



Dr. Bernd Klüppelberg

Techniken im SAP®- Berechtigungswesen

- ▶ Berechtigungskonzepte in SAP
- ▶ SE16N, Z-Programme, Menühandling
- ▶ Zahlreiche Praxisbeispiele
- ▶ Viele Tipps und Tricks aus 10 Jahren Praxiserfahrung

Inhaltsverzeichnis

1 Einführung	9
1.1 Zentrale Regel	10
1.2 Begrifflichkeiten	10
2 Rollentypen	21
2.1 Einzelrollen	21
2.2 Masterrollen	22
2.3 Abgeleitete (Child-)Rollen	23
2.4 Werterollen	24
2.5 Sammelrollen	25
2.6 Sonderrollen	26
3 Namenskonventionen	27
3.1 Forderungen an Rollennamen	28
3.2 Einflussfaktoren	29
3.3 Namenstest-Vorlage	30
3.4 Rollenkonzeption	32
4 Zu treffende Entscheidungen	35
4.1 Regelung des Tabellenzugriffs	35
4.2 Regelung des Programmzugriffs	44
4.3 Forderungen an die Entwicklung	49
4.4 Benutzertypen	53
4.5 Fazit	64
5 Techniken	65
5.1 Limits bei Rollen	65
5.2 Besonderheiten PFCG	67

5.3	Jobs für Berechtigungen	81
5.4	Suchtechniken	83
5.5	Besondere Berechtigungen aus der Basis	104
5.6	Kritische Berechtigungen	123
5.7	Z-Programme	129
5.8	Objekt-Pflege über die Transaktion SU24	137
5.9	Menühandling	143
5.10	Modularisierung, Granulierung	150
5.11	Einführung Org-Levels	161
5.12	Zusammenspiel von M-, A- und V-Rollen	163
5.13	Benutzergruppen	176
5.14	Rollenzuordnungen	177
5.15	Rollendokumentation	181
5.16	Rollentest	190
5.17	Produktivsetzung der neuen Rollen	191
6	Weitere Tipps und Tricks	195
6.1	Export des Systemmenüs	195
6.2	Löschen von Rollen	196
6.3	Transport von Rollen zwischen Mandanten	196
6.4	Rollen umbenennen	197
6.5	Benutzerzuordnung in Rollen	197
6.6	Gelöschte Transaktionen aus Rollen entfernen	198
6.7	ACCESS-DB zur Analyse	199
6.8	ST01-Berechtigungstrace	200
7	Anhang	207
7.1	Wichtige Tabellen	207
7.2	Wichtige Transaktionen	208
7.3	Abkürzungen	210

2 Rollentypen

In alten R/3-Zeiten wurden die Berechtigungen über *Berechtigungsprofile* realisiert. Nachdem man merkte, dass diese Berechtigungsprofile nicht unbedingt praktikabel waren, stülpte man sozusagen ein anderes Konstrukt über diese Profile, die sogenannten Rollen, früher auch als *Aktivitätsrollen* bezeichnet .

Eine funktionierende Rolle hat immer auch ein Profil, das der Rolle dann die Berechtigungen zuordnet. Ein Profilname kann entweder für die Rolle gewählt oder generiert werden.

Es gibt verschiedene Ausprägungen von Rollen, wobei die einfachste die sog. *Einzelrolle* ist. Darunter existieren verschieden Spielarten, wie Rollen erzeugt werden können. Diese sind abhängig von *Organisationsebenen* – auch oft *Org-Levels* genannt (vgl. Abschnitt 1.2.7).

Auch bei den Rollen gibt es zu viele missverständliche Namen und Namensgebungen, sodass es auch hier bei den Rollentypen angebracht erscheint, eine einheitliche, einfache und verständliche Nomenklatur einzuführen.

Achtung!



Rollen sind im Gegensatz zu Berechtigungsobjekten mandantenbezogen!

2.1 Einzelrollen

Eine Einzelrolle kommt immer dann zum Einsatz, wenn sich entweder die Berechtigung nicht auf Org-Levels bezieht, oder Berechtigungen – unabhängig von Org-Levels – Benutzern zugeordnet werden können.

