

Auf einen Blick

1	Umgang mit dem SAP-System und Werkzeuge zur Prüfung	31
2	Aufbau von SAP-Systemen und Systemlandschaften	125
3	Allgemeine Systemsicherheit	175
4	Protokollierungskomponenten	249
5	Remote Function Calls	365
6	Der Verbuchungsvorgang	403
7	Benutzerauswertungen	429
8	Customizing des SAP-Systems	515
9	Entwicklung in SAP-Systemen	587
10	Berechtigungskonzept in ABAP-Systemen	687
11	Praktische Prüfung von Berechtigungen	797
12	SAP HANA	867

Inhalt

Einleitung	25
1 Umgang mit dem SAP-System und Werkzeuge zur Prüfung	31
1.1 Transaktionen und SAP-Fiori-Apps	31
1.1.1 Transaktionen	32
1.1.2 SAP-Fiori-Apps	33
1.2 Reports	35
1.2.1 Das Konzept der Reports	35
1.2.2 Aufrufen von Reports	37
1.2.3 Exportieren der Reportergebnisse	39
1.2.4 Festlegung des Standardpfads zum Speichern	41
1.2.5 Speichern der Selektionsangaben (Varianten)	41
1.3 Anzeigen von Tabellen	43
1.3.1 Anzeigetransaktionen für Tabellen	43
1.3.2 Transaktion SE16	45
1.3.3 Transaktionen SE16N, S416N, S4H16N	48
1.3.4 Transaktionen SE16H, S416H, S4H16H	48
1.3.5 Transaktionen SE16S, S416S und S4H16S	51
1.3.6 Suchen von Tabellen	53
1.3.7 Exportieren von Tabellen	57
1.3.8 Speichern der Selektionsangaben (Varianten)	58
1.4 Das Benutzerinformationssystem	59
1.5 Listen als PDF-Datei speichern	62
1.6 Nutzung der Zugriffsstatistik für Prüfungen	63
1.6.1 Funktionsweise	63
1.6.2 Analyse von aufgerufenen Transaktionen und Reports	66
1.6.3 Analyse von RFC-Aufrufen	69
1.7 Tabelleninhalte mit dem QuickViewer auswerten	71
1.7.1 Erstellen eines QuickViews auf eine einzelne Tabelle	72
1.7.2 Erstellen eines QuickViews mit einem Tabellen-Join	76
1.7.3 Erstellen eines QuickViews mit einer logischen Datenbank	79

1.8 SQL-Trace	80
1.8.1 Aktivierung des SQL-Trace	81
1.8.2 Auswertung des Trace	82
1.9 Audit Information System	84
1.9.1 Die Auditstruktur	85
1.9.2 Durchführen eines Audits	87
1.9.3 Berechtigungen zur Nutzung des Audit Information Systems	89
1.10 SAP Access Control	90
1.10.1 Komponenten von SAP Access Control	90
1.10.2 Regelwerke	91
1.10.3 Auswertung der Regelwerke	96
1.10.4 SAP-Access-Control-Regelwerk für dieses Buch	102
1.11 SAP Enterprise Threat Detection	103
1.11.1 Angriffe auf SAP-Systeme – nur etwas für versierte Hacker?	104
1.11.2 Standardüberwachung von SAP-Systemen	105
1.11.3 Zentrale Sammlung von Protokollen in SAP Enterprise Threat Detection	107
1.11.4 Automatisierte Analyse von Protokollen in SAP Enterprise Threat Detection	108
1.11.5 Pseudonymisierung von Benutzernamen	111
1.11.6 Auswertung eingespielter Security Notes	113
1.12 Zugriff auf SAP HANA für Prüfer	115
1.12.1 Zugriff auf SAP HANA über das DBA Cockpit	115
1.12.2 Zugriff auf SAP HANA über das SAP HANA Cockpit	118
1.12.3 Skriptgesteuerter Export von Daten aus der SAP-HANA-Datenbank	123
 2 Aufbau von SAP-Systemen und Systemlandschaften	 125
2.1 SAP NetWeaver und SAP-Komponenten	125
2.1.1 Komponenten von SAP NetWeaver	126
2.1.2 Komponenten der SAP Business Suite	127
2.1.3 Komponenten von SAP S/4HANA	128
2.1.4 Nicht mehr unterstützte Komponenten in SAP S/4HANA	129
2.1.5 Checkliste	131

