Dieses Kapitel beschreibt die Einstellungen und Funktionen in der Rollen- und Berechtigungsadministration. Diese ermöglichen ein ausdifferenziertes Berechtigungskonzept und erleichtern Ihnen die Pflege der Berechtigungen.

7 Systemeinstellungen und Customizing

Der Aufbau dieses Kapitels folgt dem normativen Ansatz der Berechtigungspflege. Normativ ist der Ansatz, weil das Ziel der Regelkonformität (siehe Kapitel 4, »Rechtlicher Rahmen – normativer Rahmen«) nur durch möglichst präzise Regeln erreichbar ist. Aus den gesetzlichen Regeln müssen Regeln der Organisation werden. Aus diesen müssen wiederum für das Berechtigungskonzept technische Regeln werden. Die wichtigste technische Regel besteht darin, dass die Möglichkeiten des technischen Systems effizient genutzt und nicht umgangen werden.

Entsprechend ist Abschnitt 7.1, »Pflege und Nutzung der Vorschläge für den Profilgenerator«, den Berechtigungsvorschlagswerten gewidmet, die eine effiziente Pflege von Rollen erst ermöglichen. In Abschnitt 7.2, »Traces«, stellen wir die unterschiedlichen Tracemöglichkeiten vor. Abschnitt 7.3 beschreibt die Upgrade-Nacharbeiten von Berechtigungen. Wir beziehen uns in diesem Abschnitt systematisch auf die Tätigkeiten nach einem Upgrade im Bezug auf den Profilgenerator und somit auf die Überführung der Rollen, gestützt auf die Berechtigungsvorschlagswerte. Abschnitt 7.4 stellt schließlich »Parameter für Kennwortregeln« vor.

In Verbindung mit Kapitel 6, »Technische Grundlagen der Berechtigungspflege«, werden Sie mit diesen Abschnitten alle Einstellungen für den Betrieb eines normativ fundierten Berechtigungskonzepts kennengelernt und erfahren haben, welcher Zusammenhang zwischen den Möglichkeiten im SAP-System und den Anforderungen an die Regelkonformität besteht.

Die nächsten Abschnitte stellen wichtige Erweiterungen des Berechtigungskonzepts dar, die es Ihnen ermöglichen, Regelkonformität zu erreichen: Abschnitt 7.5, »Menükonzept«, beschreibt die Möglichkeiten eines normativen Menükonzepts, und Abschnitt 7.6 führt Sie in die Nutzung und Erweiterung von Berechtigungsgruppen in Bezug auf optionale Prüfungen und die Tabellenberechtigungen ein. In Abschnitt 7.7, »Parameter- und Query-Transaktionen«, erfahren Sie, wie Sie Tabellenzugriffe und Querys in Transaktionen umwandeln können, um zu verhindern, dass Endbenutzer direkte Tabellenzugriffe haben.

Um die Möglichkeiten, ein Standardberechtigungskonzept zu erstellen, auszuprägen und kundenspezifische Einstellungen, Transaktionen und Funktionen zu ergänzen, folgen die nächsten drei Abschnitte: Abschnitt 7.8, »Anhebung eines Berechtigungsfeldes zur Organisationsebene«, widmet sich der weiteren organisatorischen Differenzierung Ihres Berechtigungskonzepts mittels zusätzlicher Organisationsebenen. Abschnitt 7.9, »Berechtigungsfelder und -objekte anlegen«, beschreibt die Anlage eigener Berechtigungsobjekte. Abschnitt 7.10, »Weitere Transaktionen der Berechtigungsadministration«, stellt eine Sammlung weiterer nützlicher Transaktionen vor. Zusätzlich sollten Sie im Rahmen der Ermittlung von erforderlichen Berechtigungen vor allem in kundeneigenen Programmen die Informationen in Abschnitt 7.2, »Traces«, berücksichtigen.

7.1 Pflege und Nutzung der Vorschläge für den Profilgenerator

In diesem Abschnitt stellen wir die zentrale Funktion der Berechtigungsvorschlagswerte dar. Berechtigungsvorschläge sind vordefinierte Werte, die beim Anlegen und Ändern von Rollen auf Basis des Rollenmenüs als Berechtigungen vorgeschlagen werden. Sie erleichtern die effiziente und regelkonforme Pflege von Rollen.

Bedeutung der Vorschlagswerte

Abbildung 7.1 verdeutlicht die zentrale Bedeutung der Pflege der Berechtigungsvorschlagswerte sowohl für alle Aktivitäten der Rollenpflege als auch für alle analytischen Methoden. Im mittleren Bereich der Abbildung sehen Sie, dass für jede Anwendung (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) Berechtigungsvorschläge festgelegt werden. Diese Berechtigungsvorschläge können dann in der Rollenpflege übernommen werden. Darüber hinaus werden die Berechtigungsvorschlagswerte für die Risikoanalyse (kritische Aktionen, Funktionstrennungskonflikte) und die technische Analyse (Normeinhaltung) benötigt.

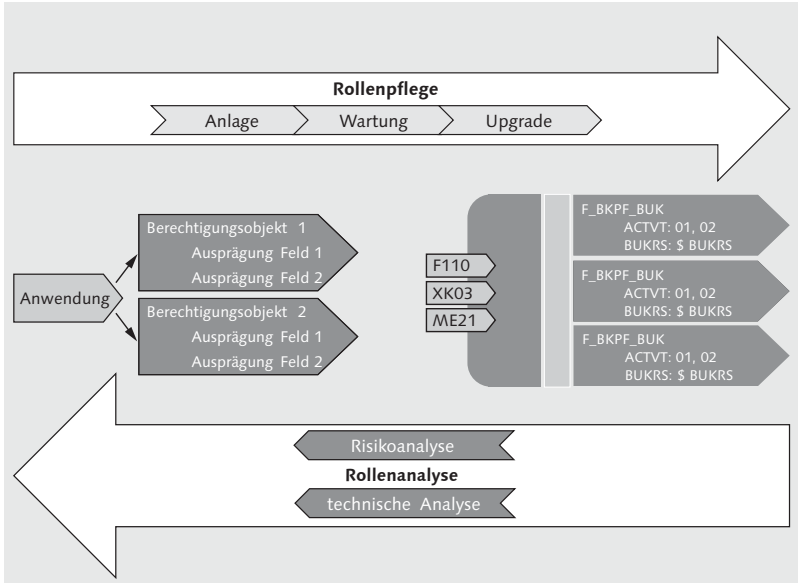


Abbildung 7.1 Berechtigungsvorschlagswerte – Unterstützung bei der Rollenpflege und -analyse

Nutzen der Vorschlagswerte

Wir werden im Folgenden darstellen, welchen Nutzen die Vorschlagswertpflege für folgende Bereiche hat:

- die Arbeit mit dem Profilgenerator (Anlage und Pflege von Rollen)
- die Berechtigungspflege beim Upgrade
- die Nachvollziehbarkeit der Regeleinhaltung
- ordentlich definierte Risikodefinitionen

In Abschnitt 6.3.1, »Manuelle Profile und Berechtigungen«, sind wir bereits auf die Funktion der Berechtigungsvorschlagswerte für den Profilgenerator eingegangen, die eine umfangreiche Automatisierung der Berechtigungspflege erlauben.

Berechtigungsvorschlagswerte enthalten eine Menge von Berechtigungen in Bezug auf jeweils eine Anwendung. Meistens werden je Anwendung zu mehreren Berechtigungsobjekten notwendige Werte vorgeschlagen. Den überwiegenden Teil dieser Vorschläge liefert

SAP aus. Die Berechtigungsvorschlagswerte müssen organisationsspezifisch ergänzt werden. Die Berechtigungsprüfungen sind unabhängig von den Vorschlagswerten, die Prüfung ist Teil des Programms. Die Berechtigungsvorschlagswerte sollten für diese Prüfung möglichst genaue Berechtigungsvorschläge in der Rollenpflege ermöglichen. Bevor wir den Nutzen der Berechtigungsvorschlagswerte darstellen, werden wir Ihnen zunächst ihren Grundzustand und ihre Pflege erläutern.

7.1.1 Grundzustand und Pflege der Berechtigungsvorschlagswerte

SAP liefert für alle dazu geeigneten Anwendungen Berechtigungsvorschlagswerte aus. Voraussetzung für die Berechtigungsvorschlagspflege ist, dass diese Berechtigungen im Programmcode der jeweiligen Anwendung als Berechtigungsprüfung implementiert sind. Nur diese Berechtigungsobjekte können als Berechtigungsvorschläge gepflegt werden. Die Berechtigungsprüfung ist allerdings abhängig von der Konfiguration der Prozesse und der Stammdatendefinition. Entschließt sich eine Organisation z. B., optionale Berechtigungsprüfungen einzusetzen, wird dies vermutlich weitere Berechtigungsprüfungen im Programmablauf zur Folge haben. Dieses Prinzip gilt für viele mögliche kundenspezifische Ausprägungen eines Prozesses in den Komponenten. Es gilt aber ebenso für die Integration der Komponenten. Mit anderen Worten: Berechtigungsvorschlagswerte sind teilweise zwingend systemspezifisch. Aus diesem Grund muss die Organisation die Berechtigungsvorschlagswerte entsprechend nachpflegen. Dazu wird die Transaktion SU24 (Pflege der Berechtigungsvorschlagswerte) genutzt.

Releasehinweis

Ab dem Basisrelease 7.02 steht eine Reihe neuer Funktionen für die Pflege der Berechtigungsvorschlagswerte zur Verfügung. Die folgenden Ausführungen beziehen sich auf Systeme mit einem Releasestand (SAP_BASIS) gleich oder größer 7.02.

Abbildung 7.2 verdeutlicht, wie die Pflege von Berechtigungsvorschlagswerten und Berechtigungen in aller Regel erfolgen soll. In der ersten Säule (Entwicklung) sehen Sie die Aufgaben der Entwicklung. Die Entwicklung legt die notwendigen Berechtigungsvorschläge fest.

Die Vorschlagswerte sollten zum Abschluss jeder Entwicklung vollständig vorliegen. Beim »Bauen einer Anwendung« legt die Entwicklung technisch fest, welche Berechtigungsobjekte im Zusammenhang mit einer Anwendung zu prüfen sind: Sie »baut den `Authority-Check`« mit konkreten Berechtigungsobjekten und ausgewählten Berechtigungswerten. Konkret: Wenn ein Entwickler in eine Anwendung einen `Authority-Check` z. B. auf `M_BEST_EKO` (Einkaufsorganisation in Bestellung) mit der Aktion Anlegen (`ACTVT`: `01`) und die zugehörige Einkaufsorganisation (`EKORG`: `$EKORG`) einbaut, dann weiß er, dass genau diese Berechtigung auch unter der Anwendung geprüft werden wird. Es ist also nur ein sehr geringer Aufwand, an dieser Stelle auch die Berechtigungsvorschlagswerte zu pflegen. Die nachträgliche Ermittlung von Vorschlagswerten beim Testen der Anwendung kostet bereits erheblich mehr. Die »historische« Ermittlung durch Mitarbeiter, die die Anwendung nicht gebaut haben, verursacht nahezu die Kosten eines erneuten Funktions- und Integrationstests.

Um eine nachträgliche Ermittlung der Vorschlagswerte zu umgehen, können Sie den Langzeitberechtigungstrace verwenden (siehe Abschnitt 7.2, »Traces«). Bei diesem Langzeittrace werden schon während der Entwicklung bzw. beim Aufruf der Anwendung Berechtigungsprüfungen getract und protokolliert.

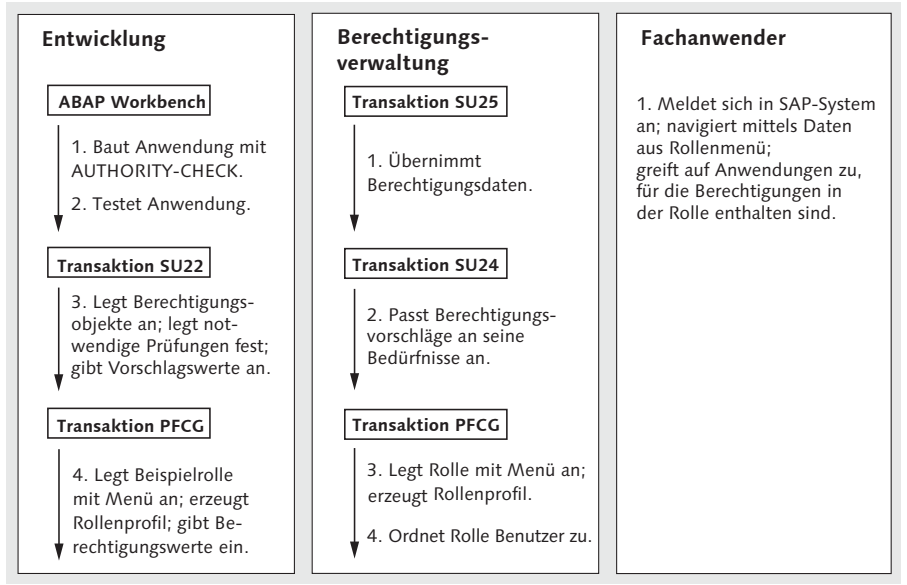


Abbildung 7.2 Von der programmierten Berechtigungsprüfung zur Rolle (nach: http://help.sap.com. SAP NetWeaver 7.0 EHP 3)

Für die Pflege von Vorschlagswerten nutzen SAP und ihre Entwicklungspartner die Transaktion SU22 (Berechtigungsvorschlagspflege – SAP). Generell können Sie für die Pflege von Berechtigungsvorschlagswerten die Transaktion SU24 (Berechtigungsvorschlagspflege) nutzen.

Für beide Transaktionen stehen (mittlerweile) Traces als Hilfsmittel zur Verfügung. Dabei handelt es sich um den Berechtigungstrace (siehe Abschnitt 7.2.1, »Vorgehen beim Berechtigungstrace«) und den Systemtrace (siehe Abschnitt 7.2.2, »Vorgehen beim Systemtrace«).

