

Inhalt

Einleitung	21
1 Einführung in SAP HANA	25
1.1 Der technische Aufbau von SAP HANA	26
1.1.1 Zeilen- und spaltenorientierte Tabellen	26
1.1.2 Der Systemtyp einer SAP-HANA-Datenbank	28
1.1.3 Schemata	28
1.1.4 Zugriff auf Daten in der SAP-HANA-Datenbank	33
1.2 SAP HANA Cockpit	33
1.2.1 Database Groups	35
1.2.2 Benutzerverwaltung im SAP HANA Cockpit	36
1.2.3 Datenbanken ins SAP HANA Cockpit einbinden	39
1.2.4 Templates für die Systemkonfiguration	43
1.2.5 Verwaltung von SAP-HANA-Datenbanken	45
1.3 SAP HANA Database Explorer	50
1.3.1 Die Oberfläche des SAP HANA Database Explorers	51
1.3.2 Der SQL-Editor	52
1.3.3 Die SQL Statement Library	53
1.4 SAP HANA Web-based Development Workbench	57
1.4.1 Berechtigungen	57
1.4.2 Der Repository-Editor	58
1.4.3 Die Catalog-Verwaltung	59
1.4.4 Die Security-Sicht	60
1.4.5 Die Trace-Sicht	61
1.5 SAP HANA Studio	62
1.5.1 Die Oberfläche von SAP HANA Studio	62
1.5.2 Suche und Anzeige von Tabellen und Views	67
1.5.3 Anlegen neuer Remote Sources	68
1.5.4 Ausführen von SQL-Statements	69
1.5.5 Das Repository der SAP-HANA-Datenbank	70
1.6 hdbsql	73
1.6.1 Skript-gesteuerte Nutzung von »hdbsql«	76
1.6.2 Ausgabe von Befehlen in eine Textdatei	77

1.7	DBA Cockpit	77
1.8	SAP HANA XS Advanced	81
1.8.1	Struktur in SAP HANA XSA	81
1.8.2	SAP HANA XSA Advanced Cockpit	83
1.8.3	SAP WebIDE	84
1.9	SAP HANA und SAP ERP bzw. SAP S/4HANA	86
1.10	Leitfäden und SAP-Hinweise zur SAP-HANA-Sicherheit	90
1.10.1	SAP HANA Platform	90
1.10.2	SAP-Hinweise	92
2	Netzwerk- und Betriebssystemsicherheit	93
2.1	Absicherung der Unix-Benutzer	93
2.1.1	Speicherung der Unix-Benutzer	94
2.1.2	Benutzer »<sid>adm«	95
2.1.3	Benutzer »sapadm«	96
2.1.4	Benutzer des SAP HANA XS Advanced	96
2.1.5	Benutzer »root«	97
2.1.6	Gruppe »sapsys«	98
2.1.7	Sperren von Benutzeranmeldungen unter Unix	98
2.2	Schutz von Dateien und Verzeichnissen	99
2.2.1	Datei- und Verzeichnisrechte	99
2.2.2	Die Datei »bash_history«	100
2.2.3	Schutz von exportierten Dateien	102
2.3	Zugriff auf die Unix-Ebene vom ABAP-Stack aus	103
2.3.1	Funktionsweise	103
2.3.2	Der Report »RSBDCOS0«	106
2.3.3	Berechtigungen für Betriebssystemkommandos	107
2.4	Protokollierung von Aktionen unter Unix	108
3	Systemsicherheit in SAP HANA	111
3.1	Lizenzen verwalten	111
3.1.1	Auswertung der aktuellen Lizenzen	112
3.1.2	Lizenzen mit dem SAP HANA Cockpit verwalten	114

