

Auf einen Blick

1	Einführung in die SAP Business Technology Platform	17
2	Sicherheit auf der SAP Business Technology Platform im Überblick	53
3	Sicherheit und Berechtigungen in der Neo-Umgebung konfigurieren	125
4	Sicherheit und Berechtigungen in der Cloud-Foundry- Umgebung konfigurieren	191
5	Cloud Connector	239
6	Administrationswerkzeuge der SAP Business Technology Plattform	299
7	Sicherheitsaspekte wichtiger Cloud-Services	339

Inhalt

Einleitung	13
------------------	----

1 Einführung in die SAP Business Technology Platform 17

1.1 Positionierung der SAP Business Technology Platform innerhalb der SAP-Strategie	18
1.1.1 Innovation: Entwicklung neuer Cloud-Lösungen	21
1.1.2 Erweiterung: Erweitern von SAP-Cloud-Lösungen	23
1.1.3 Integration: Cloud-Lösungen und On-Premise-Systeme ...	25
1.2 Umgebungen der SAP Business Technology Platform	27
1.2.1 Neo-Umgebung	29
1.2.2 Cloud-Foundry-Umgebung	31
1.2.3 Wahl der Umgebung	36
1.3 Architektur der SAP BTP	37
1.3.1 Global Account	39
1.3.2 Subaccount	42
1.3.3 Organisationen	46
1.3.4 Spaces	49

2 Sicherheit auf der SAP Business Technology Platform im Überblick 53

2.1 Sichere Kommunikation	53
2.1.1 Grundlagen der sicheren Kommunikation	54
2.1.2 SAP Destination Service	56
2.1.3 Zertifikatsbehandlung in Destinationen	60
2.2 Authentifizierung	63
2.2.1 Identity Provider für die SAP Business Technology Platform	64
2.2.2 Lightweight Directory Access Protocol	74
2.3 Autorisierung	76

2.4	SAP Cloud Identity Services	79
2.4.1	Identity Authentication	80
2.4.2	Identity Provisioning	111
2.5	SAP Cloud Identity Access Governance	120
2.6	Checkliste zur allgemeinen Sicherheit der SAP Business Technology Platform	122
3	Sicherheit und Berechtigungen in der Neo-Umgebung konfigurieren	125
3.1	Kommandozeile für die Neo-Umgebung einrichten	126
3.2	Benutzerverwaltung	129
3.3	Trust-Konfiguration	137
3.3.1	Lokalen Service Provider einrichten	137
3.3.2	Plattform-Identity-Provider einrichten	139
3.3.3	Anwendungs-Identity-Provider einrichten	143
3.4	Berechtigungsverwaltung	148
3.4.1	Rollen anlegen und verwalten	149
3.4.2	Benutzergruppen anlegen und verwalten	163
3.5	Checkliste zu Sicherheit und Berechtigungen in der Neo-Umgebung	167
3.6	Beispiele für die Benutzer- und Berechtigungsverwaltung aus der Praxis	168
3.6.1	Zwei-Faktor-Authentifizierung von Subaccount-Admins unter Verwendung des Plattform-Identity-Providers	168
3.6.2	Authentifizierung von Benutzern der SAP Web IDE mittels Microsoft Azure Active Directory	176
4	Sicherheit und Berechtigungen in der Cloud-Foundry-Umgebung konfigurieren	191
4.1	Kommandozeile für die Cloud-Foundry-Umgebung einrichten	193
4.2	Benutzerverwaltung	195