Pflege der Voschlagswerttabelle – Kundenwerte

In Abbildung 7.3 ist der Einstiegsbildschirm der Transaktion SU24 (Berechtigungsvorschlagspflege) dargestellt. Die Buttons Download ❶ und Upload ❷ dienen dem Down- und Upload der Werte; dies kann zur Sicherung oder zur Verteilung zwischen gleich konfigurierten Systemen nützlich sein. Der Button Berechtigungsvorlagen ❸ dient der Definition von Berechtigungsvorlagen, die in der Rollenpflege genutzt werden können. Diese Funktion betrachten wir nicht weiter, da wir eine Nutzung nicht empfehlen. Der Button Vorschlagswerteabgleich ❹ ermöglicht Ihnen einen selektiven Abgleich von Berechtigungsvorschlagswerten zwischen den SAP-Werten (Transaktion SU22) und den kundeneigenen Werten (Transaktion SU24). Dieser selektive Abgleich ist eine neue Funktion und steht systematisch mit Upgrade-Aktivitäten in Verbindung. Abhängig davon, für welche Anwendung Sie Berechtigungsvorschlagswerte pflegen wollen, selektieren Sie im Selektionsfeld Typ der Anwendung ❺ den entsprechenden Typ. Zur Verfügung stehen die folgenden Anwendungstypen:

- Transaktion
- Web-Dynpro-Applikation
- Web-Dynpro-Anwendungskonfiguration
- IDoc-Typ
- Workflowmuster
- RFC-Funktionsbaustein
- SAP Gateway: Service Groups Metadata
- SAP Gateway Business Suite Enablement – Service
- Zuordnung Service → Berechtigungsobjekt
- BSP-(Business-Server-Pages-)Applikation

- JCO-iView
- People Centric UI Service (CRM)
- Webservice
- CRM UIU Component
- CRM Web Channel Experience Management Module
- TADIR-Service
- externer Service
- Suche nach technischem Namen (Hashcode)

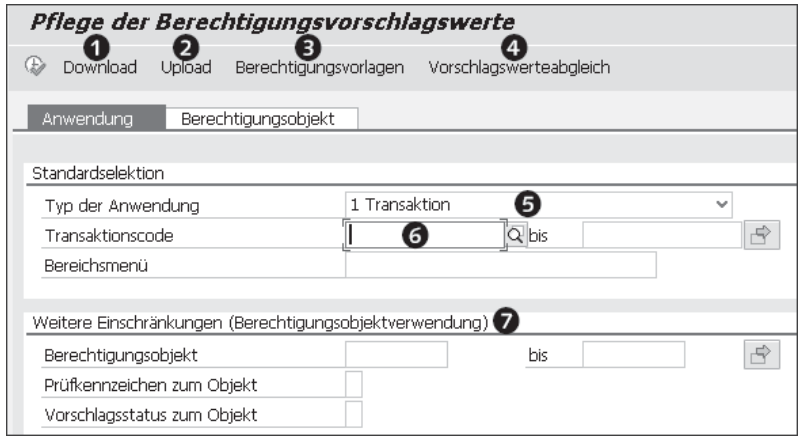


Abbildung 7.3 Einstieg in die Transaktion SU24 (Berechtigungsvorschlagspflege) – Auswahl »Transaktion«

Die Selektion einer Anwendung beeinflusst die weiteren Eingabemöglichkeiten. So sehen Sie die Selektion Transaktionscode ❻, in die ein oder mehrere Transaktionscodes eingetragen werden können. Unter Weitere Einschränkungen (Berechtigungsobjektverwendung) ❼ haben Sie die folgenden Möglichkeiten der Suche:

- Suche nach Anwendungen für ein bestimmtes Berechtigungsobjekt
- Suche nach einer Kombination aus Anwendung und Berechtigungsobjekt inklusive Prüfkennzeichen oder Vorschlagsstatus

Die Bearbeitung der Berechtigungsvorschlagswerte wird im Folgebildschirm vorgenommen (siehe Abbildung 7.4). Im mit ❶ gekennzeichneten Bereich finden Sie (von links nach rechts) folgende Buttons:

- (Anzeigen < – > Ändern): Mit diesem Button wechseln Sie zwischen Anzeige und Pflege der Berechtigungsvorschlagswerte.

- (Anderes Objekt): Mit diesem Button können Sie eine andere Anwendung oder ein anderes Objekt auswählen.
- SAP-Daten: Hier können Sie sich die SAP-Originaldaten anzeigen lassen.
- Berechtigungs-Trace: Ein oder Aus: Dieser Button informiert Sie zunächst darüber, ob der Berechtigungstrace (siehe Abschnitt 7.2.1, »Vorgehen beim Berechtigungstrace«) eingeschaltet ist. Wenn Sie daraufklicken, erhalten Sie eine Kurzinformation zum Berechtigungstrace.
- Abmischmodus für PFCG: Ein oder Aus: Über diesen Button erfahren Sie, ob der Abmischmodus für PFCG-Rollen ein- oder ausgeschaltet ist. Werden Änderungen an den Vorschlagswerten vorgenommen, so hat das Einfluss auf die Berechtigungswerte der PFCG-Rollen, die die jeweilige Anwendung im Rollenmenü beinhaltet. Ist der Abmischmodus eingeschaltet, werden betroffene Rollen in den Status Profilabgleich erforderlich gesetzt und bei der nächsten Änderung der Rolle berücksichtigt. Den Abmischmodus können Sie mittels des Parameters S42X_SET_FORCE_MIX in der Tabelle PRGN_CUST setzen.
- Rollen (Verwendung in Einzelrollen): Mithilfe dieses Buttons erhalten Sie Informationen, in welchen PFCG-Einzelrollen die ausgewählte Anwendung im Rollenmenü verwendet wird.

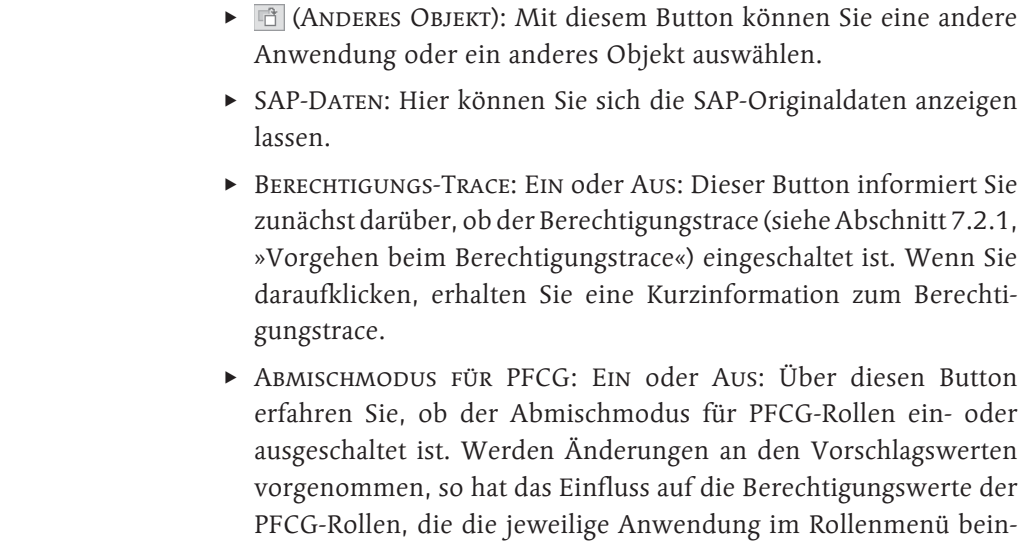


Abbildung 7.4 Transaktion SU24 (Berechtigungsvorschlagspflege) – Anzeige und Pflege

Im Bereich Selektionsergebnis ❷ sehen Sie die Menge der selektierten Objekte. Dies können, abhängig von der Selektion im Einstiegsbildschirm, entweder Transaktionen, Web-Dynpro-Applikationen, Web-Dynpro-Anwendungskonfigurationen, Workflowmuster, RFC-Funktionsbausteine, TADIR-Services, externe Services etc. sein. Durch Markieren einer Anwendung erscheinen im Bereich Berechtigungsobjekte ❸ die jeweils zugehörigen Objekte. Hier pflegen Sie die in Tabelle 7.1 spezifizierten Einstellungen. Dazu müssen Sie zunächst in den Änderungsmodus wechseln. In diesem Bereich sind alle Berechtigungsobjekte enthalten, die im Standard oder in den kundeneigenen Ausprägungen zugeordnet sind. Es handelt sich aber weder um alle Berechtigungsobjekte, die im System zur Verfügung stehen, noch unbedingt um alle, die im Programmablauf tatsächlich geprüft werden.

Im Bereich Berechtigungsvorschlagswerte ❹ können Sie für die in Bereich ❸ ausgewählten Berechtigungsobjekte Vorschlagswerte für die Berechtigungsfelder pflegen.

Im Änderungsmodus werden zusätzliche Buttons angeboten (siehe Abbildung 7.5). Zunächst jedoch sehen Sie im Titel ❶, dass Sie im Änderungsmodus sind. Mit dem Button Objekt ❷ können Sie sich (sofern unten ein Objekt selektiert ist) die Objektdefinition, die Objektdokumentation oder den Verwendungsnachweis anzeigen lassen. Sie können aber auch ein Objekt hinzufügen, entweder manuell ❷ oder aus dem Berechtigungstrace ❻ (siehe Abschnitt 7.2.1, »Vorgehen beim Berechtigungstrace«).

Abbildung 7.5 Transaktion SU24 (Berechtigungsvorschlagspflege) im Änderungsmodus: Zuordnungen und Status

Mit dem Button Prüfkennzeichen ❸ können Sie festlegen, ob ein Objekt im Programmablauf geprüft werden soll.

Das Prüfkennzeichen kann die in Tabelle 7.1 dargestellten Ausprägungen haben, in der Spalte Funktion wird die Wirkung beschrieben. Auf der folgenden Seite beschreiben wir in einem kurzen Exkurs die Funktion des Kennzeichens »nicht prüfen« etwas genauer.

Funktion	Prfkz.
Prüfkennzeichen wurde nicht spezifiziert – Berechtigungsobjekt wird geprüft.	–
Berechtigungsobjekt wird unter der Anwendung nicht geprüft.	nicht prüfen
Berechtigungsobjekt wird unter der Anwendung geprüft.	prüfen

Tabelle 7.1 Prüfkennzeichen für Berechtigungsobjektprüfungen unter Anwendungen

Sie legen über das Prüfkennzeichen fest, ob ein Objekt unter der Anwendung geprüft werden soll. Das Prüfkennzeichen wird in die Tabelle USOBX_C (Checktabelle zu Tabelle USOBT_C) eingetragen und definiert, ob ein Berechtigungsobjekt unter der Anwendung geprüft werden muss. Beachten Sie in jedem Fall, dass Sie die Unterdrückung auch transportieren oder manuell im Zielsystem vornehmen müssen. Da das Unterdrücken der Prüfung kritisch ist, unternehmen wir an dieser Stelle einen Exkurs zum Ausschalten von Prüfungen.

Exkurs: Verringerung des Umfangs von Berechtigungsprüfungen

Eine etwaige Unterdrückung der Berechtigungsprüfung kann nur nach genauer Prüfung und Dokumentation der Prüfungsergebnisse vorgenommen werden. Um Prüfungen über die Transaktion SU24 (Berechtigungsobjektprüfungen unter Transaktionen) wirksam unterdrücken zu können, muss der Profilparameter (Parameter `auth/no_check_in_some_cases`) auf `Y` gesetzt sein (Default). Diese Einstellung ist ebenfalls nötig, um den Profilgenerator überhaupt nutzen zu können.

Berechtigungsprüfungen von Berechtigungsobjekten, die zu Komponenten der Basis oder von SAP ERP Human Capital Management (HCM) gehören, lassen sich nicht unterdrücken.

Bei der Prüfung von Berechtigungskonzepten müssen Sie auf jeden Fall klären, welche Einstellungen zur Unterdrückung von Prüfungen vorgenommen wurden. Dabei gilt die Maßgabe, dass SAP-seitig vorgenommene Unterdrückungen Standard sind und kundenseitig angelegte Unterdrückungen erklärungs- und nachweisbedürftig sind.

Die Überprüfung auf Änderungen in diesem Sinne muss als kompensierende Kontrolle durchgeführt werden. Dazu wird die Tabelle USOBX_C (Checktabelle zu Tabelle USOBT_C) im Feld OK-Kennzeichen mit dem Wert `N` (keine Berechtigungsprüfung) und dem Feld Änderer = »SAP« ausgewertet.

Über den Button Vorschlag ❹ in Abbildung 7.5 legen Sie fest, ob und wie das selektierte Berechtigungsobjekt zu einer Anwendung in einer Rolle vorgeschlagen werden soll. Ihre Wahl wird dann in der Spalte Vorschlag durch ein Ja oder Nein ❽ kenntlich gemacht. Die Wirkung ist in Tabelle 7.2 zusammengefasst.

Status	Wirkung
Ja	Das Berechtigungsobjekt wird in einer Rolle vorgeschlagen und muss mit Werten ausgeprägt werden. Einige Felder enthalten bereits Vorschlagswerte.
Ja ohne Werte	Das Berechtigungsobjekt wird in einer Rolle vorgeschlagen. Es gibt allerdings keine gepflegten Vorschläge für Werte.
Nein	Das Berechtigungsobjekt wird nicht vorgeschlagen.
Neu/Ungepflegt	Das Berechtigungsobjekt wird zurückgesetzt und erhält in der Spalte Status ❾ eine rote Ampel.

Tabelle 7.2 Vorschlag und Status

Pflege der Berechtigungsvorschlagswerte auf Feldebene

Nachdem Sie das Vorschlagsverhalten festgelegt haben, können Sie nun über den Button Feldwerte ❺ detailliert die Werte pflegen, die vorgeschlagen werden sollen. Sinnvollerweise werden nur die Werte eingetragen (Bereich Berechtigungsvorschlagswerte ❹ der Abbildung 7.4), für deren Notwendigkeit es einen positiven Nachweis gibt. Dieser Nachweis ist in aller Regel ein Trace. Aus diesem Grund empfehlen wir, über die Auswertung der Traces ❻ die Berechtigungsvorschlagswerte zu pflegen.

Die Übernahme aus den Traces in die Berechtigungsvorschlagswerte entspricht dem in Abschnitt 6.6, »Vom Trace zur Rolle«, dargestellten Vorgehen. Darum werden wir dies an dieser Stelle nicht weiter ausführen.

Zur Feldpflege muss das Objekt zum Vorschlag bestimmt sein (Vorschlag JA). Sofern Sie eindeutige Feldwerte ermittelt haben, können diese als Vorschlag eingetragen werden. Sie können keine Organisationsebenen eintragen. Die anderen Werte müssen nach sorgfältiger Prüfung eingetragen werden. Oft besteht die erforderliche Eindeutigkeit nur in Bezug auf die Aktivität.

Sie können das am Beispiel der Bestellung nachvollziehen: Wenn Sie wollen, dass mit der Transaktion ME23N (Bestellung anzeigen) ausschließlich Bestellungen angezeigt werden können, müssten Sie jeweils im Feld ACTVT (AKTIVITÄT) die Werte 03 (ANZEIGEN) und 08 (ÄNDERUNGSBELEGE ANZEIGEN) mitgeben. Da es aber wahrscheinlich erforderlich ist, den Zugriff organisatorisch zu differenzieren, können Sie im Feld BELEGART IN BESTELLUNG (BSART) keinen Wert eintragen, da die Belegart ein ablauforganisatorisches Kriterium ist und Sie den Zugriff wahrscheinlich für einzelne Belegarten unterschiedlich ausprägen wollen.

Dieses Vorgehen ist erforderlich, um einerseits das Berechtigungsobjekt und die Aktivität automatisch vorgeschlagen zu bekommen. Anderseits wollen Sie verhindern, dass Sie das Feld BELEGART ändern müssen, da dies den Status des Objekts auf VERÄNDERT im Profil setzen würde.

Enjoy-Transaktionen

Die Transaktionen zur Bestellung sind deswegen ein gutes Beispiel, weil sie als Enjoy-Transaktionen prinzipiell vergleichbare Aktionen erlauben: Wenn die entsprechenden Berechtigungen zur Transaktion vergeben sind, kann aus der Transaktion ME23N (Bestellung anzeigen) eine Bestellung auch angelegt oder geändert werden (siehe SAP-Hinweis 751129 – Berechtigungen in Enjoy-Transaktionen im Einkauf). Die zu pflegenden Werte ergeben sich aus Ihrer Nutzung der Enjoy-Logik. Für das Beispiel der Transaktion ME23N (Bestellung anzeigen) heißt das:

- ausnahmslos Enjoy-Logik nutzen = Anlegen, Ändern, Anzeigen
- überwiegend Enjoy-Logik nutzen = keine Werte
- Enjoy-Logik nicht nutzen = Anzeigen

Berechtigungsvorschlagswerte stellen die mächtigste positiv regelbasierte Steuerung von Berechtigungen dar. Sie verleiten allerdings unter Umständen dazu, sie einfach zu übernehmen. Das kann jedoch falsch sein: Wenn Sie also die Transaktion ME23N (Bestellung anzeigen) tatsächlich nur zum Anzeigen nutzen wollen, wenn Sie aber die

Werte ANLEGEN, ÄNDERN und ANZEIGEN zulassen, wird mit Sicherheit irgendwann dieser Wert auch so in eine Rolle, die nur das Anzeigen erlauben soll, aufgenommen.

