

Auf einen Blick

TEIL I Grundlagen und Zusammenhänge des SAP-Berechtigungswesens

1	Grundlagen	25
2	Technische Elemente der SAP-Berechtigungsverwaltung	53
3	Konzeption und Dokumentation von SAP-Berechtigungskonzepten	85
4	Organisatorische Herausforderungen im Benutzer- und Berechtigungsmanagement	117
5	Werkzeuge für das SAP-Benutzer- und Berechtigungsmanagement	143

TEIL II Praktische Berechtigungsverwaltung in SAP S/4HANA

6	Rollenpflege	181
7	Berechtigungen in SAP Fiori	259
8	Berechtigungen in SAP HANA	325
9	Fehlerbehebung und Traces	351
10	Benutzermanagement	389
11	Praxisübungen zum Customizing	445
12	Monitoring von kritischen Berechtigungen	489
13	Methodische Vorgehensweisen im Tages- und Projektbetrieb	519

Inhalt

Einleitung	17
------------------	----

TEIL I Grundlagen und Zusammenhänge des SAP-Berechtigungswesens

1 Grundlagen	25
<hr/>	
1.1 Was sind SAP-Berechtigungen?	25
1.2 Der Unterschied zwischen SAP-Berechtigungen und SAP-Sicherheit	27
1.3 Die historische Entwicklung von SAP-Berechtigungen	28
1.4 Berechtigungen in SAP ECC	29
1.5 Berechtigungen in SAP S/4HANA	31
1.5.1 Berechtigungen bei der Umstellung auf SAP S/4HANA	33
1.5.2 Systemkonvertierung	34
1.5.3 Neuimplementierung	36
1.5.4 Selektive Datenübernahme	37
1.6 Berechtigungen im Kontext der SAP-Bereitstellungs- optionen	37
1.6.1 Berechtigungen in Cloud-Lösungen	37
1.6.2 Bereitstellungsoptionen für SAP Fiori	42
1.7 Grundlagen der SAP-Fiori-Berechtigungen	43
1.7.1 SAP-Fiori-Architektur	44
1.7.2 Berechtigungsprüfung für SAP-Fiori-Apps	48
1.7.3 Berechtigungsprüfung beim Start der SAP-Fiori-Apps	50
1.8 Zusammenfassung	52

2 Technische Elemente der SAP-Berechtigungsverwaltung 53

2.1	Rollenverwaltung	53
2.1.1	Rollen	54
2.1.2	Profile	57
2.1.3	Menüobjekte	57
2.1.4	Berechtigungsobjekte	59
2.2	Benutzerverwaltung	62
2.2.1	Benutzerstammsatz	62
2.2.2	Benutzertypen	64
2.2.3	Single Sign-on	66
2.3	Customizing und Einstellungen	67
2.3.1	SAP-Vorschlagswerte	67
2.3.2	Ausschalten der Berechtigungsprüfungen	70
2.3.3	SAP-Standardtabellen zur Steuerung der Benutzer- und Berechtigungsverwaltung	72
2.4	Post-Upgrade-Tätigkeiten in der Transaktion SU25	72
2.4.1	Installation des Profilgenerators – Kundentabellen werden initial befüllt (Schritt 1)	73
2.4.2	Automatischer Abgleich mit SU22-Daten (Schritt 2a)	74
2.4.3	Modifikationsabgleich mit SU22-Daten (Schritt 2b)	75
2.4.4	Zu überprüfende Rollen (Schritt 2c)	76
2.4.5	Suche nach obsoleten Anwendungen (2d)	76
2.5	CDS-Views	77
2.6	Berechtigungstraces	80
2.6.1	Berechtigungstrace in der Transaktion STUSOBTRACE	80
2.6.2	Systemtrace in den Transaktionen ST01 oder STAUTHTRACE	81
2.6.3	Benutzertrace für Berechtigungsprüfungen in der Transaktion STUSERTRACE	82
2.7	Zusammenfassung	83

3 Konzeption und Dokumentation von SAP-Berechtigungskonzepten 85

3.1	Konzeptionelle Grundsatzfragen	85
3.1.1	Rollenkonzept gestalten	86
3.1.2	SAP Fiori Launchpad gestalten	97
3.2	Ein SAP-Berechtigungskonzept erstellen	105
3.3	SAP-Notfallbenutzerkonzept	109
3.4	Kritische Berechtigungen	113
3.5	Zusammenfassung	115

