espresso tutorials

Dr. Bernd Klüppelberg

Techniken im SAP®-Berechtigungswesen

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

Inhaltsverzeichnis

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

G

H

I

J

K

L

M

O

P

R

S

T

U

V

W

Z