

Inhalt

Einleitung	23
------------------	----

1 Umgang mit dem SAP-System und Werkzeuge zur Prüfung 29

1.1 Transaktionen	29
1.2 Reports	31
1.2.1 Das Konzept der Reports	31
1.2.2 Aufrufen von Reports	33
1.2.3 Exportieren der Reportergebnisse	36
1.2.4 Festlegung des Standardpfads zum Speichern	37
1.2.5 Speichern der Selektionsangaben (Varianten)	38
1.3 Anzeigen von Tabellen	39
1.3.1 Anzeigetranaktionen für Tabellen	39
1.3.2 Transaktion SE16	41
1.3.3 Transaktion SE16N	42
1.3.4 Transaktion SE16H	43
1.3.5 Transaktion SE16S	46
1.3.6 Suchen von Tabellen	48
1.3.7 Exportieren von Tabellen	51
1.3.8 Speichern der Selektionsangaben (Varianten)	51
1.4 Das Benutzerinformationssystem	52
1.5 Listen als PDF-Datei speichern	55
1.6 Nutzung der Zugriffsstatistik für Prüfungen	57
1.6.1 Funktionsweise	57
1.6.2 Analyse von aufgerufenen Transaktionen und Reports	59
1.6.3 Analyse von RFC-Aufrufen	61
1.7 Tabelleninhalte mit dem QuickViewer auswerten	64
1.7.1 Erstellen eines QuickViews auf eine einzelne Tabelle	65
1.7.2 Erstellen eines QuickViews mit einem Tabellen-Join	68
1.7.3 Erstellen eines QuickViews mit einer logischen Datenbank	70
1.8 SQL Trace	72
1.8.1 Aktivierung des SQL Trace	73

1.8.2	Auswertung des Trace	74
1.9	Audit Information System	76
1.9.1	Die Audit-Struktur	76
1.9.2	Durchführen eines Audits	78
1.9.3	Berechtigungen zur Nutzung des Audit Information Systems	80
1.10	SAP Access Control	81
1.10.1	Komponenten von SAP Access Control	81
1.10.2	Regelwerke	83
1.10.3	Auswertung der Regelwerke	87
1.10.4	SAP-Access-Control-Regelwerk für dieses Buch	93
1.11	SAP Enterprise Threat Detection	94
1.11.1	Angriffe auf SAP-Systeme – nur etwas für versierte Hacker?	95
1.11.2	Standardüberwachung von SAP-Systemen	96
1.11.3	Zentrale Sammlung von Protokollen in SAP Enterprise Threat Detection	98
1.11.4	Automatisierte Analyse von Protokollen in SAP Enterprise Threat Detection	99
1.12	Zugriff auf SAP HANA für Prüfer	103
1.12.1	Zugriff auf SAP HANA über das DBA Cockpit	103
1.12.2	Zugriff auf SAP HANA über das SAP HANA Studio	107
1.12.3	Skriptgesteuerter Export von Daten aus der SAP-HANA-Datenbank	110

2 Aufbau von SAP-Systemen und Systemlandschaften 113

2.1	SAP NetWeaver und SAP-Komponenten	113
2.1.1	Komponenten von SAP NetWeaver	114
2.1.2	Die SAP Business Suite	115
2.1.3	SAP S/4HANA	116
2.1.4	Checkliste	117
2.2	Der technische Aufbau eines SAP-Systems	117
2.2.1	Applikations- und Datenbankserver	118
2.2.2	Instanzen	118

2.2.3	SAP-Prozesse und -Dienste	119
2.2.4	Checkliste	123
2.3	Systemlandschaften	123
2.3.1	Drei-System-Landschaften	124
2.3.2	Systemarten	126
2.3.3	Checkliste	127
2.4	Das Mandantenkonzept	128
2.4.1	Standardmandanten eines SAP-Systems	128
2.4.2	Eigenschaften von Mandanten	129
2.4.3	Protokollierung der Änderungen von Mandanteneigenschaften	133
2.4.4	Risiko beim Anlegen neuer Mandanten	134
2.4.5	Mandantenkopien	135
2.4.6	Zugriffsrechte	139
2.4.7	Checkliste	143
2.5	Sicherheit im Mandanten 000	144
2.5.1	Zugriff auf Daten des Produktivmandanten	144
2.5.2	Systemeinstellungen pflegen	151
2.5.3	Gesetzeskritische Berechtigungen	152
2.5.4	Patterns in SAP Enterprise Threat Detection	152
2.5.5	Checkliste	153