4 Organisatorische Herausforderungen im Benutzer- und Berechtigungsmanagement 117

4.1	Die Beteiligten	117
4.2	Prozesse im Berechtigungswesen	119
4.2.1	Rollenanlage und Rollenmodifikation	119
4.2.2	Benutzeranlage, Rollenzuweisung, Rollenentzug	120
4.2.3	Periodische Prüfung der Berechtigungen	122
4.2.4	Risikoanalyse der Berechtigungen	122
4.3	Aufgaben und Aktivitäten im Tagesbetrieb	123
4.4	Vorgehensweise im Projektbetrieb	125
4.4.1	Erstellung eines neues Berechtigungskonzepts im Rahmen der SAP-Einführung	126
4.4.2	Migration des Berechtigungskonzepts aus SAP ECC in SAP S/4HANA	129
4.4.3	Redesign eines Berechtigungskonzepts	133
4.5	Agile Projekte	135
4.6	Zusammenfassung	141

5

Werkzeuge für das SAP-Benutzer- und Berechtigungsmanagement

143

5.1	Einsatzbereiche von Berechtigungsverwaltungswerkzeugen	144
5.2	Anforderungen und Bewertungskriterien	145
5.3	Übersicht der Werkzeuge	146
5.3.1	apm Suite von Valantic	146
5.3.2	CheckAud von IBS Schreiber	147
5.3.3	Easy Content Solution von IBS Schreiber	149
5.3.4	mesaforte.Suite von wikima4	152
5.3.5	SAP Access Control	157
5.3.6	SAP Cloud Identity Access Governance	158
5.3.7	SAP Solution Manager	159
5.3.8	SAST-Suite von akquinet	160
5.3.9	SIVIS Enterprise Security von SIVIS	163
5.3.10	SUIM Solution Suite von SUIM	165
5.3.11	Xiting Authorization Management Suite von Xiting	168
5.3.12	Xiting Central Workflows von Xiting	171
5.3.13	Berechtigungsverwaltungswerkzeuge und ihre Funktionen auf einen Blick	172
5.4	Zusammenfassung	178

TEIL II

Praktische Berechtigungsverwaltung in SAP S/4HANA

6

Rollenpflege

181

6.1	Eine Namenskonvention für Rollen festlegen	182
6.2	Einzel- und Sammelrollen anlegen und pflegen	186
6.2.1	Einzelrolle anlegen	186
6.2.2	Rolle ableiten	199
6.2.3	Sammelrolle anlegen	206
6.2.4	Rolle ändern	210
6.2.5	Rollen transportieren, herunterladen und hochladen	217
6.2.6	Rollenstatus prüfen und Profile generieren	223
6.2.7	Rollen löschen	225
6.2.8	Grundrolle anlegen	227
6.2.9	Customizing-Rollen anlegen	230

6.3	Massenänderungen in Rollen durchführen	232
6.3.1	Massenänderungen mit der Transaktion PFCGMASVAL durchführen	233
6.3.2	Massenänderungen mit der Transaktion PFCG durchführen	236
6.3.3	Massenänderungen mit der Transaktion SECATT durchführen	238
6.4	Auswertungsmöglichkeiten und SAP-Tabellen für die Rollenpflege	247
6.4.1	Anwendungsfall 1: Eine Liste aller Rollen, die eine bestimmte Transaktion beinhalten, erzeugen	248
6.4.2	Anwendungsfall 2: Eine Liste aller Rollen, die ein bestimmtes Berechtigungsobjekt mit bestimmten Werten beinhalten, erzeugen	252
6.4.3	Anwendungsfall 3: Eine Liste der abgeleiteten Rollen von Masterrollen erzeugen	253
6.4.4	Anwendungsfall 4: Eine Liste mit den Berechtigungs- objekten und ihren Status in den Rollen erzeugen	254
6.4.5	Anwendungsfall 5: Rollenänderungen auswerten	256
6.5	Zusammenfassung	258

7 Berechtigungen in SAP Fiori 259

7.1	Übersicht der Aktivitäten für die Pflege der Fiori- Berechtigungen	260
7.2	Namenskonvention für SAP-Fiori-UI-Entitäten	264
7.3	Kachelkataloge anlegen und pflegen	270
7.4	Rolle aktivieren	277
7.5	Kachelgruppen anlegen und pflegen	280
7.6	Bereiche und Seiten für das SAP Fiori Launchpad anlegen und pflegen	284
7.7	Rolle testen	289
7.8	Fehlende Berechtigungen für OData-Services in die Rolle hinzufügen	291
7.9	Fiori-Kachel für SAP-GUI-Transaktion anlegen	292
7.10	Titel der SAP-Fiori-UI-Entitäten übersetzen	297