Obligatorischer Transportauftrag

Sämtliche Änderungen der Berechtigungsvorschlagswerte werden in einen Transportauftrag übernommen. Dabei sollten Sie die üblichen Empfehlungen zur Transport Policy und Ihre hauseigene Policy beachten.

Vorschlagswerttabellen und ihre Relation

Änderungen der Vorschläge für den Profilgenerator werden in unterschiedliche Tabellen geschrieben. Die Tabelle USOBT (Relation Transaktion R Ber.objekt) enthält die Auslieferungsdaten für Vorschläge. Die kundenseitigen Änderungen der Berechtigungsvorschlagswerte werden in die Tabelle USOBT_C (Relation Transaktion R Berechtigungsobjekt – Kunde) eingetragen. Die Tabelle USOBX (Checktabelle zu Tabelle USOBT) enthält die Auslieferungsdaten für Prüfkennzeichen. Die kundenseitigen Änderungen der Prüfkennzeichen werden in die Tabelle USOBX_C (Checktabelle zu Tabelle USOBT_C) eingetragen.

In Abbildung 7.6 sind beispielhaft drei Änderungen vorgenommen: In Bezug auf die Transaktion ME21N (Bestellung anlegen) wurde das Berechtigungsobjekt F_FICA_FOG (Haushaltsmanagement: Berechtigungsgruppe des Fonds) auf »nicht prüfen« gesetzt ❶, das Berechtigungsobjekt F_FICA_FCD – (Haushaltsmanagement Fonds) wurde auf Vorschlag JA gesetzt ❷, und im Feld AKTIVITÄT BERECHTIGUNGSPRÜFUNG (FM_AUTHACT) ❸ wurden die Aktionen 01, 02, 08 und 10 eingetragen.

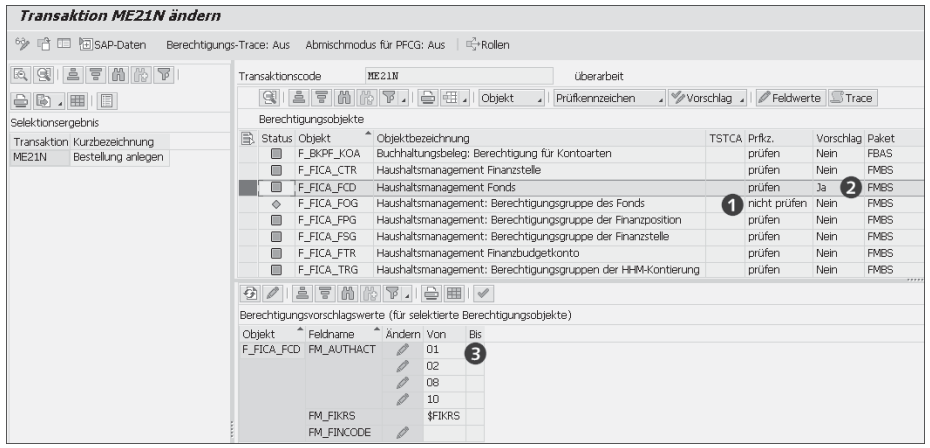


Abbildung 7.6 Exemplarische Pflege von Berechtigungsobjekten

Diese Änderungen wirken sich nicht auf die Tabelle USOBT (Relation Transaktion → Ber.objekt) und die Tabelle USOBX (Checktabelle zu Tabelle USOBT) aus. Stattdessen werden die Werte in die Tabelle USOBT_C (Relation Transaktion → Berechtigungsobjekt – Kunde) und die Tabelle USOBX_C (Checktabelle zu Tabelle USOBT_C) eingetragen.

In der Tabelle USOBT_C (Relation Transaktion R Berechtigungsobjekt – Kunde) ergeben sich durch die Änderung die in Tabelle 7.3 dargestellten Einträge. Aus der Tabelle sind zur Vereinfachung nur die folgenden Spalten dargestellt:

- Object = Berechtigungsobjekt
- Field = Berechtigungsfeld
- Low = Einzelwert oder der kleinste Wert eines Intervalls
- Modifier = letzter Änderer
- Modified = Kennzeichen für Änderung

OBJECT	FIELD	LOW	MODIFIER	MODIFIED
F_FICA_FCD	FM_AUTHACT	01	I055366	X
F_FICA_FCD	FM_AUTHACT	02	I055366	X
F_FICA_FCD	FM_AUTHACT	08	I055366	X
F_FICA_FCD	FM_AUTHACT	10	I055366	X
F_FICA_FCD	FM_FIKRS	$FIKRS	I055366	X
F_FICA_FCD	FM_FINCODE		I055366	X

Tabelle 7.3 Tabelle »Relation Transaktion ? Ber.objekt (Kunde)« nach Anpassung

Die erste Zeile bedeutet also, dass im Berechtigungsobjekt F_FICA_FCD das Feld FM_AUTHACT mit dem generischen Wert * durch den Benutzer I055366 geändert wurde.

In der Tabelle USOBX_C (Checktabelle zu Tabelle USOBT_C) ergeben sich die in Tabelle 7.4 dargestellten Einträge.

OBJECT	MODIFIER	OKFLAG	MODIFIED
F_FICA_FCD	I055366	Y	X
F_FICA_FOG	I055366	N	X

Tabelle 7.4 Tabelle »Checktabelle zu Tabelle USOBT_C« nach Anpassung

Die Änderungshistorie können Sie den in Tabelle 7.5 benannten Tabellen entnehmen.

Tabelle	Bezeichnung
USOBT_CD	Änderungshistorie für Feldwerte
USOBX_CD	Änderungshistorie zu Prüfkennzeichen

Tabelle 7.5 Weitere Tabellen zu Berechtigungsvorschlagswerten

Wenn die Berechtigungsvorschlagswerte gut gepflegt und in den Rollen entsprechend verwendet werden, kann ein Upgrade zügig durchgeführt werden. Zum Upgrade kommen wir im nächsten Abschnitt.

Der Vollständigkeit halber kommen wir noch einmal auf Abbildung 7.5 zurück. Dort hatten wir noch nicht darauf hingewiesen, dass ein Startberechtigungsobjekt in der Spalte TSTCA dieser Abbildung unter ❼ besonders gekennzeichnet ist.

7.1.2 Nutzen der Berechtigungsvorschlagswerte

Eine umfassende Pflege der Berechtigungsvorschlagswerte in Verbindung mit dem angegebenen Statusziel hat folgenden Nutzen:

- **Funktion für den Profilgenerator**
  Berechtigungspflege erfolgt regelbasiert statt *by incident*. Konkret wird eine technische Regel hinterlegt, welche Berechtigungsobjekte mit welchen Feldwerten zu einer Anwendung (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) gehören und somit in den Berechtigungen einer Rolle vorgeschlagen werden sollen. Da diese Feldwerte, Aktivitäten und differenzierenden Merkmale die konkrete Nutzung bestimmen, ist diese technische Regel auch gleichzeitig eine Norm in Bezug auf die statthaften Aktivitäten (z. B. Vorerfassen) einer Verrichtung (z. B. Belegbearbeitung). Diese Normbildung unterstützt die Regelkonformität und die Transparenz über die Erreichung der Regelkonformität. Eine detaillierte Beschreibung dazu finden Sie im Unterabschnitt »Funktion für den Profilgenerator« in diesem Abschnitt.

  Eine weitere Funktion für den Profilgenerators ist es, Erfahrungswissen zu sichern, indem Sie nicht jedes Mal neu ermitteln müssen, welche Berechtigungsobjekte für eine bestimmte Anwendung

(Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) nötig sind. Diese Funktion steigert die Effizienz und Nachhaltigkeit.

Schließlich ermöglicht die Pflege über den Profilgenerator, Rollen sauber zu halten (entzogene Anwendungen – Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc. – führen zum Entzug von Berechtigungen), auch diese Funktion sichert Regelkonformität.

- **Funktion im Upgrade**
  Die Pflege der Berechtigungsvorschlagswerte soll die Upgrade-Kosten angemessen halten. Diese Funktion ist Ausdruck der Effizienz, die bei präziser Pflege erreicht werden kann. Mehr dazu erfahren Sie im Unterabschnitt »Funktion im Upgrade« in diesem Abschnitt.
- **Normativer Nutzen**
  Pflege der Berechtigungsvorschlagswerte soll die Auditierbarkeit sicherstellen. Der technisch definierte Zusammenhang zwischen Anwendung (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) und Berechtigungsobjekt erleichtert sinnvolle Audits von Berechtigungskonzepten. Ausführliche Informationen dazu finden Sie im Unterabschnitt »Normativer Nutzen« in diesem Abschnitt.
- **Nutzen für die Risikoanalyse**
  Die Pflege der Berechtigungsvorschlagswerte soll sicherstellen, dass bei der Definition von Risiken in einem Werkzeug wie SAP Access Control die »richtigen« Werte genutzt werden. Alle selbst erstellten Risikodefinitionen basieren auf den Werten der Vorschlagstabellen. Dazu finden Sie eine detaillierte Beschreibung im Unterabschnitt »Nutzen der Berechtigungsvorschlagswerte für Risikoanalyse und externe Rollenpflegetools« in diesem Abschnitt.

Die Pflege der Berechtigungsvorschlagswerte für den Profilgenerator vereinfacht mittelfristig die Rollenpflege und macht sie transparenter.

Funktion für den Profilgenerator

Die Berechtigungsvorschlagswerte für Berechtigungen werden – im Kundensystem – über die Transaktion SU24 (Pflege der Zuordnungen von Berechtigungsobjekten zu Transaktionen) gepflegt. Sie versorgen den Profilgenerator mit Vorschlägen für Berechtigungswerte. Jede im Menü eingefügte Anwendung (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) wird mit diesen Default-Werten versorgt. Abbildung 7.7 verdeutlicht, dass in Bezug auf die im Menü vergebene Anwendung die Berechtigungsvorschlagswerte in die Berechtigungen zur Rolle übernommen werden.

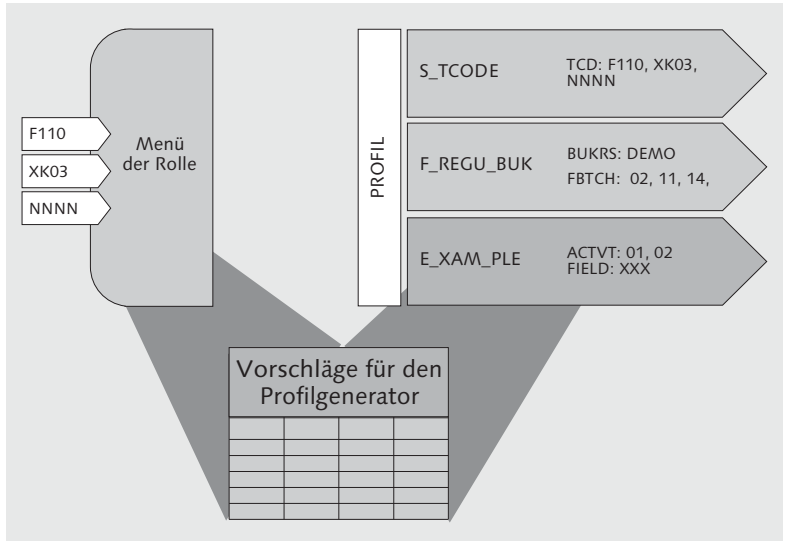


Abbildung 7.7 Übernahme der Berechtigungsvorschlagswerte für die im Menü vergebenen Anwendungen (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.)

Übernahme von Berechtigungsvorschlagswerten

Die Übernahme von Berechtigungsvorschlagswerten funktioniert bei der Rollenänderung im Menü entweder, indem Sie auf der Registerkarte Berechtigungen den Button Berechtigungsdaten ändern wählen oder auf den Button Expertenmodus zur Profilgenerierung klicken und dort Alten Stand lesen und mit den neuen Daten abgleichen auswählen. Die Pflege über den Expertenmodus sollte der Standard sein, da Sie in diesem Fall selbst festlegen, wie sich der Profilgenerator verhalten soll. Nach der Selektion springen Sie in die Pflege der Berechtigungen. Dabei fallen die unterschiedlichen Status der Berechtigungen auf, die wir schon in Abschnitt 6.3.2, »Rollenpflege«, erläutert haben.

Berechtigungsobjekte können vier Status haben:

- Manuell: Das ganze Objekt wurde manuell hinzugefügt.
- Verändert: Der Vorschlagswert wurde verändert.

- GEPFLEGT: Entspricht dem Vorschlagswert, es wurden offene Felder gepflegt.
- STANDARD: Entspricht dem Vorschlagswert.

Der Unterschied zwischen Pflegen und Verändern besteht darin, dass bei der Pflege offene Felder gepflegt, bei der Veränderung dagegen Standardfeldausprägungen verändert werden.

Status und Entzug von Anwendungen

Dieser Unterschied ist relevant. Der Mechanismus, der beim Ergänzen einer Rolle um eine Anwendung (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) abläuft, arbeitet analog beim Entziehen einer Anwendung. Die Berechtigungsobjekte im Status GEPFLEGT oder STANDARD, die ausschließlich zur entzogenen Anwendung gehören, werden wieder entzogen. Damit wird einem Kernproblem oft veränderter Rollen vorgebeugt: dem Problem, dass es keine nachhaltige logische Zuordnung von enthaltenen Berechtigungsobjekten zu den vergebenen Anwendungen gibt.

Beispiel: Verwendung von Berechtigungsobjekten in Rollen und deren Pflegestatus

Dies soll an einem Beispiel dargestellt werden: Einer Rolle, die ausschließlich Reporting-Transaktionen enthält, wird die Transaktion SQVI (QuickViewer) hinzugefügt. Da das Berechtigungsobjekt für Tabellenzugriffe (`S_TABU_DIS`) kein Standardvorschlag ist, wird es manuell der Rolle hinzugefügt. Später wird – ganz im Sinne wünschenswerter Regelkonformität – die Nutzung des QuickViewers massiv eingeschränkt, die Transaktion wird der Reporting-Rolle entzogen. Da das Berechtigungsobjekt für Tabellenzugriffe manuell hinzugefügt wurde, verbleibt es in der Rolle. Das hat Folgen:

- Die Rolle enthält mehr Berechtigungen als erforderlich.
- Das Risiko, das in einer Kombination mit anderen Rollen entstehen kann, ist erheblich und nicht vorab zu bestimmen.

Je präziser die Default-Werte in den Tabellen gepflegt sind, desto genauer passen die Berechtigungsvorschlagswerte für die Rollen. Anzustreben ist minimal ein Zustand, in dem auf Objektebene 95 % aller Berechtigungsobjekte als Default in die Rolle übernommen werden. Das heißt, dass nur noch 5 % der Berechtigungsobjekte mit dem Status VERÄNDERT gekennzeichnet sind.

Da Berechtigungsausprägungen immer einen kundenspezifischen Anteil haben, d. h. durch die Konfiguration, das Stammdatenkonzept, aber auch individuelle Präferenzen bestimmt werden, sind die Standardberechtigungsvorschlagswerte unvollständig.

Standardvorschläge pflegen

Wir empfehlen Ihnen die detaillierte Pflege der Berechtigungsvorschlagswerte ausdrücklich auch für Standardanwendungen (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.), da sinnvolle Berechtigungsvorschlagswerte gegebenenfalls besondere Nutzungen, Systemeinstellungen und Stammdatenmerkmale reflektieren.