4.3	Trust-Konfiguration	198
4.3.1	SAP ID Service einrichten	199
4.3.2	Plattform-Identity-Provider einrichten	200
4.3.3	Identity Provider von Drittanbietern einrichten	201
4.4	Berechtigungsverwaltung	203
4.4.1	Rollen anlegen und verwalten	203
4.4.2	Sammelrollen pflegen	208
4.4.3	Sammelrollen-Mapping	213
4.4.4	Reporting im Berechtigungsumfeld	216
4.5	Checkliste zu Sicherheit und Berechtigungen in der Cloud-Foundry-Umgebung	217
4.6	Beispiele für die Benutzer- und Berechtigungsverwaltung aus der Praxis	219
4.6.1	Aktivierung und sichere Konfiguration des SAP Launchpad Service	219
4.6.2	Zwei-Faktor-Authentifizierung von Benutzern über das Microsoft Azure Active Directory	227
5	Cloud Connector	239
5.1	Architektur	240
5.2	Installation und Konfiguration des Cloud Connectors	244
5.2.1	Download und Installation	244
5.2.2	Initiale Konfiguration	246
5.2.3	Verbindung zur SAP Business Technology Platform	249
5.2.4	Weitere Empfehlungen zur sicheren Konfiguration	252
5.2.5	Monitoring	254
5.3	Authentifizierungsmethoden	256
5.4	Cloud-zu-on-Premise-Verbindungen	258
5.4.1	Sicherheitsvorkehrungen für Cloud-zu-on-Premise-Verbindungen	259
5.4.2	Verbindung einrichten	263
5.4.3	Zugriffskontrolle konfigurieren	268
5.4.4	SAP Connectivity Service aktivieren	273
5.5	Einrichtung des SAP Destination Service	276
5.5.1	Destinationen in der Neo-Umgebung anlegen	277
5.5.2	Destinationen in der Cloud-Foundry-Umgebung anlegen	280

5.6	Checkliste für die Konfiguration des Cloud Connectors	281
5.7	Beispiele zur sicheren Konfiguration des Cloud Connectors in der Praxis	282
5.7.1	Einen On-Premise-Git-Server an die Neo-Umgebung anbinden	283
5.7.2	Cloud-Foundry-Umgebung an ein SAP-S/4HANA-System anbinden	289
5.7.3	Konfiguration der LDAP-Authentifizierung	294

6 Administrationswerkzeuge der SAP Business Technology Platform 299

6.1	Administration der Neo-Umgebung über die Kommandozeile	300
6.2	Verwaltung des Global Accounts mit dem SAP BTP Command Line Interface	303
6.3	Administration über APIs	305
6.3.1	SAP API Business Hub	306
6.3.2	Audit Log über APIs abrufen	308
6.3.3	Benutzerverwaltung über APIs	316
6.3.4	Berechtigungsverwaltung über APIs	321
6.3.5	APIs des SAP Cloud Management Service	324
6.4	Checkliste zur Arbeit mit der Kommandozeile und APIs	331
6.5	Beispiele zur sicheren Verwendung der Kommandozeile	331
6.5.1	Kommandozeile zur Konfiguration einer Custom Domain in der Neo-Umgebung verwenden	332
6.5.2	Kommandozeile zur Verwaltung der SAP Business Technology Platform verwenden	334

7 Sicherheitsaspekte wichtiger Cloud-Services 339

7.1	SAP Web IDE und SAP Business Application Studio	341
7.1.1	SAP Web IDE	341
7.1.2	SAP Business Application Studio	344

7.2	SAP Cloud Integration	348
7.2.1	SAP Cloud Integration in der Neo-Umgebung	348
7.2.2	SAP Cloud Integration in der Cloud-Foundry-Umgebung	353
7.2.3	Rollen und Berechtigungen	360
7.3	SAP API Management	362
7.3.1	Rollen und Berechtigungen	363
7.3.2	Absicherung der bereitgestellten APIs	365
7.4	SAP Cloud Portal Service und SAP Launchpad Service	366
7.4.1	SAP Cloud Portal Service in der Neo-Umgebung	366
7.4.2	SAP Launchpad Service in der Cloud-Foundry-Umgebung	371
7.5	SAP Internet of Things	371
7.6	SAP BTP, ABAP Environment	375
7.6.1	Benutzerverwaltung	377
7.6.2	Zugriff auf Fremdsysteme	379
7.7	Corporate User Store	380
7.8	Checkliste zur Absicherung von Cloud-Services	383

Das Autorenteam	385
Index	387