7.11	Schnelle Aktivierung von SAP Fiori	300
7.11.1	Schnelle Aktivierung von SAP Fiori im Sandboxsystem	300
7.11.2	Schnelle Aktivierung von SAP Fiori in der Produktivumgebung	308
7.12	Migration von Fiori-Kachelgruppen zu Bereichen und Seiten	312
7.12.1	Bereiche und Seiten aktivieren	313
7.12.2	Launchpad-Konfigurationsparameter für Bereiche setzen	313
7.12.3	Geschäftsrollen von Fiori-Kachelgruppen zu Bereichen und Seiten migrieren	314
7.12.4	Bereiche zum Standard-Layoutmodus machen	314
7.13	SAP Fiori Apps Reference Library	315
7.14	Auswertungsmöglichkeiten für die SAP-Fiori- Berechtigungen	319
7.15	Zusammenfassung	322

8 **Berechtigungen in SAP HANA** 325

8.1	Benutzer pflegen	325
8.1.1	Benutzertypen	326
8.1.2	Benutzerpflege mit SAP HANA Cockpit	328
8.1.3	Benutzergruppen	330
8.2	Standardbenutzer	332
8.3	Rollen erstellen und zuweisen	337
8.3.1	Berechtigungen	338
8.3.2	Rollen	344
8.3.3	Analyse von fehlenden Berechtigungen	348
8.4	Zusammenfassung	350

9 **Fehlerbehebung und Traces** 351

9.1	Die Transaktion SU53	351
9.2	Traces in verschiedenen Szenarien anwenden	357
9.2.1	Berechtigungsfehler lösen mit der Transaktion STAUTHTRACE	357

9.2.2	Berechtigungs vorgeschlagswerte pflegen mit der Transaktion STUSOBTRACE	362
9.2.3	Berechtigungsfehler lösen mit der Transaktion STUSERTRACE	367
9.2.4	Überblick über die vorgestellten Traces	371
9.3	Fehlerbehebung für CDS-Views	371
9.4	Fehlerbehebung für SAP-Fiori-Berechtigungen	377
9.4.1	SAP-Fiori-App-Support-Tool	378
9.4.2	Typische Fehler in SAP Fiori	383
9.5	Zusammenfassung	388

10 Benutzermanagement 389

10.1	Benutzer im SAP-System anlegen und pflegen	389
10.2	Benutzer massenhaft mit LSMW anlegen	403
10.3	Benutzer in der zentralen Benutzerverwaltung (ZBV) pflegen	413
10.4	Rollen über das Organisationsmanagement zuweisen	415
10.5	Business-Benutzer anlegen und pflegen	421
10.5.1	Business-Benutzer mit HR-Integration anlegen und pflegen	422
10.5.2	Business-Benutzer ohne HR-Integration anlegen und pflegen	430
10.6	Hintergrundjobs für das Benutzermanagement	431
10.6.1	Report RHAUTUPD_NEW	431
10.6.2	Report PRGN_COMPRESS_TIMES	433
10.6.3	Report RSUSR_LOCK_USERS	433
10.7	SAP-Standardbenutzer	435
10.7.1	Benutzer SAP*	435
10.7.2	Benutzer DDIC	436
10.7.3	Benutzer SAPCPIC	436
10.7.4	Benutzer TMSADM	436
10.8	Auswertungsmöglichkeiten und SAP-Tabellen für das Benutzermanagement	438
10.8.1	Anwendungsfall 1: Sie benötigen eine Liste aller Dialogbenutzer, die Zugriff auf eine bestimmte Transaktion haben	439

10.8.2	Anwendungsfall 2: Sie möchten prüfen, ob zwei Benutzer die gleichen Berechtigungen haben	440
10.8.3	Anwendungsfall 3: Sie möchten sehen, welche Änderungen am Benutzerstammsatz vorgenommen wurden	441
10.8.4	Anwendungsfall 4: Sie möchten prüfen, ob oder wann Benutzer sich das letzte Mal am System angemeldet haben	443
10.9	Zusammenfassung	444