Funktion im Upgrade

Mit der Transaktion SU25 (Upgrade-Tool für den Profilgenerator) werden verschiedene Schritte vollzogen, um im Upgrade die alten Berechtigungen und Rollen den neuen Erfordernissen anpassen zu können. Im Prinzip werden dort die alten Berechtigungsvorschlagswerte (Kunde) mit den neuen Berechtigungsvorschlagswerten (SAP) abgemischt und die Rollen mit Änderungsbedarf identifiziert. Die Upgrade-Nacharbeiten bezüglich Berechtigungen selbst werden in Abschnitt 7.3, »Upgrade-Nacharbeiten von Berechtigungen«, beschrieben.

Normativer Nutzen

Aus den in Kapitel 4, »Rechtlicher Rahmen – normativer Rahmen«, angeführten Gründen sind immer nur die nachweislich notwendigen Berechtigungen zu vergeben. Soll ein Mitarbeiter Bestellungen ändern dürfen, dann muss er einen Benutzer im System mit genau diesen Berechtigungen bekommen. Technisch sollte dabei ein Zustand erreicht werden, in dem durch das Einfügen der Transaktion ME21N (Bestellung anlegen) alle notwendigen Berechtigungsobjekte mit allen erforderlichen aktivitätsbezogenen Feldwerten vorgeschlagen werden. Auf diese Weise müssen anschließend nur noch die organisatorischen Werte wie Werk/Belegart u. Ä. eintragen werden. Wird so vorgegangen, kann auch der Auditor nachvollziehen, dass die Ausprägung der Berechtigungen den im System hinterlegten Regeln entspricht. Stellen Sie sich eine Rolle mit 100 Anwendungen, 40 Berechtigungsobjekten und 120 Feldausprägungen in den Berechtigungsobjekten vor. Wenn sämtliche Objekte manuell hinzugefügt wurden, können Sie nicht mehr erkennen, welche Berechtigungsobjektausprägung für eine bestimmte Anwendung erforderlich ist und

ob für die 100 Anwendungen wirklich nur notwendige Werte vergeben wurden. Während Sie für eine Anwendung dies gegebenenfalls über einen Trace beweisen können, dürfte der Aufwand für 100 Anwendungen meistens zu groß sein.

Wenn Berechtigungsobjekte manuell einem Profil hinzugefügt oder geändert wurden, besteht keine Relation zwischen dem Umfang an Anwendungen der Rolle (Transaktion, Web Dynpro, RFC-Funktionsbausteine, externe Services etc.) und den zugeordneten Berechtigungsobjekten. Das bedeutet, dass keine Auskunft darüber möglich ist, warum etwa ein kritisches Objekt einer Rolle zugeordnet wurde.

Vorschlagstabelle und Regelkonformität

Es besteht ein direkter Zusammenhang zwischen der Nutzung der Berechtigungsvorschlagswerte und der Regelkonformität von Berechtigungen. Berechtigungen können in einem komplexen System wie SAP ERP nur dann regelkonform sein, wenn sie technischen Regeln folgen – das sind die Berechtigungsvorschlagswerte.

Ohne Nachvollziehbarkeit keine wirksame Prüfung

Nur wenn nachvollziehbar bleibt, warum welche Berechtigungsobjekte und Werte vergeben wurden, kann die Regelkonformität von Rollen effizient geprüft werden. Diese Prüfbarkeit entsteht über die Berechtigungsvorschlagswerte.

Im Sinne eines umfassenden Verständnisses des Internen Kontrollsystems (IKS) ist ein Nachweis erforderlich, warum welcher Benutzer welche Berechtigungen hat, also auch warum eine Rolle ein bestimmtes Berechtigungsobjekt enthält. Dieser Nachweis auf Objektebene ist ohne vorschlagswertbasierte Pflege nicht möglich. Die Vorschlagswertpflege ist in diesem Sinne eine Normsetzung, wie Berechtigungen ausgesteuert werden dürfen. Die Umsetzung ist der Nachweis, ob die Norm eingehalten wurde. Die Norm selbst ist Ausdruck eines technisch detaillierten IKS.

Nutzen der Berechtigungsvorschlagswerte für Risikoanalyse und externe Rollenpflegetools

Eine detaillierte Analyse von Funktionstrennungskonflikten und kritischen Transaktionen kann nur durchgeführt werden, wenn die kundenspezifischen Berechtigungsvorschlagswerte eingeschlossen werden: Die Präzisierung der Berechtigungsvorschlagswerte stellt eine Präzisierung der notwendigen Werte für Zugriffe und somit für Risiken dar. Diese Systematik ist u. a. in der Definition neuer Risiken in SAP Access Control enthalten.

Um das an einem Beispiel darzustellen: Das mit dem Anlegen einer Bestellung verbundene Risiko wird dargestellt, indem zunächst festgestellt wird, dass die Transaktion ME21N notwendig ist. Diese sehr einfache Risikodefinition ist in Tabelle 7.6 zusammengefasst.

Anwendung	Berechtigungsobjekt	Feld	Ausprägung
ME21N	S_TCODE	TCD	ME21N

Tabelle 7.6 Einfache Risikodefinition

Mit dieser Transaktion allein kann ein Benutzer nicht viel anfangen, er benötigt in jedem Fall noch drei Berechtigungsobjekte mit den entsprechenden Ausprägungen. Mit anderen Worten: Die in Tabelle 7.6 dargestellte Definition ist zu einfach, sie wird zu falschen Befunden führen, denn jeder, der die Transaktion ME21N (Bestellung anlegen) überhaupt hat, wird erfasst.

Gute Berechtigungsvorschlagswerte – präzise Risikodefinitionen

Dementsprechend muss die Risikodefinition ergänzt werden, um sicherzustellen, dass auch nur die echten Risiken nachgewiesen werden. Dies ist exemplarisch in Tabelle 7.7 dargestellt. Wie detailliert ein Risiko zu beschreiben ist, behandeln wir in Kapitel 11, »SAP Access Control«. An dieser Stelle soll nur Folgendes deutlich werden: Ohne die Berechtigungsvorschlagswerte können Sie ein Risiko nur präzise definieren, indem Sie ersatzweise Transaktion für Transaktion tracen.

Anwendung	Berechtigungsobjekt	Feld	Ausprägung
ME21N	S_TCODE	TCD	ME21N
	M_BEST_BSA	ACTVT	01
		BSART	FO, NB
	M_BEST_EKG	ACTVT	01
		EKGRP	$EKRGP
	M_BEST_EKO	ACTVT	01
		EKORG	$EKORG

Tabelle 7.7 Präzise Risikodefinition

Das Gleiche gilt sinngemäß für alle Risikoanalyselösungen – inklusive der selbst gebauten. Sind diese nicht mit den Vorschlagstabellen integriert, können sie nicht dauerhaft die Rollenpflege Upgrade-

sicher und regelkonform vereinfachen. Das gilt auch für die Nutzung des Business Role Managements von SAP Access Control. Die Nutzung im Rollenmanagement und in der Risikoanalyse wird in Abbildung 7.8 verdeutlicht. Zu sehen ist, dass die Werte der Tabelle USOBT_C einerseits in der Risikoanalyse und andererseits im Rollenmanagement Verwendung finden.

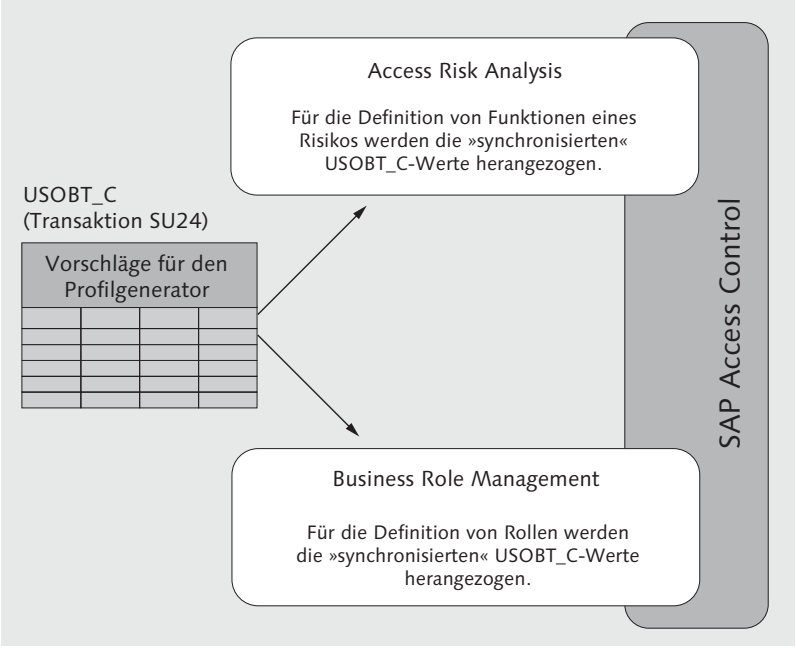


Abbildung 7.8 Nutzung der Berechtigungsvorschlagswerte für die Risikoanalyse und externe Rollenpflegelösungen

7.2 Traces

In Abschnitt 7.1.1, »Grundzustand und Pflege der Berechtigungsvorschlagswerte«, wurde der Trace als Hilfsmittel für die Ermittlung der relevanten Vorschlagswerte und in Abschnitt 6.6, »Vom Trace zur Rolle«, als Hilfsmittel für die Rollenpflege und für die Vorschlagswertpflege dargestellt. In diesem Abschnitt sollen die beiden Traces systematisch erläutert werden. Ein Trace ist in unserem Kontext und stark vereinfacht eine Aufzeichnung von Benutzeraktionen und Systemreaktionen.

Hinweis aus der Entwicklung

Ein Entwickler braucht für seine Anwendung keinen Trace, er kann aus den von ihm »eingebauten« Berechtigungsprüfungen unmittelbar die notwendigen Berechtigungsvorschläge ohne nennenswerten Aufwand festlegen.

Tracearten

Es stehen Ihnen drei Arten von Traces zur Verfügung: der Berechtigungstrace, der Systemtrace und der Benutzertrace:

Berechtigungstrace

Für die erste Befüllung der Tabelle USOBX (Checktabelle zu Tabelle USOBT) für den Profilgenerator wird SAP-intern der Berechtigungstrace genutzt. Dieser wird meistens als Langzeittrace verwendet, der mandantenübergreifend und benutzerunabhängig Daten sammelt und in der Datenbank ablegt. Sobald der Trace während der Ausführung eines Programms auf eine Berechtigungsprüfung stößt, die im Zusammenhang mit der aktuellen Anwendung bislang nicht erfasst war, legt er einen entsprechenden Eintrag in der Tracedatenbanktabelle an. Das bedeutet, dass Sie die Anwendung möglichst vollständig testen müssen, um aussagekräftige Tracedaten zu erhalten. Um den Trace auswerten zu können, müssen Sie ihn vor dem Testen/Aufzeichnen aktivieren und die wesentlichen Aktionen lokal oder im Zielsystem ausführen.

In SAP-Hinweis 543164 (Bedeutung der Werte von `auth/authorization_trace`) wird deutlich darauf hingewiesen, dass dieser Trace die Performance verringert und vom Kunden auf eigenes Risiko eingesetzt wird. Sinnvoll ist dieser Trace, um die Berechtigungsprüfungen von kundeneigenen Programmen in die Berechtigungsvorschlagswerte zu übertragen. Diese Übertragung ist eine manuelle Übernahme, da eine Bewertung erfolgen muss. Es ist ab Basisrelease 7.02 nicht mehr erforderlich, dazu die Transaktion SU22 (Berechtigungsvorschlagspflege – SAP) zu verwenden. Wie schon ausgeführt, steht für die Pflege von Berechtigungsvorschlagswerten die Transaktion SU24 (Berechtigungsvorschlagspflege) zur Verfügung. Dort können auch die Werte des Berechtigungstrace angezeigt werden, wie wir im Folgenden erläutern werden. Wir raten Ihnen dringend, diesen Profilparameter in produktiven Systemen inaktiv zu setzen – dies ist auch Auslieferungsstandard. Es ist aber durchaus empfehlenswert, diesen Trace auf dem Entwicklungs- und gegebenenfalls auch auf dem Qualitätssicherungssystem zu aktivieren, so sammeln Sie bereits während der Entwicklung von neuen Funktionen die ent-

sprechenden Berechtigungsvorschlagswerte. Profilparameter können über die Transaktion RZ11 (Pflege der Profilparameter) geändert werden.

Systemtrace Der Systemtrace (Transaktion ST01 oder STAUTHTRACE) ist ein Kurzzeittrace, der mandantenabhängig und nur auf dem aktuellen Anwendungsserver Berechtigungsdaten sammelt. In die Rollenpflege und die Vorschlagswertpflege müssen über RFC auch die Traceergebnisse aus beliebigen Zielmandanten eingebunden werden. Auch dieser Trace kann über RFC auf beliebigen Mandanten ausgeführt sowie ausgewertet werden.

Benutzertrace Der Benutzertrace ist ein neuer Trace, der ab SAP NetWeaver 7.40 verfügbar ist (siehe SAP-Hinweis 2220030). Er ist ebenfalls als Langzeittrace konzipiert, sammelt aber im Gegensatz zum Berechtigungstrace mandanten- und benutzerabhängige Berechtigungsdaten. Diese werden wie beim Berechtigungstrace in der Datenbank abgelegt. Analog zum Berechtigungstrace erfolgt die Aufzeichnung der Berechtigungsprüfungen. Dabei werden die laufende Anwendung mit der Programmstelle, das Berechtigungsobjekt und dessen geprüfte Werte sowie das Ergebnis der Berechtigungsprüfung pro Benutzer einmal gespeichert. Sie haben die Möglichkeit, die Aufzeichnung auf den Anwendungstyp, die Benutzer und die Berechtigungsobjekte hin zu filtern. Für den Filter können Sie zwei unterschiedliche Anwendungstypen, bis zu zehn Benutzer und bis zu zehn Berechtigungsobjekte festlegen.

Der Benutzertrace wird über den Profilparameter `auth/auth_user_trace` aktiviert. Sollten Sie den Benutzertrace mit einem Filter aktiviert haben, müssen Sie in der Transaktion STUSERTRACE auch einen Filter definieren, denn sonst wird nichts aufgezeichnet. Auch für den Benutzertrace gilt, dass die Aktivierung ohne einen Filter zu hohen Performanceeinbußen führen kann. Prüfen Sie daher die möglichen Anwendungsszenarien immer auch im Hinblick auf die Auswirkungen auf die Performance. Der Benutzertrace ist hilfreich bei Szenarien, in denen Sie spezielle Benutzer oder Berechtigungsobjekte auswerten wollen. Sie können z. B. die erforderlichen Berechtigungen für Batch-Benutzer oder Tabellenzugriffe über `S_TABU_NAM` aufzeichnen.

7.2.1 Vorgehen beim Berechtigungstrace

Zunächst müssen Sie die Transaktion RZ11 (Pflege der Profilparameter) aufrufen und den Parameter `auth/authorization_trace` eintragen (siehe Abbildung 7.9).

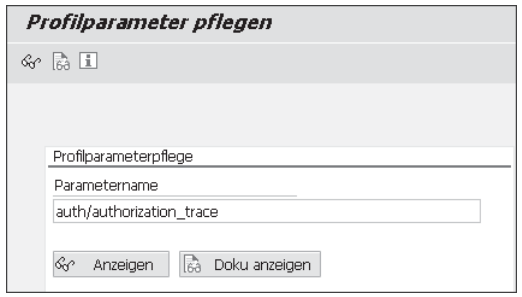


Abbildung 7.9 Profilparameterpflege für Berechtigungstrace

Klicken Sie auf den Button Anzeigen. Auf dem nächsten Bild Profilparametereigenschaften klicken Sie auf den Button Wert ändern (siehe Abbildung 7.10).