Definition Einzelrolle



Eine Einzelrolle ist eine normale Rolle, die Transaktionen und die Berechtigungen für diese Transaktionen beinhaltet. Sie besitzt ein Rollenmenü, und alle Org-Levels sind mit gültigen Werten bewertet. Dass diese Rolle eine Einzelrolle ist, sollte aus der Namensgebung für die Rolle hervorgehen.

2.2 Masterrollen

Wenn die Rechte, die einem Benutzer zugeordnet werden sollen, nur von Org-Levels abhängig sein sollen, der Benutzer sonst aber über die gleichen Zugriffsrechte verfügt, kann man das Konstrukt der *Masterrolle* und »*abgeleiteten Rolle*« benutzen.

Definition Masterrolle



Eine *Masterrolle* ist eine Art Einzelrolle, die Transaktionen und die Berechtigungen für diese Transaktionen beinhaltet. Sie besitzt ein Rollenmenü und alle Org-Levels sollten mit nicht-gültigen Werten (z. B. »?«) bewertet sein. Sie gibt nur eine »leere Hülle« einer Rolle an, wird selbst aber *nicht* zur Benutzeradministration eingesetzt.

Die Masterrolle erhält ihren Sinn erst durch die sog. Ableitung der Rolle als *abgeleitete* oder *Child-Rolle*.

Dass diese eine Masterrolle ist, sollte aus der Namensgebung hervorgehen.

Es gibt Fremdsysteme, die den Begriff der Masterrolle anders auffassen: So arbeitet Realtime-APM mit Masterrollen und Ableitungen. Letztere sind nicht auf Org-Levels beschränkt, sondern durch einen zwischengeschalteten Ableitungsordner definiert! Dieser ersetzt alle Berechtigungsfelder der Rolle. Dies hat nichts mit dem hier eingeführten Begriffen Master- und Child-Rolle zu tun, sondern stellt sich ganz anders dar.

2.3 Abgeleitete (Child-)Rollen

Durch die Bewertung der Org-Levels in der Masterrolle wird die Rolle sozusagen aktiv. Sie ist aber dann eine Rolle, welche die gleichen Transaktionen und Berechtigungsobjekte enthält wie die Masterrolle, und unterscheidet sich durch anders bewertete Org-Levels.

Definition abgeleitete Rolle



Eine abgeleitete Rolle oder auch *Child-Rolle*, wird aus einer bestehenden Masterrolle erzeugt. Sie enthält die gleichen Transaktionen, das gleiche Rollenmenü und die gleichen Berechtigungsobjekte wie die Masterrolle.

Der einzige Unterschied zwischen zwei Child-Rollen ist die unterschiedliche Bewertung der Org-Levels in den einzelnen Ableitungen. Somit ist es möglich, Rollen für Benutzer zu definieren, die sich nur in den Org-Levels unterscheiden.

Welche abgeleitete Rolle aus welcher Masterrolle ist, lässt sich über die Tabelle `AGR_DEFINE` bestimmen: Dort ist die Rolle die abgeleitete Rolle, und das Feld `PARENT_AGR` ist die Masterrolle. Dass diese eine Child-Rolle ist, sollte aus der Namensgebung hervorgehen.

Zum Einsatz kommt das Konstrukt der Master- und Child-Rolle immer, wenn Benutzer zwar die gleichen Transaktionen bspw. in der Buchhaltung durchführen dürfen, ihre Rechte sich aber hinsichtlich der Bearbeitung eines bestimmten Buchungskreises unterscheiden. Benutzer A darf zwar die Transaktion FB03 (ANZEIGEN BELEG) aufrufen, innerhalb dieser aber nur Belege sehen, die dem Buchungskreis 002 zugeordnet sind. Für andere Buchungskreise hat er keine Zugriffsrechte.

2.4 Werterollen

Manchmal kommt es vor, dass bspw. eine betriebswirtschaftliche Größe im Standard nicht als Org-Level ausgeprägt ist. Dann kann man die Rechte für dieses Objekt auch gesondert in eine Rolle stecken und dem Benutzer zuweisen. Der Benutzer-Puffer sorgt dann dafür, dass der Benutzer das Recht über die Oder-Verknüpfung erhält. Derartige Rollen sollen hier Value- oder Werte-Rollen heißen.