11 Praxisübungen zum Customizing 445

11.1	Arbeitsschritte im SU25-Abgleich	446
11.1.1	Pre-Upgrade: Praxisübung zu Report SU24_AUTO_REPAIR: Ergänze fehlende Modifikationsflags	447
11.1.2	Pre-Upgrade: Praxisübung zur Erstellung eines Backups	448
11.1.3	Pre-Upgrade: Praxisübung zur Prüfung von kunden-eigenen Organisationsebenen	451
11.1.4	Post-Upgrade: Praxisübung zu SAP-Hinweis 440231	453
11.1.5	Post-Upgrade: Praxisübung zu Report SU2X_CHECK_CONSISTENCY	453
11.1.6	Post-Upgrade: Praxisübung zu Report SU24_AUTO_REPAIR	455
11.1.7	Post-Upgrade: Praxisübung zu Schritt 2a	456
11.1.8	Post-Upgrade: Praxisübung zu Transaktion SU25 Schritt 2b	458
11.1.9	Post-Upgrade: Praxisübung zu Report SU24_AUTO_REPAIR	460
11.1.10	Post-Upgrade: Praxisübung zu Transaktion SU25 Schritt 2c	461
11.1.11	Post-Upgrade: Praxisübung zu Transaktion SU25 Schritt 2d	463
11.1.12	Post-Upgrade: Transport der SU24-Daten und der Rollen in die Folgesysteme	465
11.2	Praxisübungen zur Anzeige und Pflege von Vorschlagswerten in der Transaktion SU24	465
11.2.1	Anzeige von SU24-Vorschlagsdaten	467
11.2.2	Berechtigungsobjekte mit dem Status »Verändert«	470

11.2.3	Änderung von Vorschlagswerten in der Transaktion SU24	472
11.2.4	Anlegen von Varianten in der Transaktion SU24	475
11.3	Berechtigungen für die Geschäftspartner-Pflege einrichten	479
11.3.1	Praxisübung zur Einrichtung von Berechtigungsgruppen für die Anzeige/Pflege in Transaktion BP	480
11.3.2	Praxisübung zur Einrichtung von Feldgruppen für die Geschäftspartner-Pflege	485
11.4	Zusammenfassung	486

12 Monitoring von kritischen Berechtigungen 489

12.1	Kritische Berechtigungen definieren	489
12.2	Prüfregeln anlegen	502
12.3	Prüfung ausführen	506
12.4	SAP-Security-Audit-Log konfigurieren	509
12.5	Zusammenfassung	516

13 Methodische Vorgehensweisen im Tages- und Projektbetrieb 519

13.1	Den Betrieb eines SAP-Berechtigungskonzepts übernehmen	519
13.2	SAP-Systeme auf die Revision vorbereiten	532
13.2.1	Standardbenutzer prüfen	532
13.2.2	Benutzer mit kritischen Profilen identifizieren	532
13.2.3	Die Anzahl der Benutzer mit kritischen Berechtigungen identifizieren und reduzieren	534
13.2.4	Die korrekte Umsetzung der Passwortrichtlinien im System prüfen	535
13.2.5	Die Konfiguration des SAP-Security-Audit-Log prüfen	539
13.2.6	Die Dokumentation der Prozesse im Benutzer- und Berechtigungsmanagement aktualisieren	539
13.3	IAM-Prozesse optimieren	540

13.4 Ein neues SoD-Regelwerk einführen und Konflikte	
eliminieren	543
13.4.1 Den SoD-Bericht in verständlicher Form darstellen	547
13.4.2 Den Zyklus der Bearbeitung der SoD-Konflikte organisieren	548
13.4.3 Kennzahlen zur Fortschrittsmessung bestimmen	548
13.4.4 Sicherstellen, dass die Einzelrollen und Sammelrollen keine SoD-Konflikte beinhalten	549
13.4.5 Prüfen, ob die Rollen, die die meisten SoD-Konflikte verursachen, richtig definiert und gepflegt sind	549
13.4.6 Die Risikoeinstufung der SoD-Konflikte prüfen	549
13.4.7 Die SoD-Regeln korrigieren	550
13.4.8 Die Rollenzuweisung an die Benutzer anpassen	550
13.4.9 Überwachung der SoD-Konflikte in den Tagesbetrieb überführen	550
13.5 Ein Berechtigungsproblem lösen	551
13.5.1 Das Fehlerprotokoll aus der Transaktion SU53 herunterladen	551
13.5.2 Das Fehlerprotokoll aus dem Fiori-App-Support-Tool herunterladen	552
13.5.3 Den Berechtigungstrace ausführen	553
13.5.4 Eine fehlende Berechtigung erteilen	555
13.6 Vergabe der Transaktionen SE16 und SM30 vermeiden	556
13.6.1 Eine Parametertransaktion für die Transaktion SE16 anlegen	556
13.6.2 Eine Parametertransaktion für die Transaktion SM30 anlegen	558
13.7 ST03N-Daten verwenden	561
13.7.1 ST03N-Profile prüfen und ändern	561
13.7.2 ST03N-Daten auswerten	563
13.8 Zusammenfassung	564
Glossar	567
 Das Autorenteam	 573
Index	575