3 Allgemeine Systemsicherheit 155

3.1	Grundlagen für die Prüfung der Systemsicherheit	155
3.1.1	Der Releasestand des SAP-Systems	156
3.1.2	Systemparameter	156
3.1.3	Checkliste	161
3.2	Anmeldesicherheit	163
3.2.1	Unzulässige Kennwörter – Tabelle USR40	164
3.2.2	Protokolle von Mehrfachanmeldungen	165
3.2.3	Systemparameter zur Anmeldesicherheit	166
3.2.4	Sicherheitsrichtlinien	175
3.2.5	Schutz vor Kennwort-Hacking	179
3.2.6	Unternehmenseigene Erweiterungen zur Anmeldesicherheit	181

3.2.7	Patterns in SAP Enterprise Threat Detection	181
3.2.8	Zugriffsrechte	182
3.2.9	Checkliste	185
3.3	Das Notfallbenutzerkonzept	187
3.4	Sperren von Transaktionscodes	189
3.4.1	Sperren bis einschließlich SAP NetWeaver 7.40	189
3.4.2	Sperren ab SAP NetWeaver 7.50	190
3.4.3	Zugriffsrechte	191
3.4.4	Checkliste	192
3.5	Logische Betriebssystemkommandos	193
3.5.1	Funktionsweise	193
3.5.2	Der Report RSBDCOS0	197
3.5.3	Logische Betriebssystemkommandos zur Prüfung nutzen	198
3.5.4	Patterns in SAP Enterprise Threat Detection	199
3.5.5	Zugriffsrechte	200
3.5.6	Checkliste	201
3.6	Drucken und Speichern	202
3.6.1	Der Druckvorgang	202
3.6.2	Schutz von Druckaufträgen	207
3.6.3	Speichern von Daten in Dateien	208
3.6.4	Patterns in SAP Enterprise Threat Detection	208
3.6.5	Zugriffsrechte	209
3.6.6	Checkliste	210
3.7	Batch Input	212
3.7.1	Analyse des Batch-Input-Verfahrens	213
3.7.2	Berechtigungen für Batch-Input-Mappen	216
3.7.3	Zugriffsrechte	217
3.7.4	Checkliste	218
3.8	Funktionen von SAP Business Warehouse	220
3.8.1	Datenextraktion	220
3.8.2	Der Extraktorchecker	221
3.8.3	Berechtigungen für die Extraktion einschränken	223
3.8.4	Zugriffsrechte	224
3.8.5	Checkliste	225

4.1	Security Audit Log	227
4.1.1	Konfiguration des Security Audit Logs	229
4.1.2	Auswertung des Security Audit Logs	235
4.1.3	Löschen von Security-Audit-Log-Protokollen	236
4.1.4	Konzept zum Einsatz des Security Audit Logs	237
4.1.5	Zugriffsrechte	241
4.1.6	Checkliste	244
4.2	Systemprotokollierung	245
4.2.1	Auswertung des SysLogs	246
4.2.2	Meldungen des SysLogs	248
4.2.3	Zugriffsrechte	251
4.2.4	Checkliste	251
4.3	Protokollierung von Tabellenänderungen	252
4.3.1	Aktivierung der Tabellenprotokollierung	253
4.3.2	Protokollierung bei Transporten	255
4.3.3	Protokollierung der einzelnen Tabellen	256
4.3.4	Versionierung der Protokolleigenschaft von Tabellen	260
4.3.5	Protokollierung unternehmenseigener Tabellen	262
4.3.6	Auswertung von Tabellenänderungen	265
4.3.7	Löschen von Tabellenänderungsprotokollen	269
4.3.8	Zugriffsrechte	270
4.3.9	Checkliste	272
4.4	Protokollierung über Änderungsbelege	274
4.4.1	Suchen von über Änderungsbelege protokollierten Tabellen	276
4.4.2	Auswertung der Änderungsbelege	277
4.4.3	Löschen von Änderungsbelegen	278
4.4.4	Ändern von Änderungsbelegobjekten	278
4.4.5	Zugriffsrechte	279
4.4.6	Checkliste	280
4.5	Versionsverwaltung	280
4.5.1	Anzeige der Versionen zu einzelnen Programmen	281
4.5.2	Anzeige der Versionen aller versionierbaren Objekte	283
4.5.3	Versionserzeugung bei Importen	284
4.5.4	Löschen der Versionshistorien	285
4.5.5	Checkliste	286