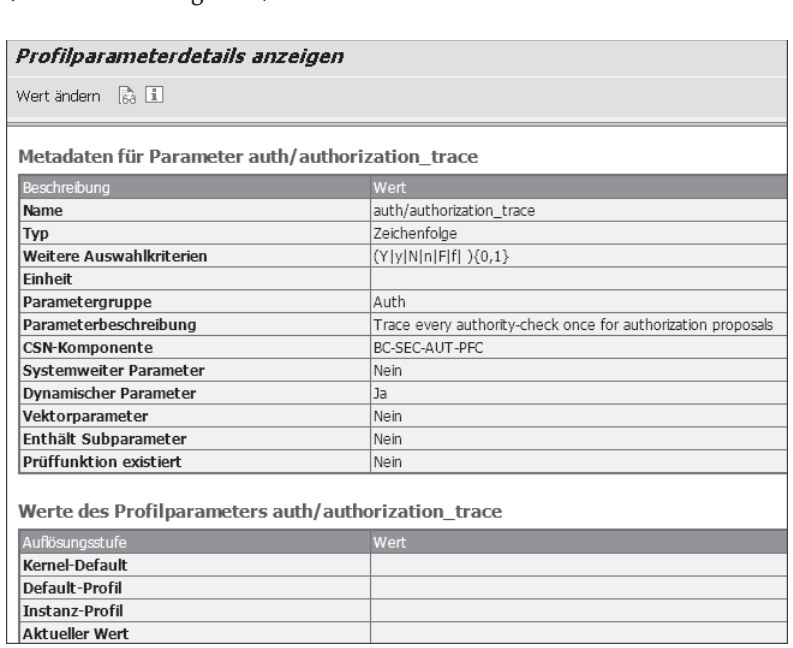


Abbildung 7.10 Profilparametereigenschaften

Auf dem folgenden Bild setzen Sie den Wert auf `Y` (aktiv) oder `F` (aktiv mit Filter) (siehe Abbildung 7.11). Den Filter für diesen Trace

können Sie über die Transaktion STUSOBTRACE festlegen und anhand der Kriterien Typ der Anwendung, Berechtigungsobjekte oder Benutzer einschränken. Den Warnhinweis Änderung nicht permanent, geht nach dem Neustart des Servers verloren bestätigen Sie, und anschließend bestätigen Sie Ihre Eingabe. Der Trace ist nun aktiv.

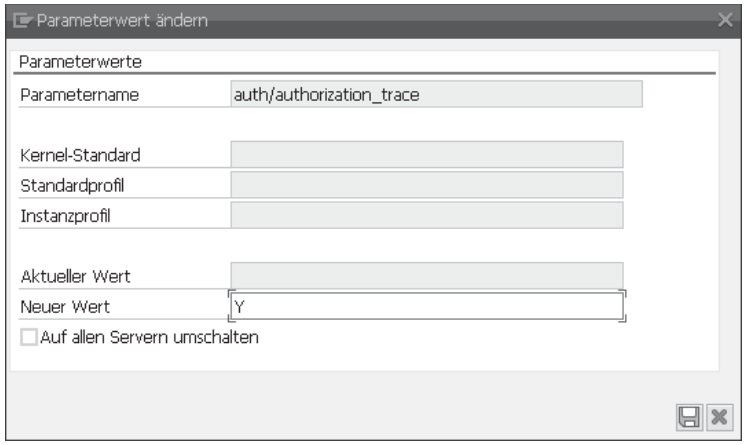


Abbildung 7.11 Parameterwert setzen

Transaktionen tracen

Führen Sie nun die Anwendung(en) aus, für die Sie die notwendigen Berechtigungsobjekte ermitteln wollen. In unserem Beispiel ist es die Transaktion, die wir in Abschnitt 7.7.1 angelegt haben, also eine Parametertransaktion zur Pflege von Tabellen über definierte Views.

Die Ergebnisse dieses Trace werden in die Tabelle USOB_AUTHVALTRC geschrieben und können ebenfalls in der Transaktion STUSOBTRACE über einen Klick auf den Button Auswerten eingesehen werden (siehe Abbildung 7.12).

Eintrag in die Berechtigungsvorschlagspflege

Für die Auswertung ist die Einschränkung Typ der Anwendung: Transaktion ausgewählt worden, damit nur Tracedaten für neue Transaktionen angezeigt werden. Die Auswertung (siehe Abbildung 7.13) listet nun für jede Transaktion Berechtigungsobjekte mit den geprüften Berechtigungswerten auf. Diese Informationen können Sie als Grundlage zur Pflege von Berechtigungsvorschlagswerten oder in der Rollenpflege verwenden.

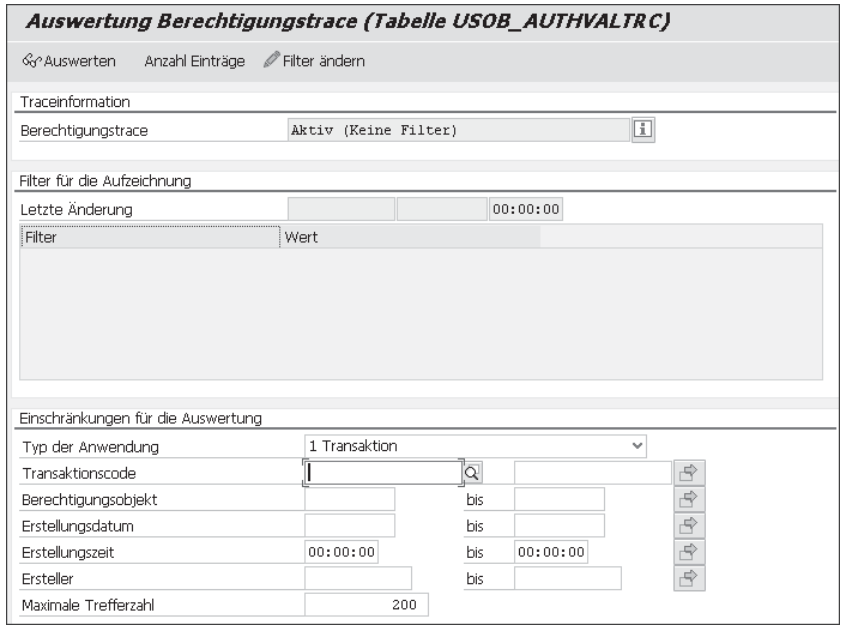
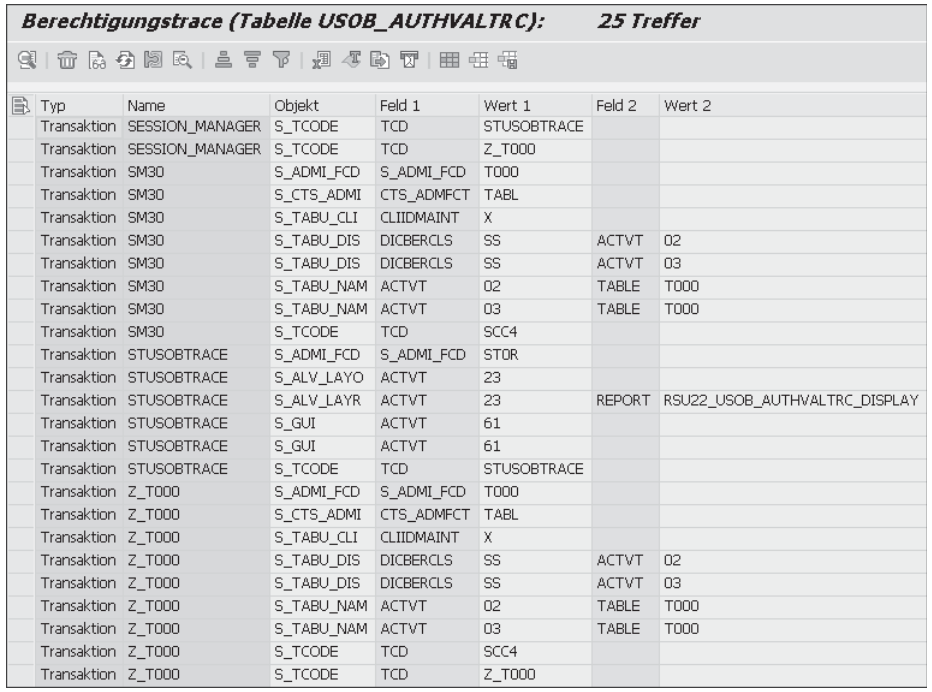


Abbildung 7.12 Auswertung des Berechtigungstrace über Transaktion STUSOBTRACE



Typ	Name	Objekt	Feld 1	Wert 1	Feld 2	Wert 2
Transaktion	SESSION_MANAGER	S_TCODE	TCD	STUSOBTRACE		
Transaktion	SESSION_MANAGER	S_TCODE	TCD	Z_T000		
Transaktion	SM30	S_ADMI_FCD	S_ADMI_FCD	T000		
Transaktion	SM30	S_CTS_ADMI	CTS_ADMFCT	TABL		
Transaktion	SM30	S_TABU_CLI	CLIIDMAINT	X		
Transaktion	SM30	S_TABU_DIS	DICBERCLS	SS	ACTVT	02
Transaktion	SM30	S_TABU_DIS	DICBERCLS	SS	ACTVT	03
Transaktion	SM30	S_TABU_NAM	ACTVT	02	TABLE	T000
Transaktion	SM30	S_TABU_NAM	ACTVT	03	TABLE	T000
Transaktion	SM30	S_TCODE	TCD	SCC4		
Transaktion	STUSOBTRACE	S_ADMI_FCD	S_ADMI_FCD	STOR		
Transaktion	STUSOBTRACE	S_ALV_LAYO	ACTVT	23		
Transaktion	STUSOBTRACE	S_ALV_LAYR	ACTVT	23	REPORT	RSU22_USOB_AUTHVALTRC_DISPLAY
Transaktion	STUSOBTRACE	S_GUI	ACTVT	61		
Transaktion	STUSOBTRACE	S_GUI	ACTVT	61		
Transaktion	STUSOBTRACE	S_TCODE	TCD	STUSOBTRACE		
Transaktion	Z_T000	S_ADMI_FCD	S_ADMI_FCD	T000		
Transaktion	Z_T000	S_CTS_ADMI	CTS_ADMFCT	TABL		
Transaktion	Z_T000	S_TABU_CLI	CLIIDMAINT	X		
Transaktion	Z_T000	S_TABU_DIS	DICBERCLS	SS	ACTVT	02
Transaktion	Z_T000	S_TABU_DIS	DICBERCLS	SS	ACTVT	03
Transaktion	Z_T000	S_TABU_NAM	ACTVT	02	TABLE	T000
Transaktion	Z_T000	S_TABU_NAM	ACTVT	03	TABLE	T000
Transaktion	Z_T000	S_TCODE	TCD	SCC4		
Transaktion	Z_T000	S_TCODE	TCD	Z_T000		

Abbildung 7.13 Auswertung des Berechtigungstrace

Starten Sie danach die Transaktion SU24 (Berechtigungsvorschlagspflege). In Abbildung 7.14 fällt im Bereich ❶ auf, dass keine Objekte enthalten sind. Sie erhalten den Hinweis Zu Ihrer Selektion existieren keine Berechtigungsobjektzuordnungen ❷. Dieser Hinweis bedeutet, dass es entweder keine Daten in der Transaktion SU22 gibt oder (der Regelfall) dass eine Übernahme noch nicht erfolgt ist. Der Button Berechtigungstrace: Ein ❸ zeigt an, dass der Berechtigungstrace aktuell eingeschaltet ist. Durch einen Klick auf den Button SAP-Daten ❹ können Sie die Übernahme der SAP-Daten starten. Sind keine SAP-Daten gepflegt, können Sie die Werte aus dem Berechtigungstrace durch einen Klick auf Objekt • Objekte aus Berechtigungstrace einfügen • Lokal einfügen.

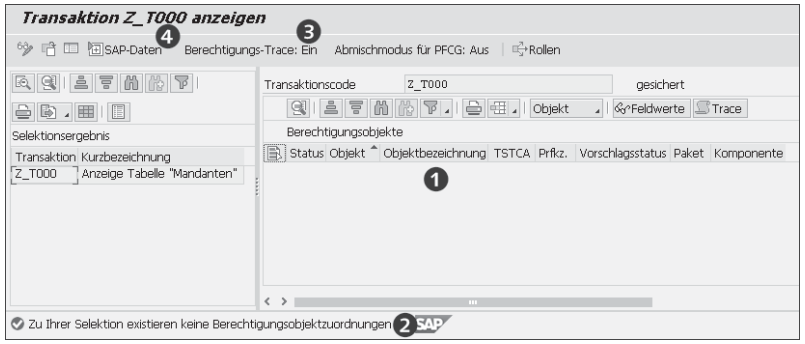


Abbildung 7.14 Werte für die kundeneigene Transaktion SU24 vor Übernahme der SAP-Daten

Berechtigungstrace für Berechtigungsvorschlagswerte und Rollenpflege

Die Werte des Berechtigungstrace stehen Ihnen auch in der Rollenpflege (Berechtigungen) zur Verfügung, siehe Abschnitt 6.6, »Vom Trace zur Rolle«.

Nach der Übernahme der SAP-Daten bzw. der Berechtigungsobjekte aus dem Berechtigungstrace sehen Sie die aufgezeichneten Objekte im Status ungepflegt (siehe Abbildung 7.15 ❶). Nun können Sie auf alle Tracewerte ❷ zur Pflege zugreifen, um die Berechtigungsvorschlagswerte auszuprägen. Die Funktion der Übernahme der Tracewerte ist vergleichbar mit dem in Abschnitt 6.6 dargestellten Verfahren.