3.1.3	Lizenzen mit dem SAP HANA Studio verwalten	114
3.1.4	Protokollierung von Änderungen an Lizenzen	115
3.2	Systemparameter pflegen	116
3.2.1	Das Konzept der Systemparameter	116
3.2.2	Ändern der Parameter mit dem SAP HANA Cockpit	120
3.2.3	Parameterwerte vergleichen	123
3.2.4	Templates für das Setzen von Parameterwerten	126
3.2.5	Parameter mit dem SAP HANA Studio ändern	128
3.2.6	Parameter mit SQL-Statements ändern	130
3.2.7	Änderungshistorie von Parameteränderungen	131
3.3	Daten verschlüsseln	135
3.3.1	Secure Store in the File System (SSFS)	135
3.3.2	Berechtigungen zur Pflege der Einstellungen zur Verschlüsselung	138
3.3.3	Initiale Verschlüsselung bei Anlegen von Datenbanken	139
3.3.4	Verschlüsselung der persistenten Daten	140
3.3.5	Verschlüsselung der Redo-Logs	144
3.3.6	Verschlüsselung der Backups	145
3.3.7	Backup der Root Keys	147
3.3.8	Protokollierung von Änderungen an der Verschlüsselung	148
3.3.9	Client-Side Data Encryption	150
3.4	Kommunikation verschlüsseln	152
3.4.1	Analyse der Einstellungen zur Verschlüsselung	153
3.4.2	Mitlesen von Daten	154
3.5	Verbindungen zu anderen Systemen – Remote Sources	157
3.5.1	Eigenschaften von Remote Sources	157
3.5.2	Secondary Credentials	160
3.5.3	Berechtigungen für Remote Sources	160
3.5.4	Pflege von Remote Sources mit dem SAP HANA Database Explorer	162
3.5.5	Pflege von Remote Sources mit dem SAP HANA Studio	166
3.5.6	Pflege von Remote Sources mit der SAP HANA Web-based Development Workbench	168
3.5.7	Pflege von Remote Sources mittels SQL-Statements	168
3.5.8	Zugriff auf Daten in der Remote Source	169
3.5.9	Protokollierung von Remote Sources	170
3.6	Skripte zur Prüfung der Systemsicherheit	171
3.6.1	Das Skript HANA_Security_MiniChecks	172
3.6.2	Das Skript HANA_Configuration_MiniChecks	175

3.7	Alerts	178
3.7.1	Statistics Service	178
3.7.2	Sicherheitsrelevante Alarmmeldungen	179
3.7.3	Auswertung und Konfiguration von Alarmmeldungen mit dem SAP HANA Cockpit	182
3.7.4	Auswertung und Konfiguration von Alarmmeldungen mit dem SAP HANA Studio	184
3.7.5	Definition von Schwellwerten	185
3.7.6	Berechtigungen zur Auswertung von Alerts	186
4	Sicherheit in Multi-Tenant-Datenbanken	189
4.1	Das Konzept der Tenant-Datenbanken	189
4.1.1	Berechtigungen zur Verwaltung von Tenants	192
4.1.2	Verwaltung von Tenants mit dem SAP HANA Cockpit	193
4.1.3	Verwaltung von Tenants mit SAP HANA XSA	195
4.2	Tenant-übergreifende Zugriffe	197
4.3	Nicht änderbare Parameter in Tenants	198
4.4	Einschränkung von Funktionen in Tenants	199
4.5	High Isolation Level für Tenants	201
4.6	Protokollierung von Änderungen an Tenants	205
5	Authentifizierung in SAP HANA	207
5.1	Authentifizierungsmethoden	207
5.1.1	Konfiguration der möglichen Authentifizierungsmethoden	207
5.1.2	Kennwortbasierte Anmeldung	208
5.1.3	Anmeldung mittels Kerberos-Authentifizierung	209
5.1.4	Anmeldung mittels SAP Logon Ticket	210
5.1.5	Anmeldung mittels Security Assertion Markup Language (SAML)	210
5.1.6	Anmeldung mittels X.509-Zertifikat	211
5.1.7	Anmeldung mittels JSON Web Token	211
5.1.8	Anmeldung mittels LDAP	211
5.1.9	Authentifizierungsmethoden setzen mit dem SAP HANA Cockpit	212
5.1.10	Authentifizierungsmethoden setzen mit dem SAP HANA Studio	214

