

Einleitung

Schon beim Schreiben unseres Buches »SAP-Berechtigungs-wesen« ist uns aufgefallen, dass wir trotz der Fülle an Informationen auf den 847 Seiten nicht alle Funktionen und Kniffe, die uns den Alltag in Kundenprojekten erleichtern, beschreiben konnten. Die große Menge an Neuerungen, die von SAP nicht nur über Basisreleases ausgeliefert wurden, hat uns dazu bewogen, in Zusammenarbeit mit Beratern, SAP-Partnern und natürlich unseren Kollegen von der SAP SE unsere Erfahrungen im vorliegenden Buch festzuhalten.

Zunächst haben wir überprüft, ob die Themen aus dem Vorgängerbuch »Berechtigungen in SAP – 100 Tipps & Tricks« noch aktuell sind. Nach Erscheinen der ersten Auflage haben wir viele Anregungen erhalten und gesammelt und diese im vorliegenden Buch umgesetzt. Eine weitere Umfrage unter Kollegen im SAP-Support, in der SAP-Entwicklung sowie in der SAP-Beratung ergab viele weitere neue Themen, die in aktuellen Kundenprojekten gefragt sind. Wir wollten im Rahmen dieser Umfrage feststellen, welche Best Practices gerne angewendet werden und welche von den Kollegen des SAP-Supports und der SAP-Entwicklung als unerlässlich erachtet werden. Auch die Ergebnisse dieser Umfrage haben wir in dieses Buch einfließen lassen.

Zum Aufbau

Wir haben uns für die Darstellung der Best Practices hauptsächlich auf das Umfeld der ABAP-Werkzeuge zur Berechtigungs- und Benutzerverwaltung sowie zur Absicherung des ABAP-Applikationsservers konzentriert. Dieses Buch ist in zwölf Kapitel gegliedert.

Kapitel 1, »Benutzerstammdaten und Voraussetzungen für die Anmeldung«, befasst sich mit Empfehlungen rund um die Benutzerstammdaten, wie z. B. Definition der Benutzergruppe als Pflichtfeld oder Umgang mit Sicherheitsrichtlinien.

Empfehlungen zur Verwaltung von Benutzern finden Sie in **Kapitel 2**, »Benutzerverwaltung«. Dazu zählen etwa die Lösungswege im Umfeld der Zentralen Benutzerverwaltung (ZBV) und zur indirekten Rollenzuordnung.

Möchten Sie eine Massenpflege an PFCG-Rollen vornehmen, sehen Sie sich **Kapitel 3**, »Rollenverwaltung«, näher an. Hier gehen wir auch auf grundsätzliche Vorgehensweisen ein und geben nützliche Hinweise, u. a. zur Verwendung des Referenzbenutzers bei der Vergabe von Berechtigungen für Schnittstellen- und Hintergrundbenutzer.

Die Verwendung von Berechtigungsvorschlagswerten ist grundlegend für die transparente und regelkonforme Rollenpflege. Deswegen haben wir diesem Thema **Kapitel 4**, »Berechtigungsvorschlagswerte«, gewidmet.

Da die Verwendung von Traces im SAP-System vielfältiger geworden ist, erläutern wir in **Kapitel 5**, »Berechtigungstraces« ausführlich die Verwendung des Systemtraces, Berechtigungstraces, Benutzertraces und RFC-Traces. Über die Rollenverwaltung hinaus existieren Systemeinstellungen, wie beispielsweise die Pflege von Parametern in Customizing-Tabellen, die Verwendung von Organisationsebenen, die Konfiguration von schaltbaren Berechtigungsprüfungen oder die Erstellung von Berechtigungsgruppen, die allesamt Hand in Hand mit der Rollenpflege gehen. Die wichtigsten Empfehlungen dazu haben wir in **Kapitel 6**, »Systemeinstellungen«, gesammelt.

In **Kapitel 7**, »Basisberechtigungen«, sehen wir uns Best Practices für die Vergabe von Berechtigungen für z. B. den generischen Programmstart oder den generischen Tabellenzugriff an.

In **Kapitel 8**, »Anwendungsberechtigungen«, beschreiben wir Berechtigungen in bestimmten Komponenten des SAP-Systems, die Ihnen im täglichen Projektgeschäft sicher häufig über den Weg laufen. Wir erläutern u. a. den Umgang mit dem Verantwortungsbereich oder die korrekte Verwendung von SAP_NEW.

Einen mit dieser Auflage neu hinzugekommenen Schwerpunkt unseres Buches stellt die »Benutzer- und Berechtigungsverwaltung in SAP HANA und SAP S/4HANA« in **Kapitel 9** dar. In diesem Umfeld zeigen wir Ihnen den Unterschied zwischen Berechtigungen in SAP HANA und SAP S/4HANA, geben einen Überblick über die Verwendung der Werkzeuge für diese SAP-Produkte und erläutern die wichtigsten Best Practices bei der Vergabe von Berechtigungen in SAP Fiori.