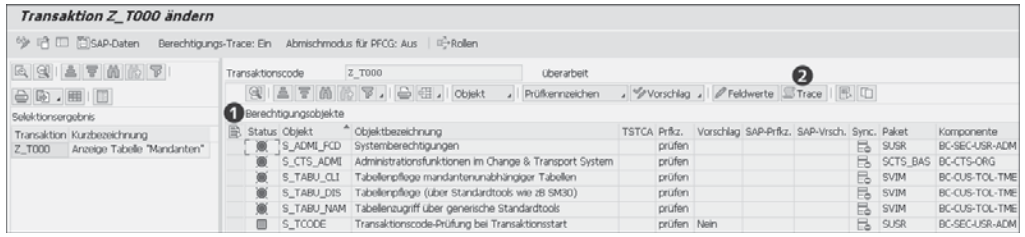


Abbildung 7.15 Werte für kundeneigene Transaktion SU24 nach der Übernahme der SAP-Daten bzw. der Daten aus dem Berechtigungstrace

7.2.2 Vorgehen beim Systemtrace

Um den Systemtrace zu nutzen, stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Wie Sie den Systemtrace aus der Auswertung in der Rollen- und Vorschlagswertpflege starten, sehen Sie in Abbildung 7.16. Sie können den Systemtrace aus folgenden Funktionen dieses Kontextes heraus starten:

- Transaktion PFCG (Pflege von Rollen) • Registerkarte Menü • Button Übernahme von Menüs • Menüeintrag Import aus Trace
- Transaktion PFCG (Pflege von Rollen) • Registerkarte Berechtigungen • Bereich Berechtigungsdaten pflegen und Profile generieren • Folgebildschirm • Button Trace
- Transaktion SU24 (Berechtigungsvorschlagspflege) • Button Trace • Folgebildschirm • Button Trace auswerten

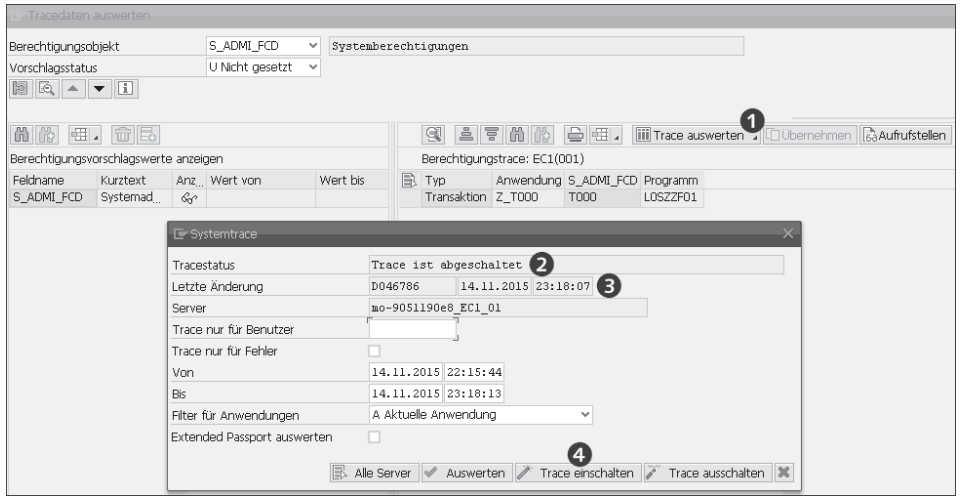


Abbildung 7.16 Trace aus der Auswertung in der Rollen- und Vorschlagswertpflege starten

Klicken Sie auf den Button TRACE AUSWERTEN (❶ in Abbildung 7.16). Sie erhalten die Info, ob der Systemtrace ein- oder ausgeschaltet ist ❷, wer der letzte Änderer war und wann die Änderung stattgefunden hat ❸, schließlich klicken Sie auf den Button TRACE EINSCHALTEN ❹, der den Trace startet.

Neben diesen Optionen steht Ihnen der Zugang über die Transaktion ST01 (Systemtrace) sowie über die Transaktion STAUTHTRACE (Berechtigungstrace) zur Verfügung.

7.2.3 Vorgehen beim Benutzertrace

Den Benutzertrace aktivieren Sie über den Profilparameter `auth/auth_user_trace`. Wie Sie Profilparameter pflegen, haben wir bereits in Abschnitt 7.2.1, »Vorgehen beim Berechtigungstrace«, beschrieben. Setzen Sie den Wert des Profilparameters auf `Y` (aktiv) oder `F` (aktiv mit Filter) (siehe Abbildung 7.11), diese Einstellungen können Sie auch dynamisch setzen. Den Filter setzen Sie, wie oben beschrieben, in der Transaktion STUSERTRACE entsprechend Ihren Anforderungen. Die Ergebnisse des Benutzertrace können Sie ebenfalls in dieser Transaktion über einen Klick auf den Button AUSWERTEN einsehen (siehe Abbildung 7.17).

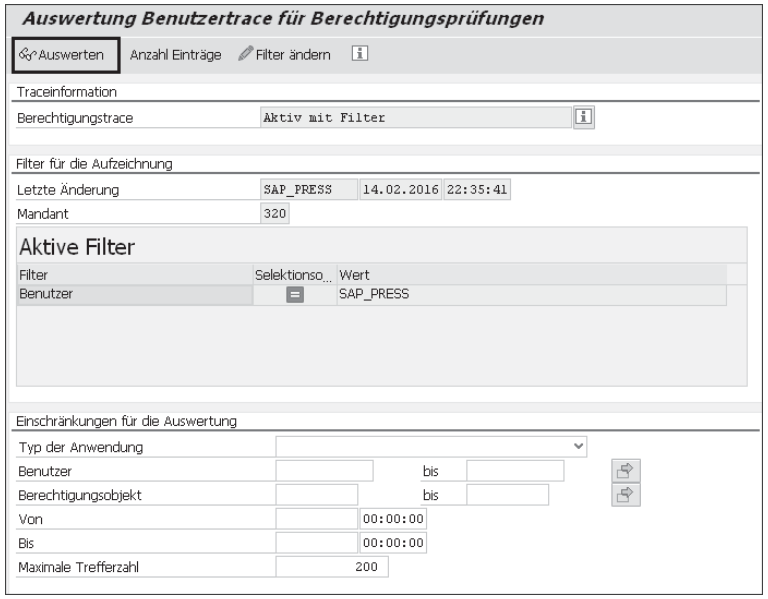
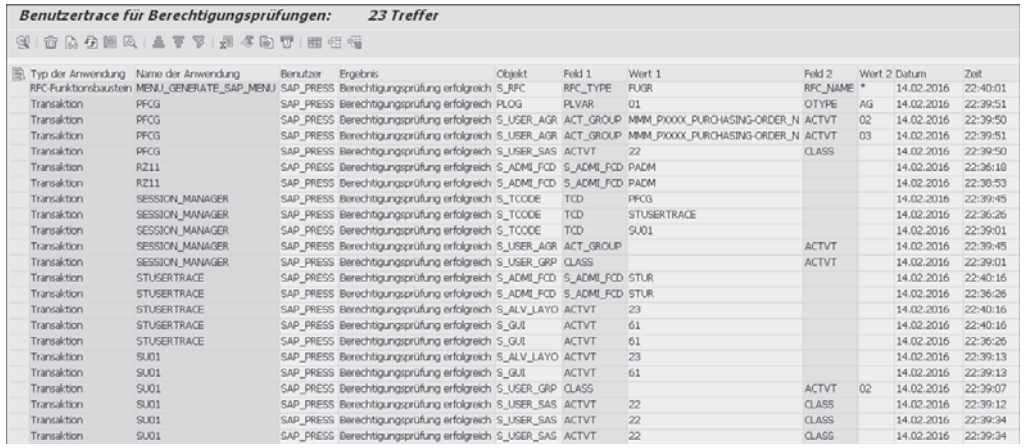


Abbildung 7.17 Einstellungen des Filters für den Benutzertrace über Transaktion STUSERTRACE

Die Auswertung (siehe Abbildung 7.18) zeigt nun alle ausgeführten Anwendungen und die darin erfolgten Berechtigungsprüfungen mit Objekt und Feldwerten an. Im Gegensatz zum Berechtigungstrace können Sie bei der Auswertung auf einen bestimmten Benutzer filtern, und die Benutzer sind in der Liste enthalten. Diese Informationen können Sie nun nutzen, um Berechtigungsvorschlagswerte oder Rollen zu pflegen.



Typ der Anwendung	Name der Anwendung	Benutzer	Ergebnis	Objekt	Feld 1	Wert 1	Feld 2	Wert 2	Datum	Zeit
RFC-Funktionsbaustein	MENU_GENERATE_SAP_MENU	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_RFC	RFC_TYPE	FUGR	RFC_NAME	*	14.02.2016	22:40:01
Transaktion	PFCG	SAP_PRESS	Berechtigungsprüfung erfolgreich	PLOG	PLVAR	01	OTYPE	AG	14.02.2016	22:39:51
Transaktion	PFCG	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_AGR	ACT_GROUP	MMM_PXXXX_PURCHASING-ORDER_N	ACTVT	02	14.02.2016	22:39:50
Transaktion	PFCG	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_AGR	ACT_GROUP	MMM_PXXXX_PURCHASING-ORDER_N	ACTVT	03	14.02.2016	22:39:51
Transaktion	PFCG	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_SAS	ACTVT	22	CLASS		14.02.2016	22:39:50
Transaktion	RZ11	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ADMI_FCD	S_ADMI_FCD	PADM			14.02.2016	22:36:18
Transaktion	RZ11	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ADMI_FCD	S_ADMI_FCD	PADM			14.02.2016	22:38:53
Transaktion	SESSION_MANAGER	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_TCODE	TCD	PFCG			14.02.2016	22:39:45
Transaktion	SESSION_MANAGER	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_TCODE	TCD	STUSERTRACE			14.02.2016	22:36:26
Transaktion	SESSION_MANAGER	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_TCODE	TCD	SU01			14.02.2016	22:39:01
Transaktion	SESSION_MANAGER	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_AGR	ACT_GROUP		ACTVT		14.02.2016	22:39:45
Transaktion	SESSION_MANAGER	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_GRP	CLASS		ACTVT		14.02.2016	22:39:01
Transaktion	STUSERTRACE	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ADMI_FCD	S_ADMI_FCD	STUR			14.02.2016	22:40:16
Transaktion	STUSERTRACE	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ADMI_FCD	S_ADMI_FCD	STUR			14.02.2016	22:36:26
Transaktion	STUSERTRACE	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ALV_LAYO	ACTVT	23			14.02.2016	22:40:16
Transaktion	STUSERTRACE	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_GUI	ACTVT	61			14.02.2016	22:40:16
Transaktion	STUSERTRACE	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_GUI	ACTVT	61			14.02.2016	22:36:26
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_ALV_LAYO	ACTVT	23			14.02.2016	22:39:13
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_GUI	ACTVT	61			14.02.2016	22:39:13
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_GRP	CLASS		ACTVT	02	14.02.2016	22:39:07
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_SAS	ACTVT	22	CLASS		14.02.2016	22:39:12
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_SAS	ACTVT	22	CLASS		14.02.2016	22:39:34
Transaktion	SU01	SAP_PRESS	Berechtigungsprüfung erfolgreich	S_USER_SAS	ACTVT	22	CLASS		14.02.2016	22:39:34

Abbildung 7.18 Auswertung des Benutzertrace über Transaktion STUSERTRACE

7.3 Upgrade-Nacharbeiten von Berechtigungen

Mit den Basisreleases 7.31 und 7.40 sind eine Reihe von Änderungen im Upgrade-Tool für den Profilgenerator vollzogen worden. Des Weiteren wurde die Dokumentationslage verbessert, die nun die Wartung von Berechtigungsvorschlagswerten und Rollen im Upgrade und beim Einspielen von Support Packages vereinfacht. Wir haben aktuelle SAP-Hinweise dazu in Tabelle 7.8 zusammengestellt.

SAP-Hinweis	Kurztext	Release
1539556	FAQ Administration von Berechtigungsvorschlagswerten	releaseunabhängig
1599128	SU25 – Optimierung der Upgrade-Nachbereitung	SAP_BASIS 70 700–702 SAP_BASIS 71 710– 30 SAP_BASIS 731

Tabelle 7.8 SAP-Hinweise zum Upgrade von Berechtigungen

SAP-Hinweis	Kurztext	Release
1696484	SU25 – Behandlung kundeneigener Berechtigungsvorschlagswerte	SAP_BASIS 70 700–702 SAP_BASIS 71 710–730
1691993	SU2X – Optimierung der Berechtigungsvorschlagswertepflege	SAP_BASIS 70 700–702 SAP_BASIS 71 710–730 SAP_BASIS 731

Tabelle 7.8 SAP-Hinweise zum Upgrade von Berechtigungen (Forts.)

Die folgenden Ausführungen und Screenshots beziehen sich auf SAP_BASIS 7.40, allerdings sind die meisten Funktionen auch in früheren Releases enthalten.

Die Transaktion SU25 (Upgrade-Tool für den Profilgenerator) dient dem initialen Befüllen der Kundentabellen zum ersten Einsatz des Profilgenerators und dazu, die Kundentabellen in einem Upgrade auf den neuesten Stand zu bringen. Insgesamt stehen in der Transaktion SU25 folgende Schritte zur Verfügung (siehe Abbildung 7.19):

- Schritt 1 bereitet den Profilgenerator auf seine erste Verwendung vor, und die Kundentabellen werden initial befüllt. Mit Hinweis 1691993 (SU2X – Optimierung der Berechtigungsvorschlagswertepflege) ist dieser Schritt so verändert worden, dass ein zufälliges Überschreiben bereits gefüllter Kundentabellen und somit die Vernichtung kundeneigener Daten erschwert wird. Mehr dazu erfahren Sie in diesem Hinweis. Durch diese neue Funktion verändert sich die Anzeige der Transaktion SU25 (Upgrade-Tool für den Profilgenerator) in Schritt 1 dann, wenn Schritt 2a bereits einmal im System ausgeführt wurde. Die neue Darstellung ist in Abbildung 7.19 unter KUNDENTABELLEN WURDEN INITIAL BEFÜLLT zu sehen.
- Die Schritte 2a–2d sind für das Upgrade selbst erforderlich.
- Schritt 3 dient dem Transport der durch die vorangegangenen Schritte geänderten Kundenvorschlagswerttabellen. Beachten Sie, dass nur diese transportiert werden.
- Schritt 4 ist ein Absprung in die Transaktion SU24 (Berechtigungsobjektprüfungen unter Transaktionen).
- Schritt 5 ermöglicht das globale Deaktivieren von Berechtigungsprüfungen.

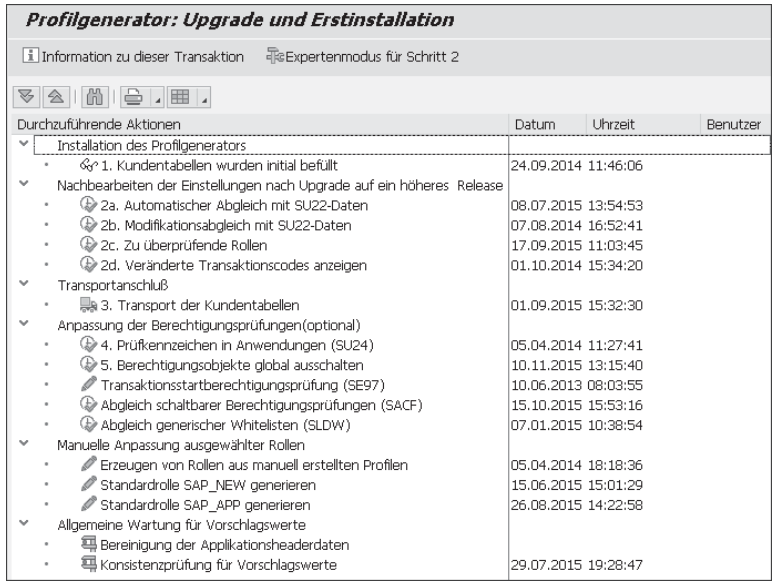


Abbildung 7.19 Upgrade-Tool für den Profilgenerator

Dargestellt wird nun das Upgrade, also das Nachbearbeiten der Einstellungen nach dem Upgrade auf ein höheres Release. Dieses wird in den Schritten 2a–2d vollzogen.

Schritt 2a: Vorbereitung – Abgleich mit SAP-Werten

Zunächst wird in Schritt 2a der Abgleich der Vorschlagswerte ausgeführt. Dieser Schritt ist zwingend erforderlich. Dabei werden die neuen Berechtigungsvorschlagswerte (also die Werte nach Upgrade oder Einspielen eines Support Packages) in die Kundentabellen übernommen.

Verwenden Sie dafür am besten den EXPERTENMODUS FÜR SCHRITT 2, indem Sie auf den gleichnamigen Button klicken. Dabei können Sie (ab Basisrelease 7.00) wählen, ob Sie einen Abgleich der SAP-Standardanwendungen oder einen Abgleich von kundeneigenen und Partneranwendungen der neu ausgelieferten Werte mit Ihren kundenspezifischen Werten vornehmen möchten, wie es in Abbildung 7.20 gezeigt wird.