5.1.11	Authentifizierungsmethoden setzen mit der SAP HANA Web-based Development Workbench	215
5.1.12	Authentifizierungsmethoden setzen mit SQL-Statements	215
5.1.13	Auswertung der zugeordneten Authentifizierungsmethoden	217
5.1.14	Protokollierung der Authentifizierung	219
5.2	Kennwortrichtlinien	221
5.2.1	Systemparameter für Kennwortrichtlinien	221
5.2.2	Unterschiede der Standardwerte für Kennwörter in SAP HANA und SAP S/4HANA	228
5.2.3	Benutzergruppenspezifische Kennwortrichtlinien	229
5.2.4	Liste der verbotenen Kennwörter	230
5.2.5	Pflege der Richtlinien mit dem SAP HANA Cockpit	231
5.2.6	Pflege der Richtlinien mit dem SAP HANA Studio	232
5.2.7	Pflege der Richtlinien mit der SAP HANA Web-based Development Workbench	233
5.2.8	Pflege der Richtlinien mit SQL-Statements	233
5.2.9	Analyse der Kennwortrichtlinien	235
5.2.10	Protokollierung der Änderung an den Kennwortrichtlinien	236
6	Benutzerverwaltung in SAP HANA	239
6.1	Der Benutzerstammsatz	239
6.1.1	Eigenschaften eines Benutzerstammsatzes	240
6.1.2	Restricted User	244
6.1.3	Temporäre Sperrung aller Nicht-Admin-Benutzer	248
6.1.4	Berechtigungen	248
6.1.5	Benutzerpflege mit dem SAP HANA Cockpit	248
6.1.6	Benutzerpflege mit dem SAP HANA Studio	253
6.1.7	Benutzerpflege mit der SAP HANA Web-based Development Workbench	254
6.1.8	Benutzerpflege per SQL	255
6.1.9	Kopieren von Benutzern und Berechtigungen	259
6.1.10	Protokollierung der Benutzerverwaltung	263
6.2	SAP-HANA-XS-Advanced-Benutzer	264
6.2.1	Eigenschaften der SAP-HANA-XSA-Benutzer	264
6.2.2	Anlegen neuer Benutzer in SAP HANA XSA	267
6.2.3	Migrieren eines Datenbankbenutzers nach SAP HANA XSA	269
6.2.4	Protokollierung von Änderungen an SAP-HANA-XSA-Benutzern	271

6.3	SAP-HANA-Standardbenutzer	272
6.3.1	Der Benutzer »SYSTEM«	272
6.3.2	Systembenutzer	274
6.3.3	Benutzer des SAP HANA XS Advanced	275
6.3.4	Benutzer der SAP HANA Deployment Infrastructure (HDI)	276
6.3.5	Der Benutzer »SAP<sid>«	277
6.4	Remote-Benutzer	278
6.5	Benutzergruppen	282
6.5.1	Pflege von Benutzergruppen mit dem SAP HANA Cockpit	283
6.5.2	Pflege von Benutzergruppen mit SQL	286
6.5.3	Protokollierung von Benutzergruppen	289
7	Das Berechtigungskonzept von SAP HANA	291
7.1	Konzept der SAP-HANA-Berechtigungen	292
7.2	System Privileges	293
7.2.1	System Privileges kategorisieren	294
7.2.2	System Privileges zuordnen	303
7.3	Object Privileges	307
7.3.1	Object Privileges für Katalogobjekte	309
7.3.2	Object Privileges auf die Daten des SAP-ERP- bzw. SAP-S/4HANA-Systems	314
7.3.3	Object Privileges zuordnen	315
7.4	Package Privileges	320
7.4.1	Kritische Package Privileges	323
7.4.2	Package Privileges zuordnen	323
7.5	Analytic Privileges	325
7.6	Application Privileges	326
7.6.1	Application Privileges in Repository-Rollen	327
7.6.2	Application Privileges in Katalogrollen	328
7.6.3	Application Privileges Benutzern direkt zuordnen	329
7.6.4	Application Privileges über Prozeduren zuordnen	330
7.7	Berechtigungen weitergeben	331
7.8	Daten maskieren	333
7.9	Privileges on Users	335
7.10	Berechtigungen kopieren	335

7.11	Berechtigungsfehler analysieren	338
7.12	Trace von Berechtigungen	340
7.12.1	Die Trace-Konfiguration	340
7.12.2	Berechtigungs-Trace für alle Benutzer	341
7.12.3	Berechtigungs-Trace für einzelne Benutzer	342
7.12.4	Berechtigungs-Trace auswerten	343
7.12.5	Trace aktivieren und auswerten mit dem SAP HANA Cockpit	345
7.12.6	Trace aktivieren und auswerten mit dem SAP HANA Studio	348
7.12.7	Trace aktivieren und auswerten mit der SAP HANA Web-based Development Workbench	351
7.13	Berechtigungen in SAP HANA XS Advanced	352
7.13.1	Role Collections	353
7.13.2	Scopes und Attributes	356
7.13.3	Rollen-Templates und Rollen	357
7.13.4	Berechtigungen auf Organizations und Spaces	359
7.14	Berechtigungsverwaltung protokollieren	361
7.14.1	Zuordnung von Privileges in SAP HANA protokollieren	361
7.14.2	Zuordnung von SAP-HANA-XSA-Rollen protokollieren	362
7.14.3	Berechtigungsvergabe auf Organizations und Spaces in SAP HANA XSA protokollieren	362