4.6	Lesezugriffsprotokollierung	287
4.6.1	Protokollierung des Zugriffs auf sensible Felder	288
4.6.2	Protokollierung des Aufrufs von Funktionsbausteinen	291
4.6.3	Konfigurationseinstellungen	293
4.6.4	Verwaltungsprotokoll	293
4.6.5	Zugriffsrechte	294
4.6.6	Checkliste	297
4.7	Zugriffsstatistik	298
4.7.1	Analyse einzelner Benutzer oder Funktionen	300
4.7.2	Analyse von Transaktionsaufrufen in Listenform	301
4.7.3	Analyse von RFC-Zugriffen	301
4.7.4	Langzeitauswertung der Statistik	303
4.7.5	Anonymisierte Auswertung von Statistiksätzen	306
4.7.6	Zugriffsrechte	307
4.7.7	Checkliste	308
4.8	Weitere Protokollkomponenten	309
4.8.1	Protokolle für die Systemänderbarkeit	309
4.8.2	Protokolle von Mandantenkopien	310
4.8.3	Protokolle von Änderungen an Systemparametern	311
4.8.4	Protokolle von Mehrfachanmeldungen	312
4.8.5	Protokolle von Änderungen an Betriebssystem- kommandos	312
4.8.6	Jobprotokolle	312
4.8.7	Protokolle von Änderungen über Transaktion SE16N	313
4.8.8	Protokolle von Änderungen an Sicherheitsrichtlinien	314
4.9	Systemüberwachung mit SAP Enterprise Threat Detection	314
4.9.1	Übertragung der Protokolle an SAP Enterprise Threat Detection	314
4.9.2	Auswahl der Patterns in SAP Enterprise Threat Detection	316
4.9.3	Definition eigener Patterns	318
4.9.4	Analyse mit SAP Enterprise Threat Detection	318
4.9.5	Zugriffsrechte	322
4.9.6	Checkliste	325

5 Remote Function Calls 327

5.1	Funktionsbausteine	327
5.1.1	Funktionsbausteine ohne Berechtigungsprüfungen	331

5.1.2	Funktionsbausteine mit schaltbaren Berechtigungen	332
5.1.3	Protokollierung von RFC-Aktionen	333
5.1.4	Patterns in SAP Enterprise Threat Detection	335
5.1.5	Zugriffsrechte	336
5.1.6	Checkliste	337
5.2	RFC-Verbindungen	338
5.2.1	Hinterlegte Kennwörter	340
5.2.2	Systemübergreifender Zugriff über Funktions- bausteine	342
5.2.3	Zugriffsrechte	343
5.2.4	Checkliste	344
5.3	Trusted Systems	345
5.3.1	Berechtigungen zur Nutzung von Trusted- Verbindungen	349
5.3.2	Zugriffsrechte	350
5.3.3	Checkliste	352
5.4	Zugriff von externen Programmen	353
5.4.1	Ermittlung der erforderlichen RFC-Berechtigungen	356
5.4.2	Zugriff auf das SAP-System über Microsoft Excel	357
5.4.3	ABAP-Quelltexte über RFC ausführen	359
5.4.4	Zugriffsrechte	361
5.4.5	Checkliste	362

