tasks 49

U

Unternehmensspezifische
 Workflows 44
 User Access Management
 (UAM) 31

V

VDS siehe Virtual Directory
 Server
 Verantwortlichkeit 21
 Virtual Directory Server 50, 52,
 54, 102, 112, 140
 GRC-Integration 114
 Grundeinstellungen 112
 Identity Service 121, 124, 126
 Virtual Directory Server (VDS)
 85

W

Web-Dynpro 50

Webservices 27

Workflow 84, 87

Z

Zentrale Benutzerverwaltung 47

Zielsystem 82