8 Das Rollenkonzept von SAP HANA 363

8.1	Eigenschaften von Rollen	363
8.1.1	Rollen speichern	364
8.1.2	Namenskonventionen für Rollen	365
8.2	Runtime-Katalogrollen	368
8.2.1	Zugeordnete Rollen weitergeben	370
8.2.2	Katalogrollen mit dem SAP HANA Cockpit pflegen	371
8.2.3	Katalogrollen mit dem SAP HANA Studio pflegen	374
8.2.4	Katalogrollen mit der SAP HANA Web-based Development Workbench pflegen	376
8.2.5	Katalogrollen mit SQL pflegen	377
8.2.6	Katalogrollen protokollieren	379
8.3	Design-Time-Repository-Rollen (XSC)	379
8.3.1	Repository-Rollen mit dem SAP HANA Studio pflegen	380
8.3.2	Repository-Rollen mit der SAP HANA Web-based Development Workbench pflegen	388

8.3.3	Repository-Rollen mit dem SAP HANA Cockpit pflegen	390
8.3.4	Ausschluss von System Privileges in Repository-Rollen	391
8.3.5	Repository-Rollen Benutzern zuordnen	391
8.3.6	Repository-Rollen protokollieren	392
8.4	Design-Time-HDI-Rollen (XSA)	394
8.4.1	HDI-Container mit SAP WebIDE pflegen	394
8.4.2	HDI-Rollen in der WebIDE pflegen	396
8.4.3	HDI-Rollen Benutzern zuordnen	404
8.4.4	HDI-Rollen protokollieren	406
8.5	SAP-HANA-Standardrollen	406
8.5.1	Die Rolle »PUBLIC«	407
8.5.2	Die Rolle »SAP_INTERNAL_HANA_SUPPORT«	408
8.5.3	Die Rolle »DBA_COCKPIT«	409
8.5.4	Die Rolle »CONTENT_ADMIN«	409
8.5.5	Die Rolle »MODELING«	409
8.5.6	Die Rolle »MONITORING«	410
8.5.7	Rollenzuordnungen protokollieren	410

9 Das SAP-HANA-Berechtigungskonzept analysieren

411

9.1	Tabellen und Views zur Analyse von Berechtigungen	412
9.2	Analysen aus Benutzersicht	413
9.2.1	Wurden Berechtigungen direkt in den Benutzerstammsatz eingetragen?	413
9.2.2	Welche Rollen wurden den Benutzern zugeordnet?	415
9.2.3	Wurden Benutzern Repository-Rollen zugeordnet?	416
9.2.4	Welche Katalogrollen wurden Benutzern zugeordnet?	416
9.3	Analysen zum Rollenkonzept	418
9.4	Effektive Berechtigungen auswerten	421
9.4.1	Der View »ACCESSIBLE_VIEWS«	422
9.4.2	Der View »EFFECTIVE_PRIVILEGES«	423
9.4.3	Der View »EFFECTIVE_PRIVILEGE_GRANTEES«	425
9.4.4	Der View »EFFECTIVE_ROLES«	428
9.4.5	Der View »EFFECTIVE_ROLE_GRANTEES«	428
9.5	Das Skript »HANA_Security_GrantedRolesAndPrivileges«	429