6 Der Verbuchungsvorgang 365

6.1	Das Prinzip der Verbuchung	365
6.1.1	Die Verbuchungskomponenten	367
6.1.2	Auswertung der Verbuchung	368
6.1.3	Zugriffsrechte	373
6.1.4	Checkliste	373
6.2	Abgebrochene Buchungen	374
6.2.1	Kontrolle auf abgebrochene Buchungen	375
6.2.2	Die Abstimmanalyse der Finanzbuchhaltung	375
6.2.3	Zugriffsrechte	378
6.2.4	Checkliste	379
6.3	Die Belegnummernvergabe	380
6.3.1	Nummernkreisobjekte	380
6.3.2	Pufferung von Belegnummern	382

6.3.3	Suche nach Lücken in Belegnummern	384
6.3.4	Zugriffsrechte	385
6.3.5	Checkliste	386

7 Benutzerauswertungen 389

7.1	Organisatorische Regelungen	389
7.2	Die SAP-Standardbenutzer	393
7.2.1	Der Benutzer SAP*	393
7.2.2	Der Benutzer DDIC	394
7.2.3	Der Benutzer SAPCPIC	394
7.2.4	Der Benutzer TMSADM	395
7.2.5	Der Benutzer EARLYWATCH	395
7.2.6	Prüfen der Standardbenutzer	396
7.2.7	Weitere Standardbenutzer	397
7.2.8	Patterns in SAP Enterprise Threat Detection	398
7.2.9	Zugriffsrechte	398
7.2.10	Checkliste	400
7.3	Der Benutzerstammsatz	402
7.3.1	Benutzereigenschaften	402
7.3.2	Die Tabellen des Benutzerstammsatzes	405
7.3.3	Benutzerauswertungen mit dem Benutzerinformationssystem	410
7.3.4	Patterns in SAP Enterprise Threat Detection	411
7.3.5	Zugriffsrechte	411
7.3.6	Checkliste	412
7.4	Referenzbenutzer	413
7.4.1	Patterns in SAP Enterprise Threat Detection	415
7.4.2	Zugriffsrechte	416
7.4.3	Checkliste	417
7.5	Benutzergruppen	419
7.5.1	Patterns in SAP Enterprise Threat Detection	422
7.5.2	Zugriffsrechte	422
7.5.3	Checkliste	423
7.6	Sammelbenutzer	424
7.7	Benutzervermessungsdaten	427
7.7.1	Prüfen der Systemvermessung	430

7.7.2	Zugriffsrechte	431
7.7.3	Checkliste	432
7.8	Initialkennwörter und Benutzersperren	433
7.8.1	Produktivkennwörter	435
7.8.2	Benutzersperren	436
7.8.3	Auswertung gesperrter Benutzer	439
7.8.4	Patterns in SAP Enterprise Threat Detection	440
7.8.5	Zugriffsrechte	440
7.8.6	Checkliste	443
7.9	Kennwortverschlüsselung	444
7.9.1	Verschlüsselungsalgorithmen	444
7.9.2	Schutz vor Hacking der Kennwörter	446
7.9.3	Patterns in SAP Enterprise Threat Detection	446
7.9.4	Zugriffsrechte	447
7.9.5	Checkliste	449
7.10	Angemeldete Benutzer	450
7.10.1	Patterns in SAP Enterprise Threat Detection	452
7.10.2	Zugriffsrechte	453
7.10.3	Checkliste	453
7.11	Die Änderungshistorie zu Benutzern	454
7.11.1	Zugriffsrechte	456
7.11.2	Checkliste	457

8 Customizing des SAP-Systems 459

8.1	Das ABAP Dictionary	459
8.1.1	Aufbau des ABAP Dictionarys	460
8.1.2	Domänen	462
8.1.3	Datenelemente	466
8.1.4	Zugriffsrechte	467
8.1.5	Checkliste	468
8.2	Das Konzept der Tabellensteuerung	469
8.2.1	Eigenschaften von Tabellen	469
8.2.2	Mandantenabhängige Tabellen	472
8.2.3	Mandantenunabhängige Tabellen	473
8.2.4	Transparente Tabellen	475
8.2.5	Dokumentationen zu Tabellen	475