Definition Value-Rolle



Eine Value- oder *Werte-Rolle* ist eine Rolle, die normalerweise keine Transaktionen und kein Rollenmenü enthält. Sie definiert und bewertet nur einzelne Berechtigungsobjekte, die im User-Puffer eine Berechtigung ergänzen.

Bei der Bildung einer Value-Rolle müssen in anderen Rollen ggf. Objekte inaktiviert werden, da sie sonst die Ausprägung der Value-Rolle im User-Buffer überlagern würden.

Dass diese Rolle eine Value-Rolle ist, sollte aus der Namensgebung hervorgehen.

Dazu ein kurzes Beispiel:

Sie wollen den Zugriff auf bestimmte Kostenstellen beschränken. Die Kostenstelle ist normalerweise kein Org-Level. Sie nehmen in der Masterrolle alle Objekte KOSTENSTELLE aus der Rolle, indem sie die Objekte inaktivieren. Nun definieren Sie einige Value-Rollen, die nur das Kostenstellenobjekt beinhalten, und bewerten es unterschiedlich. Letztlich hat dann der eine Benutzer Zugriff auf Kostenstelle xx und der andere auf Kostenstelle yy!

2.5 Sammelrollen

Man kann Rollen in einer zusammenfassen und diese dem Benutzer zuordnen. Dies führt zum Begriff der *Sammelrolle*:

Definition Sammelrolle



Eine Sammelrolle ist im System ein eigener Rollentyp, mit dem man beliebige Rollen zu einer zusammenfassen kann. Man notiert in einer eigenen Funktionalität der Transaktion PFCG eine Sammelrolle und ordnet ihr unterschiedliche bestehende andere

Rollen zu.

Damit wird es für die User-Administration ggf. leichter, einem Benutzer Rollen zuzuordnen. Dass eine Rolle eine Sammelrolle ist, ist in der Tabelle AGR_AGRS verankert.

Dass diese Rolle eine Sammelrolle ist, sollte aus der Namensgebung hervorgehen.

B Index

A

Aktivitätsrollen 21
 ALL_USER_MENUS_OFF
 149
 Änderungsdaten Rolle 72
 anonyme Benutzer 63
 anonyme User-ID 62, 63
 A-Rolle zu Master 89
 AUTHORITY-CHECK 12, 15,
 103

B

Batch-User 55
 Benutzerabgleich 81
 Benutzerabgleich Job 82
 Benutzeradministrator 53
 Benutzerinformationssystem
 83
 Benutzermenü erzwingen 149
 Benutzerpflege SU01 41
 Benutzertypen 53
 Berechtigungsgruppe 36
 Berechtigungsobjekt
 Dokumentation 70
 Berechtigungsprofile 21
 Berechtigungstrace 102
 Bereichsmenüs pflegen
 SE43N 41
 B-Feld FBTC 77

B-Feld Mahnlauf 77
 B-Feld Zahllauf 77
 B-Gruppe 36
 B-Objekt Dokumentation 70
 B-Objekt S_GUI 147
 B-Wert &NC& 36

C

CALL TRANSACTION 50

D

Debitoren-View 100
 Debugging 58
 Debugging/Replace 58, 104
 DICBERCLS 36

E

Easy_Access_Number_Of_No
 des 143
 eigene B-Objekte 51
 Einstellung ALV-Grid 88
 Entwicklerrechte 58
 Entwicklungsrichtlinie 35

F

F_KNA1_GRP 99
 F_LFA1_GRP 99
 F110 77

F150 77
Fachberater 56
Fachbereichskonzepte für
 Berechtigungen 33
Fachfremde Zugriffe 60
FALLE 59
FBTCH B-Feld 77
Feld SECU 44, 46
Feldbewertung und Blank 97
Feldprüfungen 18