2.2 Technischer Aufbau von SAP-Systemen	131
2.2.1 Applikations- und Datenbankserver	131
2.2.2 SAP-Fiori-Frontend-Server und SAP-Backend-System	133
2.2.3 Instanzen	134
2.2.4 SAP-Prozesse und -Dienste	135
2.2.5 Checkliste	138
2.3 Systemlandschaften	139
2.3.1 Drei-System-Landschaften	139
2.3.2 SAP-Fiori-Systemlandschaften	141
2.3.3 Systemarten	143
2.3.4 Checkliste	144
2.4 Das Mandantenkonzept	145
2.4.1 Standardmandanten eines SAP-Systems	146
2.4.2 Eigenschaften von Mandanten	147
2.4.3 Protokollierung der Änderungen von Mandanteneigenschaften	150
2.4.4 Risiko beim Anlegen neuer Mandanten	151
2.4.5 Mandantenkopien	153
2.4.6 Zugriffsrechte	156
2.4.7 Checkliste	162
2.5 Sicherheit im Mandanten 000	163
2.5.1 Zugriff auf Daten des Produktivmandanten	164
2.5.2 Systemeinstellungen pflegen	170
2.5.3 Anwendungsentwicklung	172
2.5.4 Gesetzeskritische Berechtigungen	173
2.5.5 Patterns in SAP Enterprise Threat Detection	173
2.5.6 Checkliste	173
 3 Allgemeine Systemsicherheit	 175
3.1 Grundlagen für die Prüfung der Systemsicherheit	175
3.1.1 Der Releasestand des SAP-Systems	176
3.1.2 Systemparameter	177
3.1.3 Zugriffsrechte	181
3.1.4 Checkliste	182
3.2 Anmeldesicherheit	183
3.2.1 Unzulässige Kennwörter – Tabelle USR40	184
3.2.2 Protokolle von Mehrfachanmeldungen	185
3.2.3 Systemparameter zur Anmeldesicherheit	186

3.2.4	Sicherheitsrichtlinien	195
3.2.5	Schutz vor Kennwort-Hacking	199
3.2.6	Unternehmenseigene Erweiterungen zur Anmeldesicherheit	200
3.2.7	Patterns in SAP Enterprise Threat Detection	201
3.2.8	Zugriffsrechte	201
3.2.9	Checkliste	204
3.3	Das Notfallbenutzerkonzept	206
3.3.1	Konzept für Notfallbenutzer	206
3.3.2	Transaktion SE16N_EMERGENCY	207
3.3.3	Checkliste	209
3.4	Sperren von Transaktionscodes	210
3.4.1	Zugriffsrechte	212
3.4.2	Checkliste	213
3.5	Logische Betriebssystemkommandos	214
3.5.1	Funktionsweise	214
3.5.2	Der Report RSBDCOS0	218
3.5.3	Logische Betriebssystemkommandos zur Prüfung nutzen	219
3.5.4	Patterns in SAP Enterprise Threat Detection	220
3.5.5	Zugriffsrechte	220
3.5.6	Checkliste	222
3.6	Drucken und Speichern	223
3.6.1	Der Druckvorgang	223
3.6.2	Schutz von Druckaufträgen	228
3.6.3	Speichern von Daten in Dateien	228
3.6.4	Patterns in SAP Enterprise Threat Detection	229
3.6.5	Zugriffsrechte	229
3.6.6	Checkliste	230
3.7	Batch-Input	232
3.7.1	Analyse des Batch-Input-Verfahrens	233
3.7.2	Berechtigungen für Batch-Input-Mappen	236
3.7.3	Zugriffsrechte	238
3.7.4	Checkliste	240
3.8	Funktionen von SAP Business Warehouse	241
3.8.1	Datenextraktion	242
3.8.2	Der Extraktorchecker	242
3.8.3	Berechtigungen für die Extraktion einschränken	245
3.8.4	Zugriffsrechte	246
3.8.5	Checkliste	247

