

# 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

---

<b>1.1 Was sind SAP-Berechtigungen?</b> .....	25
<b>1.2 Der Unterschied zwischen SAP-Berechtigungen und SAP-Sicherheit</b> .....	27
<b>1.3 Die historische Entwicklung von SAP-Berechtigungen</b> .....	28
<b>1.4 Berechtigungen in SAP ECC</b> .....	29
<b>1.5 Berechtigungen in SAP S/4HANA</b> .....	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
<b>1.6 Berechtigungen im Kontext der SAP-Bereitstellungs- optionen</b> .....	37
1.6.1 Berechtigungen in Cloud-Lösungen .....	37
1.6.2 Bereitstellungsoptionen für SAP Fiori .....	42
<b>1.7 Grundlagen der SAP-Fiori-Berechtigungen</b> .....	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
<b>1.8 Zusammenfassung</b> .....	52

## 2 Technische Elemente der SAP-Berechtigungsverwaltung

---

53

<b>2.1 Rollenverwaltung</b> .....	53
2.1.1 Rollen .....	54
2.1.2 Profile .....	57
2.1.3 Menüobjekte .....	57
2.1.4 Berechtigungsobjekte .....	59
<b>2.2 Benutzerverwaltung</b> .....	62
2.2.1 Benutzerstammsatz .....	62
2.2.2 Benutzertypen .....	64
2.2.3 Single Sign-on .....	66
<b>2.3 Customizing und Einstellungen</b> .....	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
<b>2.4 Post-Upgrade-Tätigkeiten in der Transaktion SU25</b> .....	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
<b>2.5 CDS-Views</b> .....	77
<b>2.6 Berechtigungstraces</b> .....	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
<b>2.7 Zusammenfassung</b> .....	83

### **3 Konzeption und Dokumentation von SAP-Berechtigungskonzepten** 85

---

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

### **4 Organisatorische Herausforderungen im Benutzer- und Berechtigungsmanagement** 117

---

<b>4.1 Die Beteiligten</b> .....	117
<b>4.2 Prozesse im Berechtigungswesen</b> .....	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
<b>4.3 Aufgaben und Aktivitäten im Tagesbetrieb</b> .....	123
<b>4.4 Vorgehensweise im Projektbetrieb</b> .....	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
<b>4.5 Agile Projekte</b> .....	135
<b>4.6 Zusammenfassung</b> .....	141

## **5 Werkzeuge für das SAP-Benutzer- und Berechtigungsmanagement** 143

---

<b>5.1</b>	<b>Einsatzbereiche von Berechtigungsverwaltungswerkzeugen</b> .....	144
<b>5.2</b>	<b>Anforderungen und Bewertungskriterien</b> .....	145
<b>5.3</b>	<b>Übersicht der Werkzeuge</b> .....	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
<b>5.4</b>	<b>Zusammenfassung</b> .....	178

## **TEIL II Praktische Berechtigungsverwaltung in SAP S/4HANA**

### **6 Rollenpflege** 181

---

<b>6.1</b>	<b>Eine Namenskonvention für Rollen festlegen</b> .....	182
<b>6.2</b>	<b>Einzel- und Sammelrollen anlegen und pflegen</b> .....	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

<b>6.3</b>	<b>Massenänderungen in Rollen durchführen</b> .....	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
<b>6.4</b>	<b>Auswertungsmöglichkeiten und SAP-Tabellen für die Rollenpflege</b> .....	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
<b>6.5</b>	<b>Zusammenfassung</b> .....	258

## **7 Berechtigungen in SAP Fiori** 259

---

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

<b>7.11</b>	<b>Schnelle Aktivierung von SAP Fiori</b> .....	300
7.11.1	Schnelle Aktivierung von SAP Fiori im Sandboxsystem ....	300
7.11.2	Schnelle Aktivierung von SAP Fiori in der Produktivumgebung .....	308
<b>7.12</b>	<b>Migration von Fiori-Kachelgruppen zu Bereichen und Seiten</b> .....	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
<b>7.13</b>	<b>SAP Fiori Apps Reference Library</b> .....	315
<b>7.14</b>	<b>Auswertungsmöglichkeiten für die SAP-Fiori- Berechtigungen</b> .....	319
<b>7.15</b>	<b>Zusammenfassung</b> .....	322