9.6	Praktische Beispiele für Berechtigungsanalysen	431
9.6.1	Berechtigungen zur Benutzer- und Berechtigungsverwaltung	432
9.6.2	Berechtigungen zur Systemadministration	433
9.6.3	Berechtigungen zur Anwendungsentwicklung	435
9.6.4	Berechtigungen für Datenzugriffe	437
9.6.5	Funktionstrennungen	437
9.7	Automatisierte Analysen mit SAP GRC Access Control	439
9.7.1	Das Standardregelwerk von SAP GRC Access Control für SAP HANA	439
9.7.2	Das ECS-Regelwerk für SAP GRC Access Control	441
10	Auditing in SAP HANA	443
10.1	Auditing in SAP HANA konfigurieren	443
10.1.1	Systemparameter zur Auditing-Konfiguration	443
10.1.2	Konfiguration in Multi-Tenant-Systemen	448
10.1.3	Auditing-Konfiguration mit dem SAP HANA Cockpit pflegen	449
10.1.4	Auditing-Konfiguration mit dem SAP HANA Studio und der SAP HANA Web-based Development Workbench pflegen	451
10.1.5	Auditing-Konfiguration mit SQL pflegen	452
10.2	Policies einrichten	453
10.2.1	Eigenschaften von Policies	453
10.2.2	Beispiele für Policies	460
10.2.3	Automatisch protokollierte Aktionen	462
10.2.4	Policies mit dem SAP HANA Cockpit einrichten	463
10.2.5	Policies mit dem SAP HANA Studio und der SAP HANA Web-based Development Workbench einrichten	468
10.2.6	Policies mit SQL einrichten	470
10.2.7	Policies in der Systemdatenbank für Tenants einrichten	473
10.2.8	Policies in der Datenbank speichern	474
10.3	Auditing auswerten	476
10.3.1	Die Views »AUDIT_LOG« und »ALL_AUDIT_LOG«	476
10.3.2	Konzept zur Auswertung	479
10.3.3	Auditing mit dem SAP HANA Cockpit auswerten	480
10.3.4	Auditing mit SQL auswerten	483
10.3.5	Auswertung für einzelne Policies berechtigen	484
10.3.6	Auditing im Unix-SysLog auswerten	485
10.4	Auditing-Protokolle löschen	486

- 10.5 Auditing in SAP HANA XSA** 487
 - 10.5.1 Protokollierung im SAP HANA XSA Cockpit 488
 - 10.5.2 Zuweisung von Role Collections protokollieren 491
 - 10.5.3 Protokollierung in SAP-HANA-XSA-Anwendungen 492
- 10.6 SAP-Standard-Policies** 494
- 10.7 Best-Practice-Empfehlungen** 497
 - 10.7.1 Benutzer pflegen 498
 - 10.7.2 Anmeldeinformationen pflegen 499
 - 10.7.3 Katalog- und HDI-Rollen pflegen 500
 - 10.7.4 Rollen und Berechtigungen zuordnen 501
 - 10.7.5 Anmeldungen von Benutzern zu ungewöhnlichen Zeiten 501
 - 10.7.6 Systemparameter ändern 502
 - 10.7.7 Aktionen des Benutzers »SYSTEM« protokollieren 502
 - 10.7.8 Aktionen des Notfallbenutzers protokollieren 503
 - 10.7.9 DDL-Befehle im Produktivsystem ausführen 504
 - 10.7.10 Einstellung der Verschlüsselung ändern 504
 - 10.7.11 Einstellung der Clientside Encryption ändern 506
 - 10.7.12 Zertifikate und PSEs pflegen 506
 - 10.7.13 Neue Systeme zur Authentifizierung anschließen 507
 - 10.7.14 Lizenzen einspielen und löschen 508
 - 10.7.15 Remote Sources pflegen 509
 - 10.7.16 Repository-Content importieren und aktivieren 510
 - 10.7.17 Debugging-Aktionen 510
 - 10.7.18 Auf Daten von SAP ERP/SAP S/4HANA zugreifen 511
 - 10.7.19 Versuch des Zugriffs auf Daten von SAP ERP bzw. SAP S/4HANA 511
 - 10.7.20 Tenant-Datenbanken löschen 512
 - 10.7.21 Tenant-Datenbanken pflegen 513
 - 10.7.22 Tenant-Datenbanken stoppen 513
 - 10.7.23 Protokollierung in SAP HANA XSA 514

- 11 Sicherheit und Berechtigungen in SAP HANA Cloud** 515

- 11.1 Aufbau von SAP HANA Cloud** 516
 - 11.1.1 Die SAP-HANA-Datenbank-Instanz 516
 - 11.1.2 Die Data-Lake-Instanz 517
 - 11.1.3 Die Instanzen verwalten 520