4	Protokollierungskomponenten	249
4.1	Security-Audit-Log	249
4.1.1	Konfiguration des Security-Audit-Logs	251
4.1.2	Auswertung des Security-Audit-Logs	258
4.1.3	Pseudonymisierte Auswertung des Security-Audit-Logs	259
4.1.4	Löschen von Security-Audit-Log-Protokollen	261
4.1.5	Konzept zum Einsatz des Security-Audit-Logs	262
4.1.6	Zugriffsrechte	266
4.1.7	Checkliste	270
4.2	Systemprotokollierung	271
4.2.1	Auswertung des SysLogs	272
4.2.2	Meldungen des SysLogs	274
4.2.3	Zugriffsrechte	277
4.2.4	Checkliste	277
4.3	Protokollierung von Tabellenänderungen	278
4.3.1	Aktivierung der Tabellenprotokollierung	279
4.3.2	Protokollierung bei Transporten	281
4.3.3	Protokollierung der einzelnen Tabellen	283
4.3.4	Versionierung der Protokolleigenschaft von Tabellen	288
4.3.5	Protokollierung unternehmenseigener Tabellen	291
4.3.6	Auswertung von Tabellenänderungen	295
4.3.7	Löschen von Tabellenänderungsprotokollen	299
4.3.8	Zugriffsrechte	300
4.3.9	Checkliste	302
4.4	Protokollierung über Änderungsbelege	304
4.4.1	Suchen von über Änderungsbelege protokollierten Tabellen	307
4.4.2	Residenzzeiten für Änderungsbelege	308
4.4.3	Auswertung der Änderungsbelege	309
4.4.4	Löschen von Änderungsbelegen	310
4.4.5	Ändern von Änderungsbelegobjekten	311
4.4.6	Zugriffsrechte	311
4.4.7	Checkliste	313
4.5	Versionsverwaltung	313
4.5.1	Anzeige der Versionen zu einzelnen Programmen	314
4.5.2	Anzeige der Versionen aller versionierbaren Objekte	316
4.5.3	Versionserzeugung bei Importen	317

4.5.4	Löschen der Versionshistorien	318
4.5.5	Checkliste	319
4.6	Lesezugriffsprotokollierung	320
4.6.1	Protokollierung des Zugriffs auf sensible Felder	321
4.6.2	Protokollierung des Aufrufs von Funktionsbausteinen	324
4.6.3	Konfigurationseinstellungen	326
4.6.4	Verwaltungsprotokoll	326
4.6.5	Zugriffsrechte	327
4.6.6	Checkliste	330
4.7	Zugriffsstatistik	331
4.7.1	Analyse einzelner Benutzer oder Funktionen	333
4.7.2	Analyse von Transaktionsaufrufen in Listenform	335
4.7.3	Analyse von RFC-Zugriffen	335
4.7.4	Langzeitauswertung der Statistik	336
4.7.5	Anonymisierte Auswertung von Statistiksätzen	340
4.7.6	Zugriffsrechte	340
4.7.7	Checkliste	341
4.8	Weitere Protokollkomponenten	342
4.8.1	Protokolle für die Systemänderbarkeit	342
4.8.2	Protokolle von Mandantenkopien	344
4.8.3	Protokolle von Änderungen an Systemparametern	344
4.8.4	Protokolle von Mehrfachanmeldungen	345
4.8.5	Protokolle von Änderungen an Betriebssystemkommandos	345
4.8.6	Jobprotokolle	345
4.8.7	Protokolle von Änderungen über Transaktion SE16N	346
4.8.8	Protokolle von Änderungen über den Generic Table Browser (GTB)	347
4.8.9	Protokolle von Änderungen an Sicherheitsrichtlinien	348
4.8.10	SAP Gateway – Fehlerprotokolle	348
4.8.11	Generische Auditauswertungen (Transaktion SAIS_MONI)	349
4.9	Systemüberwachung mit SAP Enterprise Threat Detection	351
4.9.1	Übertragung der Protokolle an SAP Enterprise Threat Detection	351
4.9.2	Auswahl der Patterns in SAP Enterprise Threat Detection	354
4.9.3	Definition eigener Patterns	355
4.9.4	Analyse mit SAP Enterprise Threat Detection	356
4.9.5	Zugriffsrechte	360
4.9.6	Checkliste	363