## **8 Berechtigungen in SAP HANA** 325

---

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

## **9 Fehlerbehebung und Traces** 351

---

<b>9.1</b>	<b>Die Transaktion SU53</b> .....	351
<b>9.2</b>	<b>Traces in verschiedenen Szenarien anwenden</b> .....	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
<b>9.3</b>	<b>Fehlerbehebung für CDS-Views .....</b>	<b>371</b>
<b>9.4</b>	<b>Fehlerbehebung für SAP-Fiori-Berechtigungen .....</b>	<b>377</b>
9.4.1	SAP-Fiori-App-Support-Tool .....	378
9.4.2	Typische Fehler in SAP Fiori .....	383
<b>9.5</b>	<b>Zusammenfassung .....</b>	<b>388</b>

## **10 Benutzermanagement** 389

---

<b>10.1</b>	<b>Benutzer im SAP-System anlegen und pflegen .....</b>	<b>389</b>
<b>10.2</b>	<b>Benutzer massenhaft mit LSMW anlegen .....</b>	<b>403</b>
<b>10.3</b>	<b>Benutzer in der zentralen Benutzerverwaltung (ZBV) pflegen .....</b>	<b>413</b>
<b>10.4</b>	<b>Rollen über das Organisationsmanagement zuweisen .....</b>	<b>415</b>
<b>10.5</b>	<b>Business-Benutzer anlegen und pflegen .....</b>	<b>421</b>
10.5.1	Business-Benutzer mit HR-Integration anlegen und pflegen .....	422
10.5.2	Business-Benutzer ohne HR-Integration anlegen und pflegen .....	430
<b>10.6</b>	<b>Hintergrundjobs für das Benutzermanagement .....</b>	<b>431</b>
10.6.1	Report RHAUTUPD_NEW .....	431
10.6.2	Report PRGN_COMPRESS_TIMES .....	433
10.6.3	Report RSUSR_LOCK_USERS .....	433
<b>10.7</b>	<b>SAP-Standardbenutzer .....</b>	<b>435</b>
10.7.1	Benutzer SAP* .....	435
10.7.2	Benutzer DDIC .....	436
10.7.3	Benutzer SAPCPIC .....	436
10.7.4	Benutzer TMSADM .....	436
<b>10.8</b>	<b>Auswertungsmöglichkeiten und SAP-Tabellen für das Benutzermanagement .....</b>	<b>438</b>
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
<b>10.9</b>	<b>Zusammenfassung</b> .....	<b>444</b>

## **11 Praxisübungen zum Customizing** 445

---

<b>11.1</b>	<b>Arbeitsschritte im SU25-Abgleich</b> .....	<b>446</b>
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 kundeneigenen 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
<b>11.2</b>	<b>Praxisübungen zur Anzeige und Pflege von Vorschlagswerten in der Transaktion SU24</b> .....	<b>465</b>
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
<b>11.3</b>	<b>Berechtigungen für die Geschäftspartner-Pflege einrichten .....</b>	<b>479</b>
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
<b>11.4</b>	<b>Zusammenfassung .....</b>	<b>486</b>

## **12 Monitoring von kritischen Berechtigungen** 489

---

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

## **13 Methodische Vorgehensweisen im Tages- und Projektbetrieb** 519

---

<b>13.1</b>	<b>Den Betrieb eines SAP-Berechtigungskonzepts übernehmen .....</b>	<b>519</b>
<b>13.2</b>	<b>SAP-Systeme auf die Revision vorbereiten .....</b>	<b>532</b>
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
<b>13.3</b>	<b>IAM-Prozesse optimieren .....</b>	<b>540</b>

<b>13.4 Ein neues SoD-Regelwerk einführen und Konflikte</b>	
<b>eliminieren</b>	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
<b>13.5 Ein Berechtigungsproblem lösen</b>	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
<b>13.6 Vergabe der Transaktionen SE16 und SM30 vermeiden</b>	556
13.6.1 Eine Parametertransaktion für die Transaktion SE16 anlegen	556
13.6.2 Eine Parametertransaktion für die Transaktion SM30 anlegen	558
<b>13.7 ST03N-Daten verwenden</b>	561
13.7.1 ST03N-Profile prüfen und ändern	561
13.7.2 ST03N-Daten auswerten	563
<b>13.8 Zusammenfassung</b>	564
<b>Glossar</b>	567
Das Autorenteam	573
Index	575