8.2.6	Views	476
8.2.7	Unternehmenseigene Tabellen und Views	480
8.2.8	Zugriffsrechte	481
8.2.9	Checkliste	482
8.3	Zugriffe auf Tabellen	483
8.3.1	Anzeige von Tabelleninhalten in der Datenbank	483
8.3.2	Ändern von Tabellen im SAP-System	484
8.3.3	Einführungsleitfaden	485
8.3.4	Laufende Einstellungen	488
8.3.5	Patterns in SAP Enterprise Threat Detection	489
8.3.6	Zugriffsrechte	490
8.3.7	Checkliste	491
8.4	Berechtigungen für Tabellen und Views	492
8.4.1	Berechtigungsgruppen	493
8.4.2	Berechtigungsobjekte	494
8.4.3	Schutz von Tabellen ohne Berechtigungsgruppe	499
8.4.4	Prüfen der Berechtigungen zum Zugriff auf einzelne Tabellen/Views	500
8.4.5	Prüfung der Tabellenberechtigungen für einzelne Rollen oder Benutzer	502
8.4.6	Abgleich von Tabellenberechtigungsgruppen	503
8.4.7	Zugriffsrechte	503
8.4.8	Checkliste	506
8.5	Die Tabellenpufferung	507
8.5.1	Tabellenpufferungsarten	508
8.5.2	Welche Tabellen werden gepuffert?	511
8.5.3	Puffersynchronisation	512

9 Entwicklung in SAP-Systemen 515

9.1	Entwicklerrichtlinien	515
9.2	Entwickler- und Objektschlüssel	518
9.2.1	Entwicklerschlüssel	518
9.2.2	Objektschlüssel	521
9.2.3	Umgehung der Abfrage von Entwickler- und Objektschlüsseln	522
9.2.4	Entwickler- und Objektschlüssel in SAP S/4HANA	523

9.2.5	Zugriffsrechte	524
9.2.6	Checkliste	525
9.3	Systemänderbarkeit	526
9.3.1	Prüfung der Systemänderbarkeit	527
9.3.2	Zugriffsrechte	530
9.3.3	Checkliste	531
9.4	Das Transportsystem	532
9.4.1	Der Transport Organizer	532
9.4.2	Transport Management System	540
9.4.3	Der Ablauf eines Transports	546
9.4.4	Zeitnähe der Importe	548
9.4.5	Zugriffsrechte	550
9.4.6	Checkliste	555
9.5	Eigenentwicklungen in ABAP	557
9.5.1	Die Programmiersprache ABAP	558
9.5.2	ABAP-Namensräume	562
9.5.3	Gefahrenpunkte in der ABAP-Programmentwicklung	563
9.5.4	Prüfen der Eigenschaften von ABAP-Programmen	581
9.5.5	Inhaltliches Prüfen einzelner ABAP-Programme	582
9.5.6	Programmübergreifende Analyse von Quelltexten	583
9.5.7	Code Inspector	589
9.5.8	Code Vulnerability Analyzer	592
9.5.9	Die Versionshistorie	594
9.5.10	Patterns in SAP Enterprise Threat Detection	594
9.5.11	Checkliste	594
9.6	Transaktionen	596
9.6.1	Zugriffsrechte	600
9.6.2	Checkliste	600
9.7	Berechtigungen zur Anwendungsentwicklung	601
9.7.1	Das Berechtigungsobjekt S_DEVELOP	602
9.7.2	Schutz von ABAP-Programmen durch Berechtigungsgruppen (S_PROGRAM)	604
9.7.3	Schutz von ABAP-Programmen nach Namen (S_PROGNAM)	607
9.7.4	Zugriffsrechte – Einzelberechtigungen	608
9.7.5	Zugriffsrechte – Funktionstrennungen	610
9.7.6	Patterns in SAP Enterprise Threat Detection	612