5	Remote Function Calls	365
5.1	Funktionsbausteine	365
5.1.1	Funktionsbausteine ohne Berechtigungsprüfungen	368
5.1.2	Funktionsbausteine mit schaltbaren Berechtigungen	369
5.1.3	Protokollierung von RFC-Aktionen	371
5.1.4	Patterns in SAP Enterprise Threat Detection	373
5.1.5	Zugriffsrechte	374
5.1.6	Checkliste	375
5.2	RFC-Verbindungen	376
5.2.1	Hinterlegte Kennwörter	379
5.2.2	Systemübergreifender Zugriff über Funktionsbausteine	380
5.2.3	Zugriffsrechte	382
5.2.4	Checkliste	382
5.3	Trusted Systems	383
5.3.1	Berechtigungen zur Nutzung von Trusted-Verbindungen	387
5.3.2	Zugriffsrechte	389
5.3.3	Checkliste	390
5.4	Zugriff von externen Programmen	391
5.4.1	Ermittlung der erforderlichen RFC-Berechtigungen	394
5.4.2	Zugriff auf das SAP-System über Microsoft Excel	395
5.4.3	ABAP-Quelltexte über RFC ausführen	397
5.4.4	Zugriffsrechte	399
5.4.5	Checkliste	400
6	Der Verbuchungsvorgang	403
6.1	Das Prinzip der Verbuchung	403
6.1.1	Die Verbuchungskomponenten	405
6.1.2	Auswertung der Verbuchung	407
6.1.3	Zugriffsrechte	412
6.1.4	Checkliste	413
6.2	Abgebrochene Buchungen	414
6.2.1	Kontrolle auf abgebrochene Buchungen	414
6.2.2	Die Abstimmanalyse der Finanzbuchhaltung (SAP ERP)	415
6.2.3	Zugriffsrechte	418
6.2.4	Checkliste	418

6.3	Die Belegnummernvergabe	419
6.3.1	Nummernkreisobjekte	420
6.3.2	Pufferung von Belegnummern	421
6.3.3	Suche nach Lücken in Belegnummern	425
6.3.4	Zugriffsrechte	426
6.3.5	Checkliste	426
7	Benutzerauswertungen	429
7.1	Organisatorische Regelungen	429
7.2	Die SAP-Standardbenutzer	433
7.2.1	Der Benutzer SAP*	434
7.2.2	Der Benutzer DDIC	435
7.2.3	Der Benutzer SAPCPIC	435
7.2.4	Der Benutzer TMSADM	435
7.2.5	Der Benutzer EARLYWATCH	436
7.2.6	Prüfen der Standardbenutzer	436
7.2.7	Weitere Standardbenutzer	438
7.2.8	Patterns in SAP Enterprise Threat Detection	439
7.2.9	Zugriffsrechte	439
7.2.10	Checkliste	441
7.3	Der Benutzerstammsatz	442
7.3.1	Benutzertypen	442
7.3.2	Eigenschaften der Benutzer	446
7.3.3	Auswertungen zu Benutzern	455
7.3.4	Patterns in SAP Enterprise Threat Detection	457
7.3.5	Zugriffsrechte	458
7.3.6	Checkliste	458
7.4	Referenzbenutzer	459
7.4.1	Zuordnung von Referenzbenutzern	459
7.4.2	Auswertung von Referenzbenutzerzuordnungen	460
7.4.3	Historie der Referenzbenutzerzuordnungen	461
7.4.4	Patterns in SAP Enterprise Threat Detection	462
7.4.5	Zugriffsrechte	462
7.4.6	Checkliste	464
7.5	Benutzergruppen	465
7.5.1	Patterns in SAP Enterprise Threat Detection	468