11.2	Systemsicherheit in der SAP-HANA-Datenbank-Instanz	521
11.2.1	Systemparameter pflegen	522
11.2.2	Authentifizierung in SAP HANA Cloud	523
11.2.3	Verschlüsselung von Daten	524
11.2.4	Verbindungen zu anderen Systemen – Remote Sources	524
11.2.5	Alerts	526
11.3	Benutzerverwaltung in SAP HANA Cloud	527
11.3.1	Der Benutzer »SYSTEM«	527
11.3.2	Der Benutzer »DBADMIN«	528
11.3.3	Berechtigungen für Benutzergruppen	529
11.4	Das Berechtigungskonzept von SAP HANA Cloud	530
11.4.1	System Privileges	530
11.4.2	Rollengruppen	531
11.4.3	HDI-Rollen	534
11.5	Auditing in SAP HANA Cloud	534
11.5.1	Das Auditing konfigurieren	534
11.5.2	Standard-Auditing-Policies von SAP	535
11.5.3	Von SAP empfohlene Auditing-Policies	536

12 Checklisten zur Analyse der Sicherheit von SAP HANA

12.1	Einführung in SAP HANA	539
12.1.1	Der technische Aufbau von SAP HANA	539
12.1.2	SAP HANA Cockpit	540
12.1.3	DBA Cockpit	541
12.1.4	SAP HANA XS Advanced	543
12.1.5	SAP HANA und SAP ERP bzw. SAP S/4HANA	544
12.2	Netzwerk- und Betriebssystemsicherheit	545
12.2.1	Unix-Benutzer absichern	545
12.2.2	Dateien und Verzeichnisse schützen	546
12.2.3	Exportierte Dateien schützen	547
12.2.4	Zugriff auf die Unix-Ebene vom ABAP-Stack aus	548
12.2.5	Aktionen unter Unix protokollieren	550
12.3	Systemsicherheit in SAP HANA	550
12.3.1	Lizenzen verwalten	550
12.3.2	Systemparameter pflegen	551

12.3.3	Daten verschlüsseln	553
12.3.4	Kommunikation verschlüsseln	555
12.3.5	Verbindungen zu anderen Systemen – Remote Sources	556
12.3.6	Alerts	559
12.4	Sicherheit in Multi-Tenant-Datenbanken	560
12.4.1	Das Konzept der Tenant-Datenbanken	560
12.4.2	Tenant-übergreifende Zugriffe	561
12.4.3	Nicht änderbare Parameter in Tenants	561
12.4.4	Einschränkung von Funktionen in Tenants	562
12.4.5	High Isolation Level für Tenants	562
12.4.6	Änderungen an Tenants protokollieren	563
12.5	Authentifizierung in SAP HANA	563
12.5.1	Authentifizierungsmethoden	563
12.5.2	Kennwortrichtlinien	566
12.6	Benutzerverwaltung in SAP HANA	568
12.6.1	Der Benutzerstammsatz	568
12.6.2	SAP-HANA-XS-Advanced-Benutzer	570
12.6.3	SAP-HANA-Standardbenutzer	571
12.6.4	Benutzergruppen	573
12.7	Das Berechtigungskonzept von SAP HANA	574
12.7.1	Das Konzept der SAP-HANA-Berechtigungen	574
12.7.2	System Privileges	575
12.7.3	Object Privileges	577
12.7.4	Package Privileges	578
12.7.5	Analytic Privileges	578
12.7.6	Privileges zuordnen	579
12.7.7	Berechtigungen in SAP HANA XS Advanced	580
12.8	Das Rollenkonzept von SAP HANA	582
12.8.1	Eigenschaften von Rollen	582
12.8.2	Runtime-Katalogrollen	582
12.8.3	Design-Time-Repository-Rollen (XSC)	583
12.8.4	Design-Time-HANA-DI-Rollen (XSA)	585
12.8.5	SAP-HANA-Standardrollen	587
12.9	Das SAP-HANA-Berechtigungskonzept analysieren	589
12.10	Auditing in SAP HANA	591
12.10.1	Das Auditing in SAP HANA konfigurieren	591
12.10.2	Policies einrichten	592
12.10.3	Das Auditing auswerten	594

12.10.4 Auditing-Protokolle löschen	595
12.10.5 Auditing in SAP HANA XSA	595
12.11 Sicherheit und Berechtigungen in SAP HANA Cloud	596
12.11.1 Systemsicherheit in der SAP-HANA-Datenbank-Instanz	597
12.11.2 Benutzerverwaltung in SAP HANA Cloud	597
12.11.3 Das Berechtigungskonzept von SAP HANA Cloud	598

Anhang	601
---------------	------------

A Sicherheitsrelevante Systemparameter	601
B Sicherheitsrelevante Views in SAP HANA	607

Der Autor	613
Index	615