Die Übersicht in Abbildung 7.21 zeigt, welche Anwendungen abzugleichen sind und bei welchen Anwendungen ein manueller Abgleich notwendig ist. Ein manueller Abgleich ist erforderlich, wenn Daten in der Transaktion SU24 für diese Anwendung im Vorfeld geändert worden sind und Sie entscheiden müssen, ob diese Änderungen übernommen werden oder ob die aktuellen Standardwerte aus der Transaktion SU22 übernommen werden sollen.

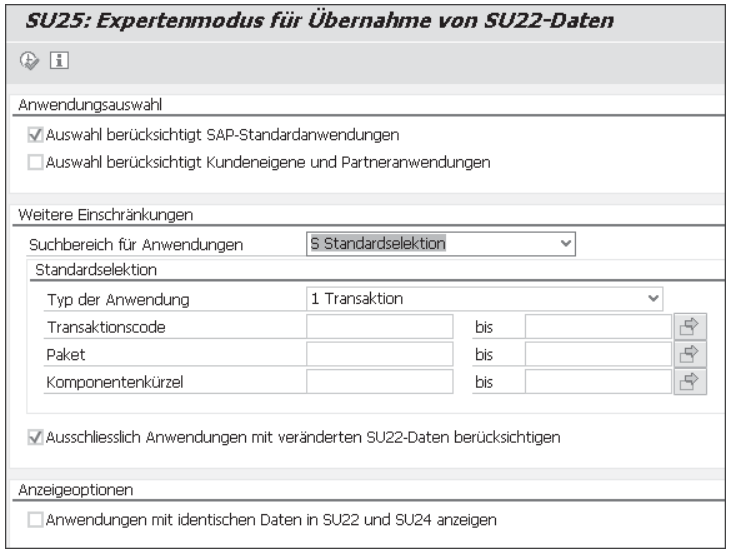


Abbildung 7.20 Auswahl des Abgleichs bei Upgrade-Nacharbeiten unter Verwendung des Expertenmodus für Schritt 2

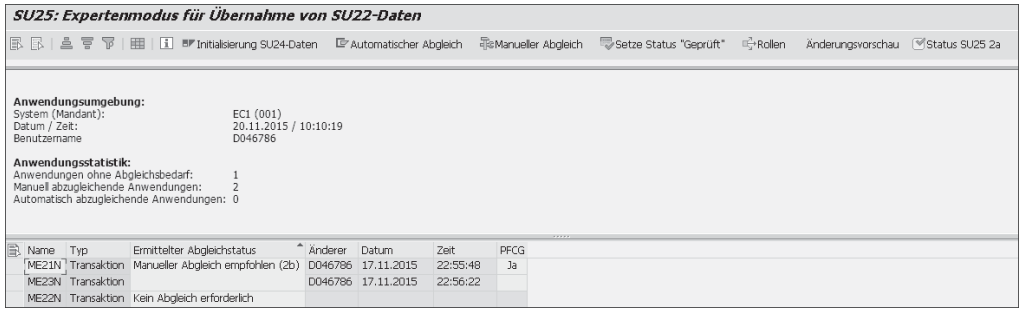


Abbildung 7.21 Übernahmeoptionen von Anwendungen in Schritt 2a

Die Werte, die in der »alten« Kundentabelle kundenseitig gepflegt wurden, werden gekennzeichnet, um sie in Schritt 2b manuell überprüfen zu können. Dabei markieren Sie die Anwendungen, die Sie manuell abgleichen möchten, und klicken auf den Button Manueller Abgleich.

Schritt 2b: Abgleich betroffener Transaktionen

Änderungen an Prüfkennzeichen oder Feldwerten werden in diesem Schritt mit den neuen SAP-Vorschlägen verglichen. In Abbildung 7.22 ist der Bereich mit ❶ gekennzeichnet, in dem die Transaktionen enthalten sind, die von den aktuellen Standardvorschlägen abweichen. Die Einstellungen, die wir in Abschnitt 7.1.1, »Grundzustand und Pflege der Berechtigungsvorschlagswerte«, in Bezug auf die

Transaktion Anzeigen einer Bestellung vorgenommen haben, werden entsprechend nach dem Abgleich in Schritt 2a in Schritt 2b zur Bearbeitung angeboten. Sie sehen in Abbildung 7.22, dass die mit ❷ gekennzeichnete Änderung des Prüfkennzeichens dazu führt, dass der neue SAP-Vorschlag angezeigt wird. Ebenso ist es mit der durch ❸ gekennzeichneten Änderung des Vorschlags. Diese Änderungen erkennen Sie daran, dass in der Spalte Sync. die Buttons SAP-Daten Kopieren zu sehen sind ❹. Durch einen Klick auf diese Buttons kopieren Sie den SAP-Vorschlag und überschreiben Ihre Kundenvorschlagswerte. Mit ❺ sind Änderungen der Feldwertvorschläge gekennzeichnet. Sie können die jeweiligen Werte nachpflegen. Im Bereich ❶ können Sie bestätigen, dass Sie die Prüfung vorgenommen haben, oder die gesamten restlichen Werte übernehmen. Davon raten wir Ihnen jedoch ab, sofern Sie regelmäßig und genau Ihre kundeneigenen Vorschläge ergänzt oder geändert haben.

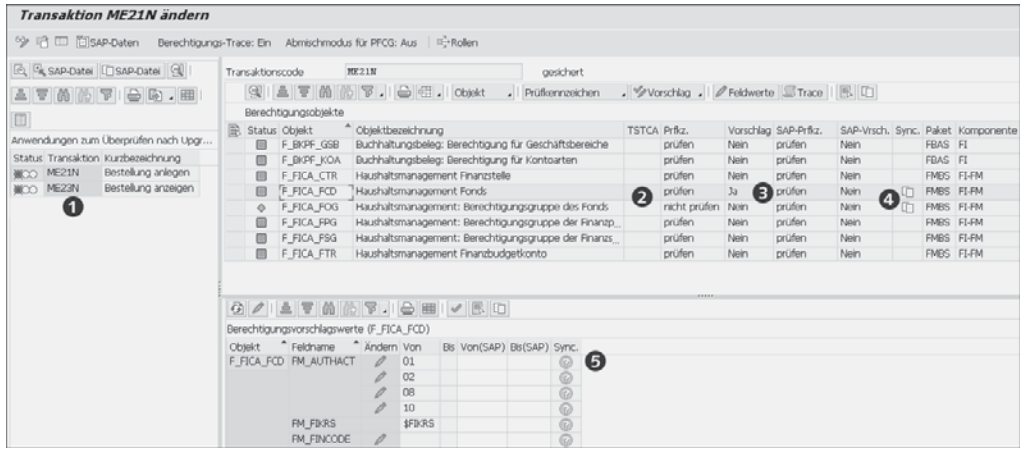


Abbildung 7.22 Berechtigungsvorschläge in Schritt 2b der Upgrade-Nacharbeiten

Die Systematik zur Pflege der Berechtigungsvorschlagswerte entspricht im Wesentlichen der Systematik, wie wir sie in Abschnitt 7.1.1, »Grundzustand und Pflege der Berechtigungsvorschlagswerte«, im Hinblick auf die Berechtigungsvorschlagswerte entwickelt haben.

Nacharbeit Schritt 2b: Kundeneigene Organisationsebenen

Sofern Sie kundeneigene Organisationsebenen nutzen (siehe Abschnitt 7.8, »Anhebung eines Berechtigungsfeldes zur Organisationsebene«), sollten Sie den Report PFCG_ORGFIELD_UPGRADE (Anpassung nach Upgrade für neue Org.-Ebenen) ausführen. Dadurch

werden alle neuen Berechtigungsvorschlagsdaten, die SAP zu neuen Transaktionen ausgeliefert hat, auf die neuen Organisationsebenenfelder umgestellt. Der Report arbeitet mandantenunabhängig (SAP-Hinweis 323817).

Schritt 2c: Zu überprüfende Rollen

In diesem Schritt findet die Nachbearbeitung der durch das Upgrade betroffenen Rollen statt. Diese werden, wie in Abbildung 7.23 zu sehen ist, vorgeschlagen; dabei markiert eine rote Ampel (links in der jeweiligen Ampel) Pflegebedarf und eine grüne (rechts in der jeweiligen Ampel), dass keine Pflege (mehr) erforderlich ist.

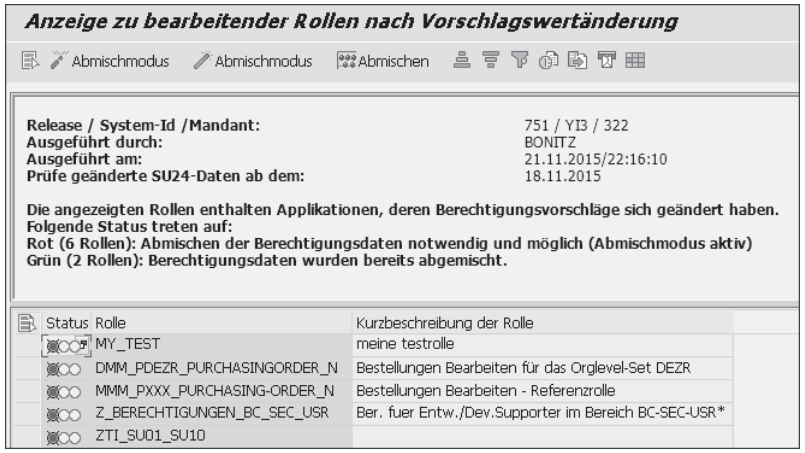


Abbildung 7.23 Rollenüberprüfung in Schritt 2c der Upgrade-Nacharbeiten

Um bei den bereits eingeführten Beispielen zu bleiben: In Abschnitt 6.3.2, »Rollenpflege«, haben wir die Rolle MMM_PXXXX_PURCHASINGORDER_N angelegt und daraus Rollen abgeleitet. Diesen Rollen ist die Transaktion ME21N (Bestellung anlegen) zugeordnet, die ebenfalls im Rahmen des Abschnitt 7.1.1, »Grundzustand und Pflege der Berechtigungsvorschlagswerte«, gepflegt wurde und nun von dem Upgrade betroffen ist.

Abbildung 7.24 zeigt, dass das ergänzte Berechtigungsobjekt erkannt und vorgeschlagen wurde. Da der Vorschlag nur das Feld Aktivität Berechtigungsprüfung betraf und das Feld Finanzkreis eine Organisationsebene ist, verbleibt nur das Feld Fonds, das manuell gepflegt werden muss. Die Änderung der Referenzrolle wird durch den Button Abgeleitete Rollen generieren automatisch mit gepflegt.

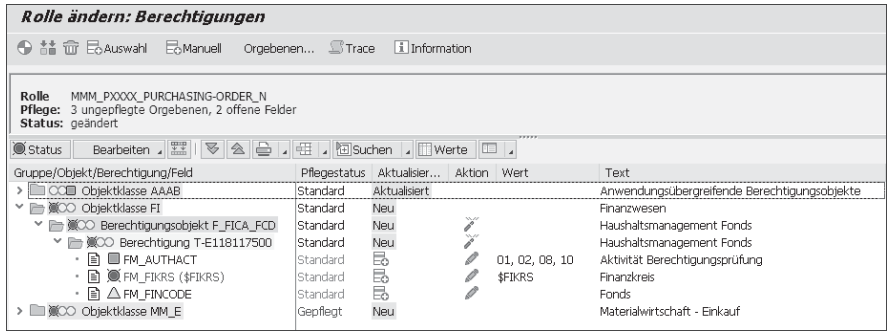


Abbildung 7.24 Rollenänderung in Schritt 2c der Upgrade-Nacharbeiten

SAP-Alternativvorschlag

In der Hilfe zu diesem Schritt wird von SAP folgende alternative Vorgehensweise vorgeschlagen:

> *Alternativ können Sie auch auf eine Nachbearbeitung der Rollen verzichten und allen Benutzern zunächst die Rolle SAP_NEW generieren und manuell zuordnen (siehe dazu SAP-Hinweis 1711620) […] Die Rollen behalten dann den Status »Profilabgleich erforderlich« und können bei der nächsten notwendigen Änderung – z. B. wenn das Menü der Rolle geändert wird – angepaßt werden. Bei Verwendung von sehr vielen Rollen kann dieses Verfahren sinnvoll sein. Sie haben dann Zeit, die Rollen nach und nach anzupassen.*
> *(Systemhilfe)*

Dieser Vorschlag birgt erhebliche Risiken, vor allem in den Fällen, in denen neue Funktionen, neue Berechtigungsprüfungen oder neue Differenzierungspotenziale bereitgestellt und genutzt werden. Die selbst generierte Rolle SAP_NEW (siehe SAP-Hinweis 1711620) enthält alle neuen Berechtigungen für das neue Release. Damit wird durch ein derartiges Vorgehen gegen das Prinzip verstoßen, dass nur die Berechtigungen vergeben werden, die für die Ausführung einer definierten Tätigkeit des Benutzers erforderlich sind. Für die Zeit der Nutzung der Rolle SAP_NEW ist davon auszugehen, dass die Berechtigungen nicht regelkonform sind. Der Gegenbeweis wäre nur durch eine Risikoanalyse – basierend auf den alten und neuen Prüfungen – anzutreten.

Einfaches Upgrade

Die Nutzung eines gewissenhaft eingehaltenen Ableitungskonzepts, stetig gepflegter Berechtigungsvorschlagswerte und des Upgrade-Tools führt zu einem einfachen Upgrade im Bereich Berechtigungen. In diesem idea-

len Fall müssen im Wesentlichen nur die neuen Transaktionen, Berechtigungsobjekte und Vorschlagsänderungen bewertet und umgesetzt werden. Der Aufwand für das Upgrade sinkt mit der Genauigkeit der Standardeinhaltung.

Empfehlung zum Aufwand

Wir haben Upgrade-Projekte mit einem Aufwand für Berechtigungen zwischen 20 und 300 Beratertagen in Konzernstrukturen kennengelernt. Kommen Sie in der Abschätzung des Aufwands zu dem Ergebnis, dass mehr als 50 Tage Aufwand zu erwarten sind, empfiehlt es sich dringend, ein Redesign und die Rückkehr zum Standard zu prüfen. Das verursacht unter Umständen sofort einen geringeren Aufwand, als den Status quo anzuheben. Definitiv werden Ihre Kosten bereits mittelfristig deutlich sinken.

Schritt 2d: Veränderte Transaktionscodes anzeigen

In diesem Schritt findet ein Abgleich statt, welche Transaktionen durch neuere Transaktionen ersetzt werden könnten. Dieser Abgleich dient vor allem der Unterstützung der Prozessverantwortlichen. Diese müssen letztlich festlegen, welche Transaktionen wie zu nutzen sind. Sie sollten das Ergebnis des Abgleichs also den Prozessverantwortlichen übermitteln und diese die Festlegung treffen lassen.

Neue Transaktionen haben gegebenenfalls Auswirkungen auf die bestehenden Prozesse, aber auch auf die bestehenden Berechtigungen. Ein Beispiel für unter Umständen nicht gewollte Auswirkungen auf Berechtigungen ist die bereits diskutierte Enjoy-Transaktion (siehe Abschnitt 7.1.1) zur Bestellung, es kann auch aus Sicht von Berechtigungen Gründe geben, lieber weiterhin auch die alte Transaktion zu nutzen.