7.5.2	Zugriffsrechte	469
7.5.3	Checkliste	470
7.6	Sammelbenutzer	471
7.7	Benutzervermessungsdaten	474
7.7.1	Konfiguration der Vermessung	474
7.7.2	Prüfen der Systemvermessung	477
7.7.3	Zugriffsrechte	479
7.7.4	Checkliste	480
7.8	Initialkennwörter und Benutzersperrungen	480
7.8.1	Initialkennwörter	481
7.8.2	Produktivkennwörter	483
7.8.3	Benutzersperrungen	484
7.8.4	Auswertung gesperrter Benutzer	487
7.8.5	Patterns in SAP Enterprise Threat Detection	488
7.8.6	Zugriffsrechte	489
7.8.7	Checkliste	491
7.9	Benutzerstammsätze sperren und löschen	492
7.9.1	Funktionsweise	493
7.9.2	Wiederanlage von Benutzer	494
7.9.3	Vetoprüfungen beim Löschen von Benutzern	495
7.9.4	Zugriffsrechte	497
7.9.5	Checkliste	498
7.10	Kennwortverschlüsselung	499
7.10.1	Verschlüsselungsalgorithmen	499
7.10.2	Schutz vor Hacking der Kennwörter	501
7.10.3	Patterns in SAP Enterprise Threat Detection	501
7.10.4	Zugriffsrechte	503
7.10.5	Checkliste	504
7.11	Angemeldete Benutzer	505
7.11.1	Informationen zu angemeldeten Benutzern – Transaktion AL08	505
7.11.2	Informationen zu den Benutzer-Terminals – Tabelle USR41	506
7.11.3	Administrative Überwachung – Transaktion SM04	507
7.11.4	Protokollierung von Benutzeranmeldungen – Security-Audit-Log	507
7.11.5	Patterns in SAP Enterprise Threat Detection	508
7.11.6	Zugriffsrechte	508
7.11.7	Checkliste	509
7.12	Die Änderungshistorie zu Benutzern	509
7.12.1	Zugriffsrechte	512
7.12.2	Checkliste	512

8	Customizing des SAP-Systems	515
8.1	Das ABAP Dictionary	515
8.1.1	Aufbau des ABAP Dictionarys	516
8.1.2	Domänen	518
8.1.3	Datenelemente	522
8.1.4	Zugriffsrechte	524
8.1.5	Checkliste	525
8.2	Das Konzept der Tabellensteuerung	526
8.2.1	Eigenschaften von Tabellen	526
8.2.2	Mandantenabhängige Tabellen	529
8.2.3	Mandantenunabhängige Tabellen	530
8.2.4	Transparente Tabellen	531
8.2.5	Dokumentationen zu Tabellen	532
8.2.6	ABAP-Dictionary-Views	533
8.2.7	ABAP-CDS-Views	538
8.2.8	Unternehmenseigene Tabellen und Views	541
8.2.9	Zugriffsrechte	542
8.2.10	Checkliste	545
8.3	Zugriffe auf Tabellen	546
8.3.1	Anzeige von Tabelleninhalten in der Datenbank	546
8.3.2	Ändern von Tabellen im SAP-System	549
8.3.3	Einführungsleitfaden	551
8.3.4	Laufende Einstellungen	553
8.3.5	Patterns in SAP Enterprise Threat Detection	555
8.3.6	Zugriffsrechte	555
8.3.7	Checkliste	557
8.4	Berechtigungen für Tabellen und Views	558
8.4.1	Berechtigungsgruppen	558
8.4.2	Berechtigungsobjekte	560
8.4.3	Schutz von Tabellen ohne Berechtigungsgruppe	566
8.4.4	Prüfen der Berechtigungen zum Zugriff auf einzelne Tabellen/Views	567
8.4.5	Prüfung der Tabellenberechtigungen für einzelne Rollen oder Benutzer	568
8.4.6	Abgleich von Tabellenberechtigungsgruppen	570
8.4.7	Zugriffsrechte	570
8.4.8	Checkliste	573

8.5	Tabellenzugriffe auf Spalten und Feldwerte einschränken (GTB-Rollen)	574
8.5.1	Berechtigungen auf Spalten eingrenzen	575
8.5.2	Berechtigungen auf Feldwerte eingrenzen	577
8.5.3	Zuordnung der GTB-Rollen	578
8.5.4	Prüfung der GTB-Rollen	579
8.5.5	Voraussetzungen zur Nutzung von GTB-Rollen	582
8.5.6	Zugriffsrechte	583
8.5.7	Checkliste	584
9	Entwicklung in SAP-Systemen	587
9.1	Entwicklerrichtlinien	587
9.2	Entwickler- und Objektschlüssel	590
9.2.1	Entwickler- und Objektschlüssel in SAP S/4HANA	590
9.2.2	Entwicklerschlüssel	591
9.2.3	Objektschlüssel	594
9.2.4	Umgehung der Abfrage von Entwickler- und Objektschlüsseln	594
9.2.5	Zugriffsrechte	596
9.2.6	Checkliste	596
9.3	Systemänderbarkeit	598
9.3.1	Prüfung der Systemänderbarkeit	599
9.3.2	Zugriffsrechte	602
9.3.3	Checkliste	603
9.4	Das Transportsystem	604
9.4.1	Der Transport Organizer	604
9.4.2	Transport Management System	612
9.4.3	Der Ablauf eines Transports	618
9.4.4	Zeitnähe der Importe	621
9.4.5	Zugriffsrechte	623
9.4.6	Checkliste	627
9.5	Eigenentwicklungen in ABAP	629
9.5.1	Die Programmiersprache ABAP	630
9.5.2	ABAP-Namensräume	635
9.5.3	Gefahrenpunkte in der ABAP-Programmentwicklung	636
9.5.4	Prüfen der Eigenschaften von ABAP-Programmen	652
9.5.5	Inhaltliches Prüfen einzelner ABAP-Programme	653