10.1 Funktionsweise des Berechtigungskonzepts	614
10.1.1 Berechtigungsobjekte	615
10.1.2 Rollen	619
10.1.3 Sammelrollen	625
10.1.4 Profile	627
10.1.5 Berechtigungen	630
10.1.6 Ablauf einer Berechtigungsprüfung	632
10.1.7 Patterns in SAP Enterprise Threat Detection	633
10.1.8 Checkliste	633
10.2 Konzepte zum SAP-Berechtigungswesen	634
10.2.1 Das Dateneigentümerkonzept	635
10.2.2 Das Antrags-, Test- und Freigabeverfahren	637
10.2.3 Der Ablauf der Benutzerverwaltung	641
10.2.4 Konzept für übergreifende Berechtigungen	642
10.2.5 Das interne Kontrollsystem	642
10.2.6 Namenskonventionen für Rollen	644
10.2.7 Konventionen für die technische Rollenausprägung	645
10.2.8 Rollenkonzepte	646
10.2.9 Komponenten- und systemspezifische Teilkonzepte	647
10.2.10 Berechtigungen in Eigenentwicklungen	648
10.2.11 Sicherheitskonzept zum Berechtigungskonzept	648
10.2.12 Checkliste	650
10.3 Customizing zum Berechtigungskonzept	652
10.3.1 Systemparameter	652
10.3.2 Benutzermenüs	655
10.3.3 Customizing-Schalter in Tabelle PRGN_CUST	658
10.3.4 Deaktivierte Berechtigungsobjekte	660
10.3.5 Deaktivierung von einzelnen Berechtigungsprüfungen ...	661
10.3.6 Transaktionsaufrufe durch CALL TRANSACTION	663
10.3.7 Zugriffsrechte	665
10.3.8 Checkliste	668
10.4 Prüfung von Zugriffsrechten	670
10.4.1 Referenzbenutzer	671
10.4.2 Kritische Standardprofile	672
10.4.3 Zugriffsrechte für Benutzer auswerten	675
10.4.4 Zugriffsrechte für Rollen auswerten	680
10.4.5 Patterns in SAP Enterprise Threat Detection	682

10.5	Trace von Benutzerberechtigungen	682
10.5.1	Transaktion SU53	682
10.5.2	Der Berechtigungs-Trace	683
10.5.3	Der Benutzer-Langzeit-Trace	685
10.5.4	Übernahme von Trace-Ergebnissen in eine Rolle	687
10.6	Berechtigungen für Prüfer	688

11 Praktische Prüfung von Berechtigungen 691

11.1	Zugriffsrechte im Bereich der Berechtigungsverwaltung	691
11.1.1	Zugriffsrechte zur Benutzerverwaltung	692
11.1.2	Zugriffsrechte zur Rollenverwaltung	697
11.1.3	Zugriffsrechte zu Profilen	698
11.2	Gesetzeskritische Berechtigungen	698
11.3	Kritische Basisberechtigungen	700
11.3.1	Löschen von Sperreinträgen anderer Benutzer	701
11.3.2	Administration der Sperrverwaltung	701
11.3.3	LDAP-Zugriffe	701
11.3.4	Verwaltung der Ein- und Ausgabe-Queue	702
11.3.5	Administration der Datenarchivierung	702
11.3.6	Laufende Prozesse löschen	703
11.3.7	Verwaltung der TemSe-Dateien	703
11.3.8	Anlegen von Jobs unter anderem Benutzernamen	704
11.3.9	Verwaltung der Hintergrundjobs	704
11.3.10	Daten ohne Archivierung zurücksetzen und löschen	705
11.3.11	Dateien von SAP-Server auf Client kopieren	705
11.3.12	Dateien von Client auf SAP-Server kopieren	706
11.3.13	Nutzung von Transaktion PFCG_EASY	707
11.4	Customizing-Berechtigungen	708
11.4.1	Transaktionen zur Tabellen- und View-Pflege	708
11.4.2	Customizing im Finanzwesen	710
11.4.3	Customizing in der Materialwirtschaft	717
11.4.4	Customizing in SAP ERP HCM	720
11.5	Analyse der Qualität des Berechtigungskonzepts	722
11.5.1	Manuelle Berechtigungen	722
11.5.2	Manuell gepflegte Organisationsebenen	724
11.5.3	Offene Organisationsebenen in Rollen	727
11.5.4	Offene Berechtigungen in Rollen	728