G

Generalziel bei Rollen 150
generische Prüfung 18
Granulierung von Rollen 150

H

H1481950 (SAP-NOTE) 42
Help-Desk 56
Hilfe zu B-Objekt 70

I

IDOC-User 55
Intervallprüfungen 19

J

Job für SAPPROFC_NEW 83
Job
 PFCG_TIME_DEPENDENC
 Y 82

K

Key-User 60
Kopierhilfe ALV-Grid 88

Kreditoren-View 100
Kritikalitätsfaktor 125, 128
kundeneigene Tabellen 37

L

LEAVE TO TRANSACTION
 50

M

Mahnlauf 77
Massengenerierung 83
Modularisierung von Rollen
 150

O

Objekt S_USER_AGR 176
Objekt S_USER_GRP 176
Organisationsebenen 21
Org-Level 21

P

P_ORGIN 101
Parametertransaktion SE93
 38
PFCG 15, 67, 129, 147
PFCG_TIME_DEPENDENCY
 82
PFCG-Expertenmodus 148
PFUD 82
Positiv-Trace 103
Programm SAPPROFC_NEW
 83
Prüfung bei Rollen 15

R

Rahmenkonzept 32
 Report
 PFCG_ORGFIELD_CREAT
 E 162
 Reporttransaktionen 47
 RFC-User 55
 Rolle Änderungsdaten 72
 Rollenadministrator 54
 Rollenamen mit SAP 30
 Rolleneigner 60
 Rollengenerierung in
 Produktion 52
 Rollenmenü löschen 147
 Rollennamen 27
 Rollenverantwortlichkeit 60
 RSBDCOS0 108
 RSCSAUTH 46, 109

S

S_BCE_68001409 84
 S_BCE_68001409 92
 S_BCE_68001425 84
 S_BCE_68001429 84
 S_BCE_68001430 84
 S_PROGRAM 46
 S_TABU_DIS 35
 S_TABU_NAM 42
 S_TCODE 50
 SA38 45
 Sachkonten 101
 Sammelrolle 90
 SAP-Help über Internet 71
 SAP-Help-Seite 71
 SAP-Support 57
 SCC4 107

SCC7 80
 SCC8 80
 Schulungs-User 62
 SE06 107
 SE16 35
 SE16N 35, 104
 SE37 106
 SE38 45
 SE43N 41
 SE93 38, 47
 SM21 106
 SM30 35
 SM49 108
 SP01 auf eigenen Listen 116
 ST01 102
 START_REPORT 45
 Statusbericht Rollen 52
 SU01 41
 SU20 95, 99
 SU21 13, 169
 SU24 132, 137, 169
 SU53 bei S_TABU_NAM 44
 SU56 150
 SUIM 83
 Systemadministrator 54
 Systemkopie P nach Q 80

T

Tabelle AGR_1251 85, 173
 Tabelle AGR_1252 91
 Tabelle AGR_AGRS 25, 90
 Tabelle AGR_DEFINE 23, 89,
 163, 167
 Tabelle AGR_TEXTS 27
 Tabelle AGR_TIME 72
 Tabelle AGR_TIMEB 72
 Tabelle AGR_TIMEC 72

Tabelle AGR_TIMED 72
Tabelle AGR_USERS 86, 88
Tabelle SSM_CUST 149
Tabelle TACT 131
Tabelle TDDAT 36, 44
Tabelle TRDIR 44, 46
Tabelle TSTC 93
Tabelle TSTCP 93
Tabelle TSTCT 93
Tabelle USERS_SSM 149
Tabelle USOBT 138
Tabelle USOBX 138
Tabelle USOBX_C 137, 138
Tabelle UST04 91
Tabelle V_TBGR 36
Tabellenfeld BEGRU_B 100
Tabellenfeld KTOKD 100
Tabellenfeld KTOKK 100

U

Unvereinbarkeitsmatrix 124,
127
User-Sperre 56
USRBF2 67
UST04 66

V

Value-Rolle Definition 24
Vier-Augen-Prinzip 53, 60

W

Wer hat SAP_ALL 91
Werte-Rolle Definition 24

Z

Zahlalauf 77
ZCUST-Objekt 122
Z-Tabellen 37