9.5.6	Programmübergreifende Analyse von Quelltexten	654
9.5.7	Code Inspector	660
9.5.8	Code Vulnerability Analyzer	663
9.5.9	Die Versionshistorie	665
9.5.10	Patterns in SAP Enterprise Threat Detection	665
9.5.11	Checkliste	665
9.6	Transaktionen	667
9.6.1	Transaktionsarten	668
9.6.2	Pflege von Transaktionen	669
9.6.3	Protokollierung von Änderungen an Tabellen	670
9.6.4	Suche nach verwandten Transaktionen	671
9.6.5	Suche nach Transaktionen mit generischem Tabellenzugriff	672
9.6.6	Zugriffsrechte	674
9.6.7	Checkliste	674
9.7	Berechtigungen zur Anwendungsentwicklung	675
9.7.1	Das Berechtigungsobjekt S_DEVELOP	675
9.7.2	Weitere Berechtigungsobjekte zur Anwendungsentwicklung	677
9.7.3	Schutz von ABAP-Programmen durch Berechtigungsgruppen (S_PROGRAM)	678
9.7.4	Schutz von ABAP-Programmen nach Namen (S_PROGNAM)	682
9.7.5	Zugriffsrechte – Einzelberechtigungen	683
9.7.6	Zugriffsrechte – Funktionstrennungen	684
9.7.7	Patterns in SAP Enterprise Threat Detection	686
10	Berechtigungskonzept in ABAP-Systemen	687
10.1	Funktionsweise des Berechtigungskonzepts	688
10.1.1	Berechtigungsobjekte	689
10.1.2	Rollen	696
10.1.3	Sammelrollen	702
10.1.4	Profile	704
10.1.5	Berechtigungen	707
10.1.6	Ablauf einer Berechtigungsprüfung	709
10.1.7	Patterns in SAP Enterprise Threat Detection	711
10.1.8	Checkliste	711
10.2	Das Berechtigungskonzept in SAP S/4HANA	712
10.2.1	Simplification List for SAP S/4HANA	713
10.2.2	SAP Fiori Apps Reference Library	714
10.2.3	Das Konzept der SAP-Fiori-Apps	717

10.2.4	Kachelgruppen und -kataloge	719
10.2.5	Berechtigungen auf dem Frontend-Server	722
10.2.6	Berechtigungen auf dem Backend-Server	724
10.2.7	Auswertung von App-Berechtigungen für Benutzer	726
10.2.8	Auswertung von App-Berechtigungen in Rollen	727
10.2.9	Zugriffsrechte	729
10.2.10	Checkliste	731
10.3	Konzepte zum SAP-Berechtigungs-wesen	731
10.3.1	Das Dateneigentümerkonzept	732
10.3.2	Das Antrags-, Test- und Freigabeverfahren	734
10.3.3	Der Ablauf der Benutzerverwaltung	738
10.3.4	Konzept für übergreifende Berechtigungen	739
10.3.5	Das interne Kontrollsystem	739
10.3.6	Namenskonventionen für Rollen	741
10.3.7	Konventionen für die technische Rollenausprägung	742
10.3.8	Rollenkonzepte	743
10.3.9	Pflege von Kachelgruppen und -katalogen	744
10.3.10	Komponenten- und systemspezifische Teilkonzepte	745
10.3.11	Berechtigungen in Eigenentwicklungen	745
10.3.12	Sicherheitskonzept zum Berechtigungskonzept	746
10.3.13	Checkliste	747
10.4	Customizing zum Berechtigungskonzept	750
10.4.1	Systemparameter	750
10.4.2	Benutzermenüs	753
10.4.3	Customizing-Schalter in Tabelle PRGN_CUST	755
10.4.4	Deaktivierte Berechtigungsobjekte	757
10.4.5	Deaktivierung von einzelnen Berechtigungsprüfungen	759
10.4.6	Transaktionsaufrufe durch CALL TRANSACTION	761
10.4.7	Zugriffsrechte	763
10.4.8	Checkliste	766
10.5	Prüfung von Zugriffsrechten	768
10.5.1	Referenzbenutzer	769
10.5.2	Kritische Standardprofile	769
10.5.3	Berechtigungsobjekte zu startbaren Anwendungen suchen	774
10.5.4	Zugriffsrechte für Benutzer auswerten	775
10.5.5	Zugriffsrechte für Rollen auswerten	782
10.5.6	Patterns in SAP Enterprise Threat Detection	786
10.6	Trace von Benutzerberechtigungen	787
10.6.1	Transaktion SU53	787
10.6.2	Der Berechtigungs-Trace	788