11.5.5	Sternberechtigungen in Berechtigungswerten	729
11.5.6	Fehlende Pflege der Berechtigungen in Transaktion SU24 für kundeneigene Transaktionen	730
11.5.7	Quantitative Auswertungen zu Rollen und Rollenzuordnungen	731
11.6	Analyse von Berechtigungen in SAP Business Warehouse	733
11.6.1	Administrative Berechtigungen	733
11.6.2	Berechtigungen für PSA-Tabellen	736
11.6.3	Testen der Berechtigungen anderer Benutzer	738
11.6.4	Berechtigungen zur Datenmodellierung	739
11.6.5	Verwaltung von Analyseberechtigungen	743
11.6.6	Reporting-Berechtigungen	746

12 SAP HANA 751

12.1	Aufbau eines SAP-HANA-Systems	751
12.1.1	Zugriff auf Daten in der SAP-HANA-Datenbank	753
12.1.2	Die Entwicklungsumgebung	756
12.2	Sicherheit auf Unix-Ebene	759
12.2.1	Unix-Standardbenutzer	759
12.2.2	Sperren von Benutzeranmeldungen unter Unix	761
12.2.3	Berechtigungen auf Betriebssystemebene	762
12.2.4	Checkliste	763
12.3	SAP-HANA-Systemsicherheit	764
12.3.1	Multitenant-Datenbanken	764
12.3.2	Systemparameter	767
12.3.3	Secure Store in the File System (SSFS)	769
12.3.4	Datenverschlüsselung	771
12.3.5	Verschlüsselung der Kommunikation	773
12.3.6	Checkliste	775
12.4	Die Anmeldesicherheit	777
12.4.1	Authentifizierung	777
12.4.2	Anmeldeparameter	779
12.4.3	Verbotene Kennwörter	782
12.4.4	Checkliste	783
12.5	Benutzerverwaltung	785
12.5.1	Benutzerkonten	785

12.5.2	Standardbenutzer in SAP HANA	789
12.5.3	Restricted Users	790
12.5.4	Checkliste	791
12.6	Berechtigungen in SAP HANA	792
12.6.1	System Privileges (Systemberechtigungen)	793
12.6.2	Object Privileges (Objektberechtigungen)	796
12.6.3	Package Privileges (Paketberechtigungen)	798
12.6.4	Analytic Privileges (Analyseberechtigungen)	801
12.6.5	Application Privileges (Anwendungsberechtigungen)	802
12.6.6	Debugging-Berechtigungen für andere Benutzer	804
12.6.7	Zuordnung von Privileges zu Benutzern	804
12.6.8	Kritische Berechtigungen	805
12.6.9	Checkliste	807
12.7	Rollen in SAP HANA	808
12.7.1	Katalogrollen	808
12.7.2	Repository-Rollen	810
12.7.3	Versionierung von Repository-Rollen	812
12.7.4	Konzeptionelle Anforderungen an das Rollenkonzept	814
12.7.5	Checkliste	815
12.8	Prüfung des SAP-HANA-Berechtigungskonzepts	817
12.8.1	Prüfungen aus Benutzersicht	818
12.8.2	Prüfungen aus Berechtigungssicht	823
12.8.3	Prüfung kritischer Systemberechtigungen	827
12.8.4	Checkliste	831
12.9	Das Security Audit Log in SAP HANA	832
12.9.1	Einrichten von Policies	835
12.9.2	Prüfen der Konfiguration des Security Audit Logs	839
12.9.3	Auswertung des Security Audit Logs über die Datenbank	840
12.9.4	Auswertung des Auditings über das Unix-SysLog	842
12.9.5	Checkliste	844

Anhang 847

A	Leitfäden zur SAP-Systemsicherheit	849
B	Wichtige Systemparameter	851
C	Wichtige Transaktionen	859

D	Nützliche Reports	865
E	Wichtige Tabellen	871
F	Glossar	879
G	Der Autor	885
	Index	887