Mit Ihren eigenen Berechtigungen befassen wir uns in **Kapitel 10**, »Kundeneigene Berechtigungen«. Wir geben Ihnen hier u. a. Empfehlungen zur Erstellung von Berechtigungsobjekten und zur Implementierung eigener Berechtigungsprüfungen.

In **Kapitel 11**, »Auswertungen von Berechtigungen und Benutzerstammsätzen«, beschreiben wir Möglichkeiten für Auswertungen zu Benutzern und Berechtigungen. Wir stellen Ihnen Reports des Benutzerinformationssystems und zusätzliche Auswertungsmöglichkeiten, etwa über SAP Query oder die Verwendung des Audit Information Cockpits, vor.

Unsere Zusammenstellung schließen wir mit **Kapitel 12**, »Systemsicherheit«, ab, in dem wir Ihnen zeigen, wie Sie Ihren Applikationsserver sinnvoll absichern, beispielsweise über den Schutz des RFC-Gateways und des Message Servers. Wir stellen Ihnen Möglichkeiten der Tabellenprotokollierung, die Verwendung des Security Audit Logs und Funktionen des SAP Solution Managers vor.

Informationskästen

In hervorgehobenen Informationskästen in diesem Buch sind Inhalte zu finden, die wissenswert und hilfreich sind, aber über die eigentliche Erläuterung hinausgehen. Damit Sie die Informationen in den Kästen sofort einordnen können, sind die Kästen mit Symbolen gekennzeichnet:

- In Kästen, die mit dem Pfeilsymbol gekennzeichnet sind, finden Sie Informationen zu *weiterführenden Themen* oder wichtigen Inhalten, die Sie sich merken sollten. 
- Die mit dem Plus-Symbol gekennzeichneten *Tipps* geben Ihnen spezielle Empfehlungen, die Ihnen die Arbeit erleichtern können. 
- Das Ausrufezeichen weist Sie auf *Besonderheiten* hin, die Sie beachten sollten. Es *warnt* Sie außerdem vor typischen Fehlern oder möglicherweise auftretenden Problemen. 

Systemvoraussetzungen

Die in diesem Buch beschriebenen Best Practices basieren auf aktuellen Support Packages zu verschiedenen SAP-NetWeaver-Releases. Sollten die Funktionen nur in höheren Releases verfügbar sein, weisen wir Sie in den entsprechenden Abschnitten darauf hin.

Danksagung

All diese Tipps wären nicht ohne unsere Ideengeber zustande gekommen. Einige konnten wir sogar als Co-Autoren gewinnen und danken ihnen auf diesem Wege ganz herzlich für die wunderbare Zusammenarbeit. Zu dieser 2. Auflage haben einige Co-Autoren noch wesentlich stärker beigetragen, und wir möchten uns für die hervorragende Unterstützung gerade in der zeitlich knappen Schlussphase des Schreibens bei ihnen bedanken: Dr. Ronald Baudisch (SAP Deutschland SE), Dieter Gödel (SAP SE), Markus Griem (SAP Deutschland SE), Anne Kempa (SAP Deutschland SE), Daniela Pranghofer (SAP Deutschland SE), Birger Tödtmann (SAP Deutschland SE) und Christian Weide (SAP Deutschland SE).

Besonderer Dank gilt auch unseren Kollegen, die uns intensiv beim Schreiben der Best Practices unterstützt haben und diese anschließend Korrektur lasen. Hier sind vor allem die Kollegen Holger Biber, Roland Hoyss, Christian Wippermann, Yvonne Jasiewicz und Dr. Andreas Leitheusser aus dem Bereich Security Development sowie Frank Buchholz vom Global CoE für Security Services zu erwähnen. Ohne ihr Engagement wäre die Erstellung und Überarbeitung dieses Buches nicht möglich gewesen.

Natürlich dürfen wir unsere Kunden nicht vergessen: Ohne die spezifischen Problemstellungen in ihren Projekten wären wir nicht auf die Idee zu dem ein oder ande-

ren Tipp oder Trick gekommen. Außerdem haben sie die Auswahl der Themen maßgeblich beeinflusst, da typische Probleme immer wieder und in zahlreichen Unternehmen auftreten. Wir haben uns über positives Feedback und konstruktive Kritik gefreut und beides bei der Erstellung dieser 2. Auflage berücksichtigt.

Last, but not least gilt unser besonderer Dank für die Korrekturen, Ergänzungen und vor allem ihre Geduld Janina Karrasch (SAP PRESS).

Anna Otto und Katharina Stelzner