7.4 Parameter für Kennwortregeln

Die für das Login geltenden Kennwortregeln werden über Profilparameter gesetzt. Diese werden über die Transaktion RZ10 (Pflege der Profilparameter) gepflegt. Die Pflege der Profilparameter fällt in die Verantwortung der Basisadministration. Wir empfehlen Ihnen, die gewünschten Einstellungen Ihrer Basisadministration zu überlassen.

Die Auswertung der Profilparameter ist über den Report RSPARAM (Anzeige der SAP-Profilparameter) möglich (siehe Abbildung 7.25). Einige exemplarische Parameter sind in Tabelle 7.9 dargestellt.

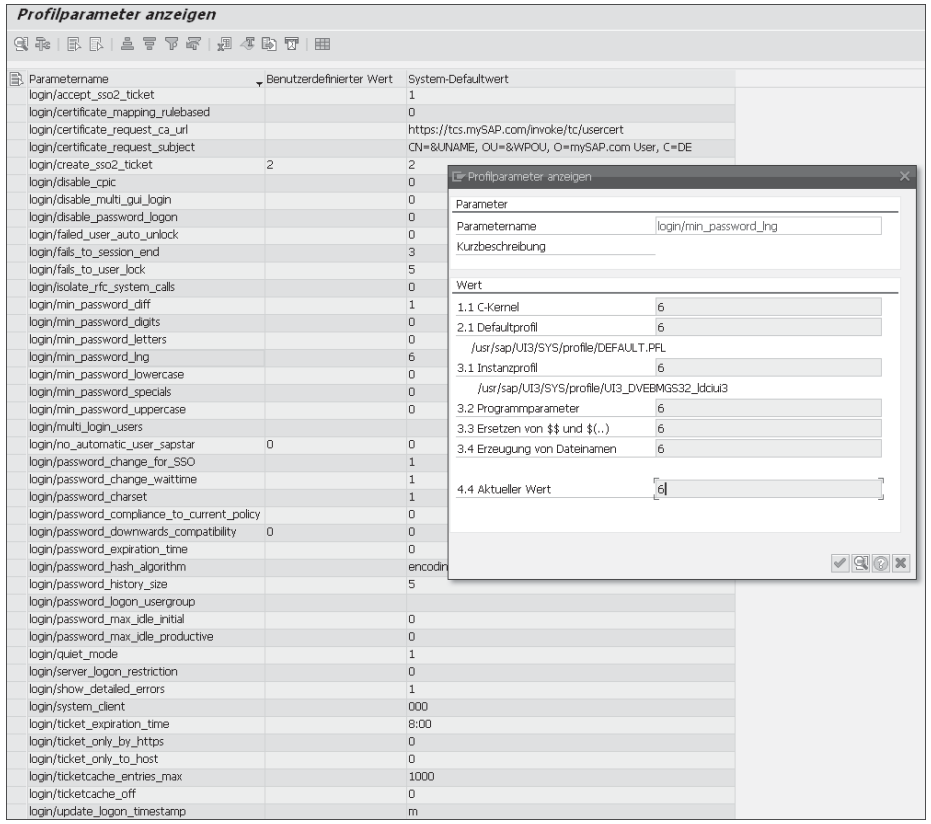


Abbildung 7.25 Anzeige der Profilparameter

Parameter	Beschreibung
`login/accept_sso2_ticket`	Um ein Single Sign-on (SSO) zwischen SAP-Systemen bzw. auch übergreifend zu Nicht-SAP-Systemen zu ermöglichen, können SSO-Tickets verwendet werden.
`login/failed_user_auto_unlock`	Kontrolliert die Entsperrung von durch Fehlanmeldungen gesperrten Benutzern. Ist der Parameter auf 1 gesetzt, werden Sperren, die wegen fehlgeschlagener Kennwortanmeldeversuche gesetzt wurden, automatisch am nächsten Tag durch das System aufgehoben.
`login/fails_to_session_end`	Anzahl der Falschanmeldungen, die mit einem Benutzerstamm gemacht werden können, bis das Anmeldeverfahren abgebrochen wird

Tabelle 7.9 Parameter für Kennwortregeln
(Angaben aus der Systemdokumentation)

Parameter	Beschreibung
login/fails_to_user_lock	Bei jedem fehlerhaften Kennwortanmeldeversuch wird der Falschanmeldezähler für den betreffenden Benutzerstammsatz erhöht. Die Anmeldeversuche können im Security Audit Log protokolliert werden. Bei Überschreiten der durch diesen Parameter vorgegebenen Grenze wird der betreffende Benutzer gesperrt. Dieser Vorgang wird zusätzlich im Syslog protokolliert.
login/min_password_diff	Mit diesem Parameter kann der Administrator festlegen, in wie vielen Zeichen sich ein neues Kennwort vom alten Kennwort mindestens unterscheiden muss, wenn der Benutzer sein Kennwort ändert.
login/min_password_digits	Dieser Parameter bestimmt die minimale Anzahl von Ziffern (0–9), die im Kennwort enthalten sein müssen. Er wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen von Kennwörtern.
login/min_password_letters	Dieser Parameter bestimmt die minimale Anzahl von Buchstaben, die im Kennwort enthalten sein müssen. Er wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen von Kennwörtern.
login/min_password_lng	Der Parameter bestimmt die Minimallänge des Anmeldekennwortes. Das Kennwort muss mindestens drei Zeichen lang sein. Der Administrator kann aber auch eine größere Minimallänge festlegen. Diese Vorgabe wirkt sich sowohl bei der Vergabe neuer Kennwörter als auch beim Ändern oder Rücksetzen bestehender Kennwörter aus.
login/min_password_lowercase	Dieser Parameter bestimmt die minimale Anzahl von Kleinbuchstaben, die im Kennwort enthalten sein müssen. Er wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen von Kennwörtern. Dieser Parameter wird nicht ausgewertet, wenn der Profilparameter login/password_downwards_compatibility auf den Wert 5 gesetzt ist.

Tabelle 7.9 Parameter für Kennwortregeln (Angaben aus der Systemdokumentation) (Forts.)

Parameter	Beschreibung
login/min_password_specials	Dieser Parameter bestimmt die minimale Anzahl von Sonderzeichen, die im Kennwort enthalten sein müssen. Er wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen von Kennwörtern.
login/min_password_uppercase	Dieser Parameter bestimmt die minimale Anzahl von Großbuchstaben, die im Kennwort enthalten sein müssen. Er wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung bzw. beim Rücksetzen von Kennwörtern. Dieser Parameter wird nicht ausgewertet, wenn der Profilparameter login/password_downwards_compatibility auf den Wert 5 gesetzt ist.
login/password_change_waittime	Mit diesem Parameter kann festgelegt werden, nach welcher Zeitspanne (gemessen in Tagen) ein Benutzer sein Kennwort erneut ändern kann. Nur Kennwortänderungen, die der Benutzer veranlasst hat, werden in Betracht gezogen.
login/password_expiration_time	Gültigkeitsdauer von durch den Benutzer gesetzten Kennwörtern (in Tagen) bis zur nächsten Änderung. Die Berechnung erfolgt abhängig vom Datum der letzten Kennwortänderung.
login/password_max_idle_productive	maximale Zeitspanne (in Tagen) zwischen dem Zeitpunkt der letzten Anmeldung mit einem durch den Benutzer gesetzten Kennwort und der nächsten Anmeldung mit diesem Kennwort
login/password_max_idle_initial	maximale Zeitspanne (in Tagen) zwischen dem Zeitpunkt der Kennwort(rück)setzung, Initital-kennwort durch den Administrator gesetzt, und der nächsten Anmeldung mit diesem Kennwort
login/password_history_size	Dieser Parameter regelt die Größe der Kennworthistorie. Die Kennworthistorie wird ausgewertet, wenn ein Benutzer ein neues Kennwort wählt: Das System lehnt die (Wieder-) Verwendung von Kennwörtern, die in der Kennworthistorie gespeichert sind, ab.

Tabelle 7.9 Parameter für Kennwortregeln (Angaben aus der Systemdokumentation) (Forts.)

Bitte beachten Sie auch den SAP-Hinweis 2467 (Kennwortregeln und Vermeidung fehlerhafter Anmeldungen).

Verbotene Kennwörter in der Tabelle USR40

In der Tabelle USR40 (Tabelle für verbotene Kennwörter) können darüber hinaus »verbotene« Kennwörter hinterlegt werden. Dies ist sowohl als Muster »*WORT*, *20??*,« als auch als konkreter Wert »Mama« möglich. Da dies Auswirkungen auf die Performance hat, sollten Sie unbedingt über die genannten Parameter eine sinnvolle Password Policy erzwingen, in dieser Tabelle sollten Sie möglichst nur unmittelbar offensichtliche Werte eintragen, wie z. B. den Namen des Unternehmens.

Customizing-Parameter in der Tabelle PRGN_CUST

Über die Customizing-Parameter in der Tabelle PRGN_CUST wird der Kennwortgenerator in den Transaktionen SU01 und SU10 gesteuert. Eine Übersicht über diese Customizing-Parameter finden Sie in Tabelle 7.10. Die Werte der Profilparameter übersteuern die Einträge zu den Customizing-Parametern, damit keine ungültigen Kennwörter generiert werden. Sollte also der Wert eines Customizing-Parameters kleiner sein als der Wert des korrespondierenden Profilparameters, wird stattdessen der Standardwert des Customizing-Parameters gezogen. Analog verhält es sich, wenn kein Wert gepflegt wurde.

Parameter	Beschreibung
GEN_PSW_MAX_LENGTH	Legt die maximale Länge des generierten Passwortes fest.
GEN_PSW_MAX_LETTERS	Legt die maximale Anzahl an Buchstaben im generierten Passwort fest.
GEN_PSW_MAX_DIGITS	Legt die maximale Anzahl an Zahlen im generierten Passwort fest.
GEN_PSW_MAX_SPECIALS	Legt die maximale Anzahl an Sonderzeichen im generierten Passwort fest.

Tabelle 7.10 Parameter für die Kennwortgenerierung

Sicherheitsrichtlinien

Zusätzlich zu den globalen Einstellungen der Kennwortregeln können Sie ab Release SAP NetWeaver 7.31 Kennwortregeln auch individuell über Sicherheitsrichtlinien definieren. Sie ordnen einem Benutzer die jeweilige Sicherheitsrichtlinie über die Transaktion SU01 zu. Ist einem Benutzer eine Sicherheitsrichtlinie zugeordnet, überschreiben die Werte der Sicherheitsrichtlinie die global gültigen Kennwortregeln. Für Einstellungen, deren Parameter nicht in der Sicherheitsrichtlinie gepflegt wurden, oder Benutzer, denen keine Sicherheitsrichtlinie zugeordnet ist, bleiben die globalen Einstellungen der Profilparameter weiterhin relevant. Sie definieren Sicherheitsrichtlinien über die Transaktion SECPOL; ein Beispiel haben wir in Abbildung 7.26 dargestellt und einige exemplarische Parameter sind in Tabelle 7.11 aufgeführt.

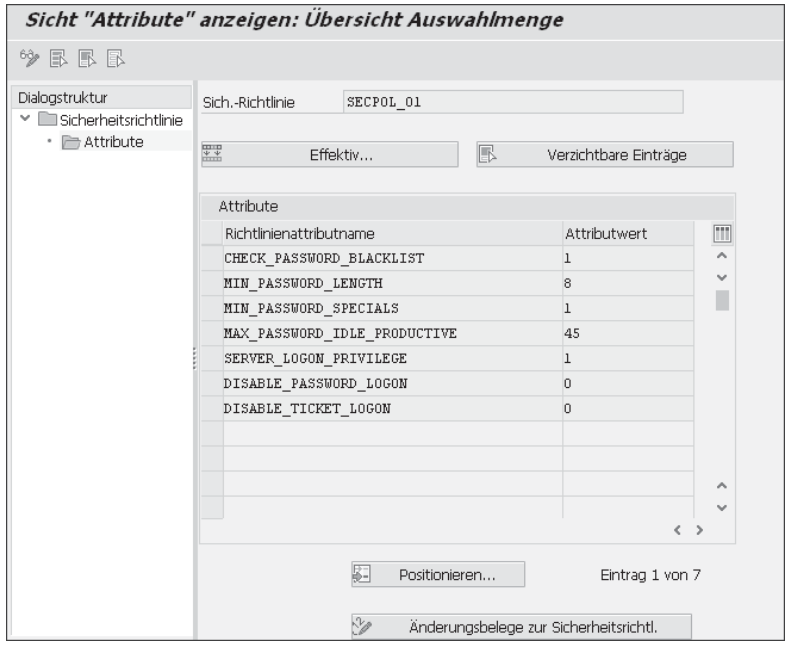


Abbildung 7.26 Definition einer Sicherheitsrichtlinie in der Transaktion SECPOL

Parameter	Beschreibung
DISABLE_TICKET_LOGON	Legt fest, ob sich ein Benutzer mit Anmelde- oder Zusicherungsticket am System anmelden kann.
MAX_FAILED_PASSWORD_LOGON_ATTEMPTS	Funktion analog zum Profilparameter login/fails_to_user_lock
MIN_PASSWORD_DIFFERENCE	Funktion analog zum Profilparameter login/min_password_diff
MIN_PASSWORD_DIGITS	Funktion analog zum Profilparameter login/min_password_digits
MIN_PASSWORD_LETTERS	Funktion analog zum Profilparameter login/min_password_letters
MIN_PASSWORD_LENGTH	Funktion analog zum Profilparameter login/min_password_lng

Tabelle 7.11 Parameter der Sicherheitsrichtlinien

Parameter	Beschreibung
PASSWORD_CHANGE_INTERVAL	Funktion analog zum Profilparameter login/password_expiration_time
CHECK_PASSWORD_BLACKLIST	Prüft bei der Eingabe des Kennwortes gegen die Negativliste verbotener Kennwörter (es werden die Einträge in der Tabelle USR40 geprüft).
SERVER_LOGON_PRIVILEGE	Legt fest, ob sich ein Benutzer trotz gesetzter Zugriffsbeschränkung für einen Server an diesem anmelden kann. Über den Profilparameter login/server_logon_restriction können Sie so eine Zugriffsbeschränkung setzen.

Tabelle 7.11 Parameter der Sicherheitsrichtlinien (Forts.)

Mit der Einführung der Sicherheitsrichtlinien gelten nun auch die Regeln zu den Inhalten der Kennwörter für Benutzer vom Typ System und Service. Regeln für die Änderung von Kennwörtern sind weiterhin nicht für diese Benutzertypen gültig. Diese Änderung ist erfolgt, da es Ihnen nun möglich ist, für diese Benutzer eigene Sicherheitsrichtlinien zu definieren und so z. B. sicherzustellen, dass weiterhin abwärtskompatible Passwörter für diese Benutzer verwendet werden.

7.5 Menükonzept

Ein Menükonzept wird häufig verwendet, um den Endbenutzern übersichtliche Benutzermenüs anzubieten. Das Menükonzept bedeutet keine Einschränkung von Berechtigungen. Im Folgenden werden wir Ihnen einen einfachen Vorschlag machen, wie ein Menükonzept aussehen kann. Dabei gehen wir davon aus, dass Sie entweder das »alte« Bereichsmenü (Transaktion SE43) oder Menüvorlagen, die in nicht weiter ausgeprägten Rollen vorgehalten werden, als Schablone für das Rollenmenü nutzen. Darüber hinaus empfehlen wir lediglich, alle Rollenmenüs auf Basis dieser Schablonen einzurichten.

Präferenzen für Menüs

Die einzige dringende Anforderung, die an ein Menükonzept zu stellen ist, ist die, dass es logisch konsistent sein muss. Ob ein Menükonzept für Ihre Organisation sinnvoll ist und ob Sie Ihr Menü auf Standard-,