10.6.3	Der Benutzer-Langzeit-Trace	790
10.6.4	Übernahme von Trace-Ergebnissen in eine Rolle	792
10.7	Berechtigungen für Prüfer	794
11	Praktische Prüfung von Berechtigungen	797
11.1	Zugriffsrechte im Bereich der Berechtigungsverwaltung	797
11.1.1	Zugriffsrechte zur Benutzerverwaltung	798
11.1.2	Zugriffsrechte zur Rollenverwaltung	803
11.1.3	Zugriffsrechte zu Profilen	804
11.1.4	Zugriffsrechte für Kachelkataloge und -gruppen	805
11.2	Gesetzeskritische Berechtigungen	805
11.3	Kritische Basisberechtigungen	808
11.3.1	Löschen von Sperreinträgen anderer Benutzer	808
11.3.2	Administration der Sperrverwaltung	808
11.3.3	LDAP-Zugriffe	809
11.3.4	Verwaltung der Ein- und Ausgabe-Queue	809
11.3.5	Administration der Datenarchivierung	810
11.3.6	Löschen von laufenden Prozessen	810
11.3.7	Verwaltung der TemSe-Dateien	811
11.3.8	Anlegen von Jobs unter anderem Benutzernamen	811
11.3.9	Verwaltung der Hintergrundjobs	812
11.3.10	Zurücksetzen und Löschen von Daten ohne Archivierung	812
11.3.11	Kopieren von Dateien vom SAP-Server auf den Client	813
11.3.12	Kopieren von Dateien vom Client auf den SAP-Server	814
11.4	Berechtigungen für das Hacking von SAP-Systemen	815
11.4.1	Datendiebstahl	815
11.4.2	Datenmanipulation	816
11.4.3	Password-Cracking	818
11.4.4	Verschleierung von Aktionen	820
11.4.5	Code-Insert	821
11.5	Customizing-Berechtigungen	824
11.5.1	Transaktionen zur Tabellen- und Viewpflege	824
11.5.2	Customizing im Finanzwesen	826
11.5.3	Customizing in der Materialwirtschaft	834
11.5.4	Customizing in SAP ERP HCM	836

11.6	Analyse der Qualität des Berechtigungskonzepts	838
11.6.1	Manuelle Berechtigungen	839
11.6.2	Manuell gepflegte Organisationsebenen	841
11.6.3	Offene Organisationsebenen in Rollen	844
11.6.4	Offene Berechtigungen in Rollen	845
11.6.5	Sternberechtigungen in Berechtigungswerten	846
11.6.6	Fehlende Pflege der Berechtigungen in Transaktion SU24 für kundeneigene Transaktionen	847
11.6.7	Quantitative Auswertungen zu Rollen und Rollenzuordnungen	848
11.7	Analyse von Berechtigungen in SAP Business Warehouse	850
11.7.1	Administrative Berechtigungen	850
11.7.2	Berechtigungen für PSA-Tabellen	853
11.7.3	Testen der Berechtigungen anderer Benutzer	855
11.7.4	Berechtigungen zur Datenmodellierung	856
11.7.5	Verwaltung von Analyseberechtigungen	860
11.7.6	Reportingberechtigungen	863
12	SAP HANA	867
12.1	Einführung in SAP HANA	867
12.1.1	Der Systemtyp einer SAP-HANA-Datenbank	868
12.1.2	Schemata	868
12.1.3	Zugriff auf Daten in der SAP-HANA-Datenbank	870
12.1.4	Entwicklungsumgebung SAP HANA XS (Repository)	873
12.1.5	Entwicklungsumgebung SAP HANA XSA	874
12.1.6	Aufruf von Tabellen und Views	875
12.1.7	Zugriff auf Daten in der SAP-HANA-Datenbank	875
12.2	Systemsicherheit in SAP HANA	876
12.2.1	Tenant-Datenbanken	876
12.2.2	Systemparameter	878
12.2.3	Verschlüsselung von Daten	882
12.2.4	Verschlüsselung der Kommunikation	885
12.2.5	Verbindungen zu anderen Systemen – Remote Sources	886
12.2.6	Checkliste	888
12.3	Anmeldesicherheit	891
12.3.1	Authentifizierungsmethoden	891
12.3.2	Systemparameter für Kennwortrichtlinien	892
12.3.3	Benutzergruppenspezifische Kennwortrichtlinien	895

12.3.4	Liste der verbotenen Kennwörter	896
12.3.5	Checkliste	897
12.4	Benutzerverwaltung in SAP HANA	898
12.4.1	Der Benutzerstammsatz	898
12.4.2	Restricted User (Eingeschränkte Benutzer)	901
12.4.3	Standardbenutzer in SAP HANA	903
12.4.4	Remotebenutzer	907
12.4.5	Benutzergruppen	909
12.4.6	Checkliste	910
12.5	SAP HANA XSA	912
12.5.1	Struktur in SAP HANA XSA	913
12.5.2	SAP HANA XSA Cockpit	914
12.5.3	SAP Web IDE	914
12.5.4	Benutzer in SAP HANA XSA	915
12.5.5	Berechtigungen in SAP HANA XSA	917
12.5.6	Checkliste	923
12.6	Das Berechtigungskonzept von SAP HANA	924
12.6.1	Berechtigungen in SAP HANA	924
12.6.2	System Privileges (Systemberechtigungen)	925
12.6.3	Object Privileges (Objektberechtigungen)	928
12.6.4	Package Privileges (Paketberechtigungen)	930
12.6.5	Analytic Privileges (Analyseberechtigungen)	933
12.6.6	Application Privileges (Anwendungsberechtigungen)	934
12.6.7	Privileges on Users (Debugging des eigenen Benutzers zulassen)	935
12.6.8	Weitergabe von Berechtigungen	936
12.6.9	Checkliste	937
12.7	Das Rollenkonzept von SAP HANA	939
12.7.1	Eigenschaften von Rollen	939
12.7.2	Runtime-Katalogrollen	941
12.7.3	Design-Time-Repository-Rollen in SAP HANA XS	942
12.7.4	Design-Time-HDI-Rollen in SAP HANA XSA	945
12.7.5	Standardrollen in SAP HANA	945
12.7.6	Checkliste	948
12.8	Analyse des SAP-HANA-Berechtigungskonzepts	950
12.8.1	Tabellen und Views zur Analyse von Berechtigungen	951
12.8.2	Benutzerauswertungen	951
12.8.3	Welche Berechtigungen haben einzelne Benutzer (View EFFECTIVE_PRIVILEGES)?	954
12.8.4	Welchen Benutzern und Rollen sind bestimmte Berechtigungen zugeordnet (View EFFECTIVE_PRIVILEGE_GRANTEES)?	956

12.8.5	Welche Rollen sind einem Benutzer oder einer Rolle zugeordnet (View EFFECTIVE_ROLES)?	958
12.8.6	Welchen Benutzern und Rollen sind bestimmte Rollen zugeordnet (View EFFECTIVE_ROLE_GRANTEES)?	959
12.8.7	Das Skript HANA_Security_GrantedRolesAndPrivileges	960
12.8.8	Checkliste	962
12.9	Auditing in SAP HANA	963
12.9.1	Konfiguration des Auditings in SAP HANA	963
12.9.2	Einrichten von Policies	966
12.9.3	Auswertung der eingerichteten Policies	971
12.9.4	Auswertung des Auditings	972
12.9.5	Löschen von Auditing-Protokollen	975
12.9.6	Konzept zur Auswertung	975
12.9.7	Checkliste	975

Anhang

979

A	Leitfäden zur SAP-Systemsicherheit	979
B	Glossar	981

Der Autor	989
Index	991